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

Copyright SANS Institute
Author Retains Full Rights

This paper is from the SANS Penetration Testing site. Reposting is not permitted without express written permission.

Interested in learning more?
Check out the list of upcoming events offering
"Web App Penetration Testing and Ethical Hacking (SEC542)"
at https://pen-testing.sans.org/events/
ITDOCS
One Admin's Documentation is their Hacker's Pentest

GIAC GPEN Gold Certification

Author: Rob VandenBrink, rvandenbrink@metafore.ca
Advisor: Pedro Bueno

Accepted: 11 December, 2009

Abstract

At the beginning of a recent client engagement, I was asked to create system documentation for a mixed Windows, Linux and Netware environment. Since the actual engagement was to include upgrades to all of these components, documenting the soon-to-be-destroyed environment didn’t seem like time well spent. Instead, it was decided to automate the documentation, using a set of scripts with a simple front-end web page. As the scripts were created, it was found that the initial job of documentation actually took significantly less time than assembling and arranging the system information manually, even accounting for the development effort. Since the documentation was automated, we scheduled it to run daily, ensuring that system documentation was always up to date during the project. This set of scripts has grown to a point that they are worth describing in their own right. The collection of scripts has been named “IT-DOCS”, since “IT” Documents “IT” infrastructure. IT-DOCS now includes scripts to generate documentation reports for various platforms, scripts to audit for change control and scripts to audit for compliance.
1. Introduction

This paper describes the background, design and specifics of an automated, script based documentation system for IT infrastructure called IT-DOCS. We begin with a short background on scripting, outlining common motives for scripting – for simplifying common, repetitive operations, to facilitate repeatability for benchmarks and audits, and for training and education purposes. It is felt that the IT-DOCS project fills all three of these goals.

We then discuss specific uses for scripting that are addressed by IT-DOCS – namely documentation, audit for compliance and audit for change control. Operating System specific scripting methods and issues are discussed, as well as how scripting, documentation and IT-DOCS interacts with penetration tests.

Finally, specifics of the IT-DOCS tool are discussed, including design constraints, implementation for various operating platforms, example script illustrations and output examples.

2. Some Common Goals of Scripting:

Scripts are created for many reasons. The common wisdom is “anything worth doing twice is worth scripting”.

Scripts are often created for common operations, any task that needs to be done frequently. Repetitive tasks and operations that have a high risk of error, either because of typo’s, missed steps, or simply different people doing the same task correctly, but differently. Creation of new user accounts is a great example of this, where you may have many people, all creating accounts in slightly different ways as they navigate the standard operating system interfaces. This is generally an undesirable situation, especially in larger corporations, and the solution is often to script the task.
Repetitive Tasks and Operations are another example where scripts can “come to the rescue”. A good example of this might be periodic audits of disk space used by user files, where a set of simple tasks (adding file space in a directory) must be executed hundreds or thousands of times to create a final report.

Repeatable operations are slightly different than repetitive operations. Repeatable operations are often complex tasks that must be repeated in exactly the same way in similar situations for later comparison against previous runs or an original benchmark. Scripts used in security or documentation audits, or audits of any kind, are an excellent example of this. An audit report is much more useful if the items being measured are measured in exactly the same way on successive runs. This allows successive audits to show either positive or negative progress. Also, if a complex script is written that measures compliance against a regulatory requirement, that same script can measure the same compliance metric at multiple clients as well as on successive runs for the same company.

Education is an important component that is often not discussed when describing scripts. The act of writing a script, especially a complex script that handles complex operations or situations, is a great way of learning aspects of an Operating System or environment that would otherwise never be explored. In addition, because scripts are usually collections of standard commands that can be run from the command line interface of the target operating system, a properly written, commented and documented script is an excellent education tool for other team-members, or for clients if the script is written as part of a consulting engagement.

Of course, these almost never occur in isolation. Many scripts replace repetitive, complex operations, that must be repeatable, and can also serve as an education conduit.

Rob VandenBrink. rvandenbrink@metafore.ca
In all cases, the underlying intent of scripting an operation is to minimize the effort of completing the operation in the minimum amount of time, with no mistakes.

2.1. Documentation
A common use of scripting which is explored in this paper, is to create basic system documentation, which is a critical tool in maintaining a reliable system. This approach can be used to create documentation on a local host, or remotely over a network. Both approaches are discussed in this paper.

2.2. Audit for Compliance
Another common use of scripting, which is related to basic system documentation is to document a system with a final output expressing a compliance stance as compared to an external specification. Reports of this kind are often to compare a system's configuration against a regulatory compliance specification or security benchmark. This is also addressed in this paper, with a script measuring VMware ESX (version 3.5 or 4.0) compliance against the VMware Hardening Guide version 3.5, the current version as of the release of this paper.

2.3. Audit for Change Control
2.3.1. Zero day code
During a discussion about malware at a recent SANS class, the instructor (Ed Skoudis) remarked - “Sure you could catch zero days [malware] – just list all the processes on all the windows machines on your network, every day. You all know what’s normal on your systems right?” (paraphrased) (Skoudis, 2008). This sparked an idea, which in turn became a SANS paper in it’s own right. In a recent SANS Technology Institute (http://sans.edu) paper, Jim McMillan and I wrote exactly this, a set of CMD files and WMIC scripts that inventory all running processes on all stations in a Windows domain. Known good processes are

Rob VandenBrink. rvandenbrink@metafore.ca
whitelisted in a text file, and known bad processes are similarly listed in a different text file. At each run, any new processes that have appeared since the last run are listed in a DIFF file.

The idea is that as as the script is used over time, the whitelist file grows to include most (if not all) applications used in the corporation, and the daily DIFF report becomes very small.

This approach has worked extremely well. During initial testing (in a 100 user domain), the DIFF report between Days 1 and 2 identified 1 single net new process, which turned out to be the soft phone application used in the company. The Day 3 run found both an unapproved application and a windows host infected with malware.

The paper and script components can be found on the SANS.edu website, at http://www.sans.edu/resources/student_projects/200909_02.pdf.

In penetration tests, unauthenticated reconnaissance is almost always done early in the process. A script of this type is also included in IT-DOCS, a TCP connect scan is done of identified subnets. While maintaining a real-time representation of this is of questionable use, the intent of this is to integrate this scan into the change control loop described here. This then identifies new listening services on the network, in addition to net new running processes.
2.4. Scripting methods on various Operating Systems

Windows
Windows has a wide range of commands for displaying and modifying the configuration, including function specific commands such as “ipconfig”, more general command such as “net” or very wide scope command sets, with their own language, such as “netsh”. ADSI (Active Directory System Interface) offers both local and remote access to Active Directory functions and some host functions.

However, for this project, WMIC was chosen for most functions. WMIC (Windows management interface command) has access to the full WMI scope of functions, and permits export of local or remote windows configuration information to several different file formats, including flat text, CSV (Comma Separated Variables) and HTML.

Linux
In contrast to Windows, Linux does not have a general purpose API or command set that can be used for remote documentation. However, it does have several advantages in documentation. Almost everything in Linux is represented in a file. For instance, CPU utilization can be accessed by simply typing the file /proc/cpuinfo, and CPU information (speed, cache and model) can be displayed by typing the file /proc/xasef. Most configuration parameters for the Operating System are represented in a simple fashion in text files, located in /etc. In addition, Linux has a rich set of command line text manipulation facilities, featuring command ssuch as sed, awk, cut and tr. Expert use of these tools allow pinpoint accuracy in extracting information from files in /proc, /etc or other locations, or output from any system command. Access to this full spectrum of tools is best accomplished using SSH. Full and mature support for SSH permits secure access to the system using any supported method.

Rob VandenBrink. rvandenbrink@metafore.ca
ITDOCS: One Admin’s Documentation is their Hacker’s Pentest

Rob VandenBrink. rvandenbrink@metafore.ca

© 2010 The SANS Institute
VMware

The VMware ESX COS (Console Operating System) is very similar to Linux (specifically, Redhat Linux) in it’s documentation facilities, in that the command line has a rich set of Linux commands available to document the server. VMware specific commands are also available to document things such as Virtual Machine configuration, Virtual Switch configuration and connections, and other VMware specific functions.

However, the ESXi product is based on Busybox Linux rather than the Redhat base that the ESX COS enjoys. The ESXi product has a much more minimalistic and security conscious stance, to the point that direct remote access via SSH is not available on the product as shipped, and is not recommended to be enabled. This does not mean that there are no opportunities to script though. Scripting can be accomplished using the RCLI (Remote Command Line), using many of the same or similar commands as on ESXi. In addition, the RCLI function can be delivered within a virtual appliance called VMA (Vmware Management Appliance).

The RCLI and VMA methods are limited to accessing the ESX and ESXi servers in the farm. To access the higher level functions within vCenter, the best alternative remains Powershell. While Powershell is a powerful language, it is a large, object oriented language that poses a significant barrier to entry to many system administrators. In addition, all of the Powershell commands that access VMware functions are specific to the PowerCLI interface, so they are not familiar to most system administrators, in fact even the object oriented format and method of collecting data will be foreign to most. Finally, Powershell has a modular approach, where the PowerCLI is an imported module of commands. As more and more modules are in common use within powershell, we will find that powershell programs will or won’t work

Rob VandenBrink. rvandenbrink@metafore.ca
SSL and Telnet Enabled Devices and Hosts

Any device that can be administered remotely via telnet or SSH command line can easily documented using that method. The client of choice in this situation would be plink.exe, the text-only terminal application that is part of the PUTTY suite of products (reference here), which supports both SSH and Telnet.

While Netware is reaching end of life, there is still in use by a large install base. Scripting in Netware is split into two sections. At the server command line, scripts are most often run at the local screen and keyboard, or scheduled via a native CRON facility. There is an SSH function available, however, most Netware shops are in “don't rock the boat” mode. Their efforts are concentrated towards minimizing change until a migration project can be approved and started, rather than making non-critical changes to the existing environment.

2.5. Aspects of Scripting in Penetration Tests

There are two aspects to scripting in penetration testing. The more common aspect is the use of scripts in the penetration test itself. Scripting definitely addresses issues in penetration testing that we identified earlier in this paper – penetrations tests involve complex operations, which need to be both repeatable during the penetration test, and consistent between one penetration test and another. In addition, the scripts serve as a valuable education component, especially in consulting engagements when educating the client is always a positive thing to strive for.

For instance, the IT-DOCS toolkit outlined in this paper has been very valuable in penetration tests in several security engagements. A common timeline for an internal penetration test might be:

- Using a Windows host, get a DHCP IP Address
- Run “ipconfig /all”

Rob VandenBrink. rvandenbrink@metafore.ca
• Using CAIN, run a Man in the Middle Attack on the first DNS Server in the workstation’s list – this is almost always one of the Windows Domain Controllers.

• What is found in almost all cases is that System Administrators just can’t help it – every problem or task seems to involve an RDP (Remote Desktop Protocol) session to their Domain Controller. Within an hour or so, you’re almost certain to have the Domain Administrator password. (http://isc.sans.org/diary.html?storyid=7303)

• Because administrators almost always use common passwords between platforms, you can now generally acquire most or all of the objectives of the Penetration Test, either directly or using other passwords that are now obtainable from the domain.

• With the formal pentest objectives (especially credentials) obtained, IT-DOCS has proven to be a great toolset to collect large volumes of data on the target environment in a very short period of time. By the end of Day 1, it’s almost always possible to state that all the objectives are attained, and have several hundred pages of ancillary material to use as raw material for additional findings.

Of course, the use of IT-DOCS and similar tools has to fall within the bounds of the Statement of Work that describes the Penetration Test.

A much less common aspect of scripting and documentation in Penetration Testing is related to the fact that every IT department seems to have a subdirectory for IT information in the corporate share, often called “IS”, “MIS”, “IT” or similar. This directory almost always has detailed system documentation for almost every critical infrastructure component in the environment. In the case of IT-DOCS, this directory could be the output directory, which holds the documentation, or the input directory, which holds both the collection scripts and the credentials used to collect the configuration data. Also, if any scripts used for documentation happen to store temporary files on the hosts themselves (which IT-DOCS currently does in some cases), these are just as valuable. Finding such a subdirectory or file is a “finding” indeed.

Rob VandenBrink. rvandenbrink@metafore.ca
While in many engagements corporate documents “found” during an assessment cannot be opened, even the sight of a file or directory listing in a Penetration Test Report is enough to raise the blood pressure of any self-respecting IT Director.

3. The IT-DOCS tool

3.1. Implementation constraints

IT-DOCS was designed in the context of a consulting engagement. The tool had to be completed within a set period of time, in fact it had to be completed within the time estimated for a manual documentation process.

This meant that we had to use the methodology of “progressive elaboration” that is part of the Project Management Body of Knowledge (PMBOK) as discussed in SANS Management 525 course and GCPM certification. In the PMBOK context, progressive elaboration means that as a project progresses, the tasks at hand will have maximum detail associated with them, while tasks in the future will very likely not be fully defined until they are closer in the schedule.

Progressive elaboration in this project meant that existing reports, open source tools and operating system tools were all “in play” when designing version 1.0 of the application. As the application evolves, a common approach, common toolsets and especially a common output format will be defined and used across all target operation platforms. This approach means that version 1.0 of the tool, while not perfect, filled the immediate business requirement within the schedule and budget allocated.
3.2. Design

The IT-DOCS toolset has several basic design points:

**Remote execution** – It was decided early to, as much as possible, consolidate all code for documentation into a single repository. Running documentation scripts on the target hosts themselves not only complicates the build and deployment process for new hosts, it also makes it more likely to miss hosts in the documentation process. Centralizing all scripts and reports tends to make documentation a single process, rather than a process on each host.

**No artefacts left on documented hosts** – Leaving intermediate or final files associated with system documentation on target hosts is a clear security risk. A penetration tester or attacker browsing the filesystem who found such a file would then have critical information regarding the overall configuration of the target host, which might otherwise be much more difficult to collect.

**Central collection of all data** – From a customer perspective, it is highly desirable to browse documentation for all target systems from a single interface – in this case a simple 3-pane web page. It is critical, however, to implement proper authentication and filesystem security on this web site, ensuring that only authorized individuals have access to this sensitive information.

**Common report format across all target platforms** – The report formatting should be similar across all platforms. In Version 1 of IT-DOCS, the Linux configuration report and the VMware ESX Compliance report come very close to the final standard desired. Each section should have a title, a short description, the command used to collect the data, the audit finding (in the case of an audit report), and the raw data.
4. IT-DOCS Description - Version 1.0

4.1. Windows
The Windows documentation generated by version 1.0 of IT-DOCS is based mostly on WMI (Windows Management Interface), using the WMIC command. The current reports are all in WMI’s native HTML format, which is at odds with all other IT-DOCS modules. A future version of IT-DOCS will use WMI’s text output instead, and reformat it to match the other reports.

4.1.1. Windows Host Enumeration
The emphasis on version 1.0 of IT-DOCS was in documentation of servers, so a static list of target hosts is used for scheduled reporting in this version. However, in a future version of the tool, windows host enumeration could be done either by sweeping a set of subnets or by using Active Directory to identify domain members.

Sweeping a subnet could be done by using NMAP or some other port scanner, for instance by scanning for hosts with open “windows ports”, such as 445/tcp. However, as more and more windows hosts implement the Windows Firewall, this approach can become problematic. A more reliable method might be to use the DSQUERY command, which can be used to output the names of all hosts in the domain. The format of this command might be similar to this, which outputs the ip addresses of all computers in a domain (note that this command line is wrapped):

```
dsquery computer -s DCname -u domainname\administrator -p adminpassword -limit 10000 | cut -d "," -f1 | cut -d "=" -f2 >>iplist.txt
```

this could be modified and run as “dsquery server ...” to output only server names in a domain.

Rob VandenBrink. rvandenbrink@metafore.ca
However, this dsquery approach has the obvious problem of missing non-domain members entirely. The obvious solution is to implement both approaches, and use the best approach for any given situation.

4.1.2. Windows Host Assessment

As discussed, WMI is the mechanism chosen for Windows Host assessment. While the information of many WMI commands can be expressed by other command line utilities, WMI gives us a common method of collecting almost everything required, with a single syntax and a single output format. Most WMI inventory commands will look very similar. For instance, this one lists the BIOS version information of a target host (command line is wrapped):

```
wmic /output:%DIRNAME%\bios.htm /user:%UID% /password:%PWD% /node:%IP% bios list brief /format:htable
```

where:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/output:%DIRNAME%\bios.htm</td>
<td>Command output is to be written to a file “bios.htm”, in the directory specified by the %DIRNAME% variable</td>
</tr>
<tr>
<td>/user:%UID%</td>
<td>Login to the target host using the value of the %UID% variable as the username</td>
</tr>
<tr>
<td>/password:%PWD%</td>
<td>Use the %PWD% variable as the password</td>
</tr>
<tr>
<td>/node:%IP%</td>
<td>The target host is represented by the variable %IP%, but can be either the ip address, or a resolvable hostname (CN or FQDN).</td>
</tr>
<tr>
<td>bios list brief</td>
<td>This is the actual WMI command to execute – in this case, a brief listing of the bios information is requested.</td>
</tr>
<tr>
<td>/format:htable</td>
<td>The output format in this case is to an HTML table.</td>
</tr>
</tbody>
</table>

The WMI commands used for host documentation in Version 1.0 of IT-DOCS are:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qfe list brief</td>
<td>List all patches and Hotfixes</td>
</tr>
<tr>
<td>os.get name,</td>
<td>Get the Operating System and Service Pack version.</td>
</tr>
<tr>
<td>servicepackmajorversion</td>
<td></td>
</tr>
<tr>
<td>os list full</td>
<td>List Operating System Information</td>
</tr>
<tr>
<td>bios list brief</td>
<td>List BIOS version information</td>
</tr>
<tr>
<td>computersystem list</td>
<td>Basic system information</td>
</tr>
<tr>
<td>logicaldisk list brief</td>
<td>List logical disk partition information, including volume names, sizes and free space.</td>
</tr>
<tr>
<td>csproduct list brief</td>
<td>List installed products</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>group list</td>
<td>List local groups. If the target is a domain controller, all groups in the domain are listed.</td>
</tr>
<tr>
<td>useraccount list</td>
<td>List local user accounts. If the target is a domain controller, all users in the domain are listed.</td>
</tr>
<tr>
<td>sysaccount list</td>
<td>Built in system account status</td>
</tr>
<tr>
<td>netclient list</td>
<td>Network clients installed, which might include Microsoft networking client, NFS client, Terminal Services client, or in some cases Antivirus clients.</td>
</tr>
<tr>
<td>share list</td>
<td>List all shares on the host.</td>
</tr>
<tr>
<td>nicconfig list</td>
<td>List network card information</td>
</tr>
<tr>
<td>product get vendor, name, version, installdate, packagecache, description, identifyingnumber</td>
<td>List information on all installed applications.</td>
</tr>
<tr>
<td>service list</td>
<td>List all services, including current status and startup settings.</td>
</tr>
</tbody>
</table>

These commands can and should all be refined significantly – in many cases too much information is returned. For instance, “wmic share list” might be more succinctly stated “wmic share get name, path” and “wmic nicconfig list” might be more useful as “wmic niconfig ipaddress,macaddress”. In addition, some additional information might be required – for instance, more hardware information might be needed if IT-DOCS was to be used to evaluate which desktop computers might be due for replacement (by evaluating CPU hardware information or disk utilization statistics for instance).

In the next version of the tool, the scope of each tool will be evaluated in much more detail, and the format of the output will most likely be modified to comply with the final format standard.

### 4.1.3. Windows Active Directory Enumeration

As stated above, many Active Directory metrics can be reported on simply by taking host commands and directing them to a Domain Controller. User and Group lists for instance fall into this category.

Rob VandenBrink. rvandenbrink@metafore.ca
However, there are many Domain parameters that do not seem to be accessible from the WMIC command line tool. The DSQUERY command for instance can be useful in this regard. Some common DSQUERY commands (used by IT-DOCS) are listed here:

<table>
<thead>
<tr>
<th>Dsquery computers</th>
<th>List all computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dsquery servers</td>
<td>List all servers</td>
</tr>
<tr>
<td>Dsquery ou</td>
<td>List all Organizational Units (OUs)</td>
</tr>
</tbody>
</table>

Group Policy is not nearly as well represented with scripting tools. In order to get supported scripting interface to Group Policy in windows 2003 for instance, you must install GPMC, which installs COM objects and a number of JSCRIPT and VBSERSCRIPT scripts that can in turn be used from the command line. However, in Server 2008, this function is moved over to powershell, where a series of cmdlets are available for Group Policy administration and reporting, after importing the group-policy module. This is described in detail at


For instance, in Server 2003, the ListSOMPolicyTree script lists all links between AD Objects and Group Policy Objects. A partial listing is shown below

C:\Program Files\GPMC\Scripts>cscript /nologo ListSOMPolicyTree.wsf
== GPO Links for domain THEDOMAIN ==
DC=THEDOMAIN
  GPO=Default Domain Policy
  GPO=Office2000
  GPO=Outlook-EditOptions
  GPO=IE-Options
  GPO=Outlook2002-SecuritySettings
  GPO=Citrix-UserConnectionSettings
  GPO=Citrix-NoIdleDisconnect
  GPO=Outlook2002-CheckSecuritySettingsFromExchange
OU=Domain Controllers
  GPO=Default Domain Controllers Policy
  GPO=Block-IE7-WindowsUpdate
  GPO=DNS-DynamicUpdateSingleNameDomain
OU=IRELAND USERS - NO INTERNET
  GPO=No Internet
  GPO=[Inaccessible]
OU=QA TESTERS
  GPO=QA TESTERS
OU=FLOOR USERS
  GPO=No Internet
  GPO=Floor Users - Least Restrictive

Rob VandenBrink. rvandenbrink@metafore.ca
GPO=Floor Users
OU=Workstations
  GPO=Block-IE7-WindowsUpdate
  GPO=DST Registry Update and Refresh
  GPO=DNS-DynamicUpdateSingleNameDomain
OU=CitrixFarm
  GPO=Block-IE7-WindowsUpdate
  GPO=Citrix-DeleteCachedRoamingProfiles
  GPO=Citrix-DisableScreenSaver
  GPO=Citrix-FolderRedirection
  GPO=Citrix-HideSystemDrives
  GPO=Citrix-PreventAddPrinter
  GPO=Citrix-IE-BlockInternet
  GPO=Citrix-PreventControlPanel
  GPO=Citrix-IE-SecurityZones
  GPO=DISCONNECT Terminal connections

=== GPO Links for sites in forest DC=THEDOMAIN ===
  CN=CA
  CN=Default-First-Site-Name
  CN=MO
  CN=NC

C:\Program Files\GPMC\Scripts>cscript /nologo DumpGPOInfo.wsf
workstations

Name: Workstations
ID: {0F58606C-FOED-4968-9BF6-F188B46DE7D4}

-- Details --
Created: 3/1/2006 2:51:04 PM
Owner: THEDOMAIN\Domain Admins

User Enabled: False
Mach Enabled: True

-- Version Numbers --
User DS: 0
User Sysvol: 0
Mach DS: 7
Mach Sysvol: 7

-- Who this GPO applies to --
Authenticated Users

-- Who can edit this GPO --

-- Who can edit settings, modify security and delete this GPO --
Domain Admins
Enterprise Admins
SYSTEM

Rob VandenBrink. rvandenbrink@metafore.ca
-- Who only has Read access --
ENTERPRISE DOMAIN CONTROLLERS

-- Who has custom permissions --

-- Where this GPO is linked (Sites, Domain, OU) --
Workstations (OU)

==============================================
The command “C:\Program Files\GPMC\Scripts> cscript
GetReportsForAllGPOs.wsfc:\reports” outputs the actual settings in each Group Policy in the domain to both HTML and XML report formats – the output for a single policy is shown below:

Citrix-DeleteCachedRoamingProfiles
Data collected on: 12/6/2009 12:35:39 PM

<table>
<thead>
<tr>
<th>General</th>
<th>hide all</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain</strong></td>
<td>THEDOMAIN</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>THEDOMAIN\Domain Admins</td>
</tr>
<tr>
<td><strong>Created</strong></td>
<td>9/20/2006 3:38:28 PM</td>
</tr>
<tr>
<td><strong>Modified</strong></td>
<td>12/3/2009 12:13:16 PM</td>
</tr>
<tr>
<td><strong>User Revisions</strong></td>
<td>0 (AD), 0 (sysvol)</td>
</tr>
<tr>
<td><strong>Computer Revisions</strong></td>
<td>1 (AD), 1 (sysvol)</td>
</tr>
<tr>
<td><strong>Unique ID</strong></td>
<td>(459C00EB-F08C-45F3-B0A5-41D086C76FF7)</td>
</tr>
<tr>
<td><strong>GPO Status</strong></td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Details</th>
<th>hide</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location</strong></td>
<td>Enforced</td>
</tr>
<tr>
<td>CitrixFarm</td>
<td>No</td>
</tr>
<tr>
<td>CitrixServers</td>
<td>No</td>
</tr>
</tbody>
</table>

This list only includes links in the domain of the GPO.

Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:

<table>
<thead>
<tr>
<th>Name</th>
<th>hide</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT AUTHORITY\Authenticated Users</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WMI Filtering</th>
<th>hide</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WMI Filter Name</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

Delegation
These groups and users have the specified permission for this GPO:

<table>
<thead>
<tr>
<th>Name</th>
<th>Allowed Permissions</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>THEDOMAIN\Domain Admins</td>
<td>Edit settings, delete, modify security</td>
<td>No</td>
</tr>
<tr>
<td>THEDOMAIN\Enterprise Admins</td>
<td>Edit settings, delete, modify security</td>
<td>No</td>
</tr>
<tr>
<td>NT AUTHORITY\Authenticated Users</td>
<td>Read (from Security Filtering)</td>
<td>No</td>
</tr>
<tr>
<td>NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Read</td>
<td>No</td>
</tr>
<tr>
<td>NT AUTHORITY\SYSTEM</td>
<td>Edit settings, delete, modify security</td>
<td>No</td>
</tr>
</tbody>
</table>

Computer Configuration (Enabled)
Administrative Templates
System/User Profiles
Policy | Setting |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delete cached copies of roaming profiles</strong></td>
<td>Enabled</td>
</tr>
</tbody>
</table>

User Configuration (Enabled)
No settings defined.

Rob VandenBrink. rvandenbrink@metafore.ca
4.1.4. Enumeration of Unauthorized Windows Software

In a recent paper, the discussion of using WMIC to enumerate a Windows domain for unauthorized software was discussed. The dsquery command is used to list all member computers, and with this list, each computer can then be queried using “wmic process list brief” or similar.

This process list is then evaluated in several ways. A blacklist file is maintained, listing known undesirable processes. A whitelist file is similarly created and maintained, listing all known good processes. At the beginning of the process, both files would be empty, but after the first run, a careful analysis of the output from one known good machine makes a good start on the whitelist file.

At this point, things can become very interesting. As daily runs accumulate, the “diff” command can be used to highlight new processes. These might be as a result of installing new software or patches, in which case they go into the whitelist file. However, in many cases these new processes will represent unauthorized software installed by the end user. In some cases these new processes will represent malware that has been missed by the antivirus software resident on the target computer.

When implemented on a typical domain, this approach can be used to locate unauthorized software or malware almost from Day 1.

This approach is not yet included in the IT-DOCS tool-set, but will certainly be added in the next version. All the code described in this approach is included in the paper that describes this set of scripts, located at http://www.sans.edu/resources/student_projects/200909_02.pdf.

Rob VandenBrink. rvandenbrink@metafore.ca
4.2. Linux

For documentation of the Linux Operating System, a shell script called “sysinfo” authored by Makarand Hazari was used (http://developer.novell.com/wiki/index.php/Sysinfo_-_A_Linux_Box_System_Information_Retriever, 2006). While this script is somewhat old, and originally intended for SUSE linux, it is easily adapted to almost any flavor of Linux. In addition, as a shell script it is easy to see all the commands and components involved in the final output. The script was used as downloaded from the Novell site, with the addition of a single command – “chkconfig –list”, which shows the startup status of all services on the system.

The approach of this script is very much in line with the overall goal of this project. The script is simple, the output shows the section title, the command used for the output, then the output itself. This not only documents the system, but adds to the education component of the entire project.

Since this script was selected late in the project, most of the other IT-DOCS reports do not share this format. The VMware ESX compliance report has a similar format, all other reports will be reformatted to this approach in version 2.0 of the toolset.

However, there are a few drawbacks to using this script. It runs as a shell script, and the output of the script is written to a directory on the target system. The intent of IT-DOCS is to run everything possible remotely, and to collect all output directly to a single repository without leaving any artefacts on the target systems. To this end, this script will be re-written using the plink single-line approach described in the SSH section.

Rob VandenBrink. rvandenbrink@metafore.ca
4.3. VMWare ESX

4.3.1. Configuration Script

VMware ESX offers an extremely rich scripting interface, including the commands vmware-cmd, vimsh, the esxconfig-* commands, and especially the often overlooked esxconfig-info command. In addition, the vm-support script is the standard data collection script for VMware Technical Support, and can be used to collect a huge amount of information about the operating environment of the ESX server it is run on.

In addition to commands, simply browsing the files in /etc, especially the vmware-specific files in /etc/vmware such as /etc/vmware/esx.conf and /etc/vmware/config can yield a wealth of information. Listing the individual .vmx files for each virtual machine can also be useful.

Unfortunately, all of these “traditional” methods are in the process of being phased out. The COS (Console Operating System) of VMware ESX is being replaced by the much smaller ESXi COS. Configuration scripts for ESX will need to be writing using the RCLI (Remote Command Line) or VMA (VMware Management Appliance) interfaces. In addition, all vCenter components are native to the Windows Host that vCenter is installed on. The primary scripting interface for querying vCenter configurations remains Powershell.

The VMware ESX configuration script for IT-DOCS is currently in development, and will be a combination of RCLI or VMA, with a companion set of Powershell scripts.

4.3.2. Compliance Script – Compliance to VMware Hardening Guide

A script for auditing the security posture of an VMware ESX server was written as part of IT-DOCS. All sections within the hardening guide that are “script friendly” are covered. Each section is titled, and descriptions of each check and all commands

Rob VandenBrink. rvandenbrink@metafore.ca
used are outlined in the output. When possible, a check for compliance is made, compliance status is red/green colour coded. Lastly, the raw data is shown.

Some sections of the VMware Hardening Guide are not “script friendly”. For instance, the existence of a dedicated management network is not readily deduced from any script output. In cases such as this, the audit point is still addressed - the script outputs the raw information required for evaluation, with a description of the test’s intent and goal. It is left to the auditor to make the final compliance decision based on that information.

4.4. SSL and Telnet Accessible Network Infrastructure

Data collection from any device that supports administrative access via SSL or Telnet is very simple. The PUTTY utility “PLINK” is used in both instances. For simple devices such as Routers, Switches, UPS PDU’s, I/O redirection can be used. For instance, for a simple Router or Switch configuration information can be collected using a text file similar to rtrinven.in (below):

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>term len 0</code></td>
<td>Do not paginate the output. “term length 0” is the command on cisco routers, on HP or Brocade, you would use the “skip” command.</td>
</tr>
<tr>
<td><code>show ver</code></td>
<td>Show the version information of the device</td>
</tr>
<tr>
<td><code>show config</code></td>
<td>Show the configuration information of the device</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Logout of the device</td>
</tr>
</tbody>
</table>

And calling that text file using the syntax:

```
plink -l %1 -p %2 %3 < rtrinven.in >%3_inventory.txt
```

However, as the complexity of the input file increases, it is common for plink to simply halt in midstream, and leaving the script in a state that never exits.

To solve this, there are two approaches. The simplest approach is to simply call PLINK for each single command, executing the required commands line-by-line. For instance, the command list above would be executed in a CMD file as:

```
plink -l %1 -p %2 %3 "show ver" >%3_inventory.txt
plink -l %1 -p %2 %3 "show config" >> %3_inventory.txt
```

Rob VandenBrink. rvandenbrink@metafore.ca
Where:

- \%1 is the first argument, the userid to login as
- \%2 is the password
- \%3 is the host identifier (ip address or resolvable host name)

Notice that when calling commands using this method, output pagination doesn’t need to be considered.

A final approach is to encapsulate the entire ssh or telnet process within a higher level language, such as perl, expect or python. This approach runs counter to one of the major advantages of scripting however, namely education. Adding a higher level language simply makes it harder to understand and document the documentation process itself. In consulting, cross-training is often an essential part of the process – the client hires an expert so that not only does the job at hand get done well, but they have an opportunity to learn new methods and approaches along the way. Adding a higher level language simply makes that learning that much more difficult in many cases.

### 4.5. Netware

While Novell Netware is reaching it’s end of life as far as Novell is concerned (March 2010 marks the date that Novell will stop supplying patches and security updates), it is still in use in some large environments who still need reliable, consistent documentation. The approach for documenting a Netware environment took a multi-pronged approach:

**CONFIG.NLM**, running on the Netware server console, is used to create a local config file. **CONFIG.NLM** is called using the command line arguments to collect information that is deemed important at that site. Common switches that might be considered for documentation purposes include:

Rob VandenBrink. rvandenbrink@metafore.ca
/s, to get all local server SET parameters.
/e eDirectory information, and a list of partitions
/f include all NCF files in C: and SYS: volumes
/w include Java and Client executable files
/j list all running Java processes
/z include boot drive and netware storage device and volume information
/m lists the versions of all running modules
/ALL will list all this information, as well as pages and pages of other info.
(http://support.novell.com/docs/Readmes/InfoDocument/2974871.html)
As can be seen, each additional configuration switch will add to the length of the report. Care should be taken that only the most useful information is collected, so that the report remains readable.

The CONFIG.NLM run is scheduled using CRON, first by ensuring that CRON is running (ensure that “LOAD CRON” is in the AUTOEXEC.NCF file), and by editing /etc/crontab, and adding the line:

```
1 0 * * * SYS:SYSTEM/CONFIG.NLM /sefm
```
which will run the CONFIG.NLM process at 1 minute past midnight, every day.

Netware commands are used to collect additional information. “CX” is used to collect NDS Tree information. NLIST is used to collect user information, including information specific to unused or disabled accounts, or accounts that do not require a password. NLIST is also used to collect group membership data. The RIGHTS command is used to collect rights assignments in the Netware filesystem. Specific command line switches for each command are listed in the Netware Scripts Appendix.

After all this is completed, the text outputs are converted to HTML to make viewing with a browser simpler.

Rob VandenBrink. rvandenbrink@metafore.ca
5. IT-DOCS Development Plan
As noted in the implementation constraints, the toolset as it stands now is far from complete. The current script has different report formats across the different platforms,

5.1. Version 1.0
As discussed, version 1.0 of IT-DOCS was completed under a hard time limit. While all the target Operating Systems have documentation reports in the output, there are several issues with the current code:
• All of the credentials required to collect the documentation information from each OS are stored in a clear text file
• Linux reports are created on each local Linux host, and stored locally on a text file on each host for later collection.
• Windows reports are use the Microsoft HTML output format, which differs from all other reports.
• VMware reports are all done via shell scripts.
• Some popular operating environments are simply not represented. For instance, a request for AS/400 (IBM iSeries) support in the current version was deferred to a later version of the code. In addition, support has been requested for documentation of applications such as MS Exchange, MS SQL and other popular applications.
To this end, a roadmap for future development has been identified, outlined here. In all future releases, the report information itself will also be updated in each version going forward. For instance, many of the Windows reports simply contain too much information, or in some cases tables with empty columns. It’s also very likely that there is information that is missed entirely. For instance, the current version does not contain any of the Active Directory Group Policy reports.

Rob VandenBrink. rvandenbrink@metafore.ca
5.2. Version 2.0

There is an immediate need for changes to IT-DOCS before it can be used for other customer projects or environments.

Remote execution is required for the Linux reports. The function currently delivered by sysinfo.sh will be migrated to a remote ssh approach. This removes the script and more importantly the script output from the host being documented.

Reformat all windows reports to the common format. The current native Microsoft HTML does not match the standard IT-DOCS format. The windows reports should, for each audit point or section have a title, a short description of the section, the command used to create the output, and the output itself. This not only standardizes the output of the Windows reports, but more importantly meets the education requirement of the IT-DOCS package.

The VMware documentation and audit scripts should be re-written to run remotely. The current thinking is that vCLI (vSphere Command Line Interface) or VMA (vSphere Management Assistant) might be the desired development platform for these reports, instead of shell scripts. The stated direction of VMware is to move the ESX product towards the ESXi model (based on busybox linux), where shell scripts and ssh access are simply not viable options for documentation. VMA is actually a virtual appliance that offers an alternative to scripting, but keeps the approach of using common commands to create scripts.

Powershell, coupled with VMware’s PowerCLI is also a very good alternative approach for a future direction. However powershell is simply too complex to satisfy the education component of the IT-DOCS tools. While Powershell is certainly available on all modern Windows platforms, complex Powershell applications are often not as portable as other scripting languages are, due to requirements for the implementation of exact versions of the appropriate Powershell bolt-ons make consistent delivery of a script to all clients problematic.

Rob VandenBrink. rvandenbrink@metafore.ca
While vCLI or VMA might be the preferred platforms for auditing or documenting individual ESX or ESXi hosts, these approaches cannot be used to document higher level vSphere constructs, such as DataCenter settings, Resource Pool settings, security within vCenter or settings on distributed virtual switches. For the higher level constructs within vSphere, Powershell is truly the only approach possible.

**DIFF reports**
The inclusion of DIFF reports in the documentation allows comparison of configuration settings between one day and another. This facilitates several things:

- Verification that approved changes were completed as described and on schedule
- Verification that unapproved changes are not occurring
- “Unapproved changes” certainly includes installation of unauthorized software, including malware in many cases.

### 5.3. Version 2.1

**Encryption of all credentials stored on disk**
As a security professional, storing all the user credentials for collection of the IT-DOCS data and reporting is an obvious problem. This approach was taken in the interest of getting a set of automated scripts working in as short a time as possible. However, cleartext credentials simply cannot be kept as a long or even short term solution. It’s a obvious security problem, and would be a clear finding on any security audit based on any regulatory framework you’d care to name. All authentication and authorization information used by IT-DOCS should be encrypted on disk. The encryption method has not yet been selected.

Support for client certificates in the SSH collection routines will also be included at this time.
5.4. Version 3.0

Support for other Operating Systems

If interest is expressed, there is no reason that IT-DOCS can't be expanded to include a more diverse set of operating systems. Common server applications are also on the roadmap, and in fact some of these scripts are already started. For instance, Citrix XENAPP reports were completed for a different project, but are not yet in IT-DOCS tool. A list of future IT-DOCS targets might include:

<table>
<thead>
<tr>
<th>Platforms:</th>
<th>Applications:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• OSX</td>
<td>• MS Exchange</td>
</tr>
<tr>
<td>• IBM iSeries (AS/400)</td>
<td>• MS SQL Server</td>
</tr>
<tr>
<td>• Citrix XenApp / Presentation Server</td>
<td>• MS IIS</td>
</tr>
<tr>
<td>• XEN (XEN Server)</td>
<td>• Domino</td>
</tr>
<tr>
<td>• Citrix (XEN APP)</td>
<td>• Oracle</td>
</tr>
<tr>
<td>• IBM pSeries (AIX)</td>
<td>• MySQL</td>
</tr>
<tr>
<td>• Solaris</td>
<td></td>
</tr>
<tr>
<td>• BSD Unix</td>
<td></td>
</tr>
<tr>
<td>• Fiber Channel Switches (Brocade and Cisco)</td>
<td></td>
</tr>
<tr>
<td>• SAN Support (IBM, HP, EMC)</td>
<td></td>
</tr>
</tbody>
</table>

Rob VandenBrink. rvandenbrink@metafore.ca
6. References


Rob VandenBrink. rvandenbrink@metafore.ca

This shell script outputs HTML, it is normally called as ./esxaudit.sh >auditoutput.html. Where “auditoutput.html” is collected after execution to a central repository, generally using a CRON job that calls scp. The output of this job on a test ESX host follows immediately after the commented script.

```bash
#!/bin/bash

#<pre> is an html keyword that indicates the output is pre-formatted, so that end of line characters are handled with carriage-return/linefeed instead of html markup <p> and </p>

#<H1> Compliance Report for ESX Host - </H1>
hostname

#<H3><HR><p style="background-color: #C0C0C0;">Test Description: Inventory ESX Version and Patch Levels</p></H3>
echo -n "Test Commands\n\ncat /etc/vmware-release\n\nesxupdate -l query"

#<HR>

#<H3><HR><p style="background-color: #C0C0C0;">Test Description: Inventory Guests on this ESX Host</p></H3>
for vm in `vmware-cmd –l`
do
  name=`vmware-cmd "$vm" getconfig displayname -q`
  echo VM Displayname $n
  echo VM Path $vm
done

#<H3><HR><p style="background-color: #C0C0C0;">Test Description: Inventory Virtual Switches on each ESX Host</p></H3>
esxcfg-vswitch -l

#<H3><HR><p style="background-color: #C0C0C0;">Test Description: Inventory Guest VM Virtual Switch Connectivity</p></H3>
esxcfg-vswitch -l
```

*vmware-cmd –l* lists all guests
ITDOCS: One Admin's Documentation is their Hacker's Pentest

Rob VandenBrink. rvandenbrink@metafore.ca

```
# Test Commands:
cat /pathspec/guestname.vmx | grep networkName

echo "<b>Test Results:</b>"
echo "<HR>"

for vm in `vmware-cmd -l`
do
    name=`vmware-cmd "$vm" getconfig displayname -q`
    echo $name
    echo -e 'cat $vm | grep networkName'

    echo

done

# Test Description: Verify Guest VM Cut / Paste Restrictions
# This is the first test where we test for actual compliance.

echo "<b>Test Detailed Description: </b> Disable copy and paste operations for the guest operating system between the guest OS and the Remote Console"

echo "<b>Commands to Test (for each VM):</b>"
echo "cat vmname.vmx | grep isolation.tools.copy"
echo "cat vmname.vmx | grep isolation.tools.paste"
echo "cat vmname.vmx | grep isolation.tools.setGUI"
echo "Blank Output indicates default settings (cut/paste permitted)"

for vm in `vmware-cmd -l` ;
do
    name=`vmware-cmd "$vm" getconfig displayname -q`

    val1=`cat $vm | grep isolation.tools.copy | grep -iv true | wc -l`
    val2=`cat $vm | grep isolation.tools.paste | grep -iv true | wc -l`
    val3=`cat $vm | grep isolation.tools.setGUI | grep -iv true | wc -l`
    iscomp=$(($val1+$val2+$val3))

    if [ $iscomp -lt 3 ] ; then
        echo "<FONT COLOR=Red>NONCOMPLIANT</FONT>"
        echo "Non Compliant settings:"
        if [ $val1 -eq 0 ] ; then echo "isolation.tools.copy=true" is required" ; fi
        if [ $val2 -eq 0 ] ; then echo "isolation.tools.paste=true" is required" ; fi
        if [ $val3 -eq 0 ] ; then echo "isolatioln.tools.setGUI=true" is required" ; fi
    else
        echo "<FONT COLOR=Lime>COMPLIANT</FONT>"
    fi

done

# Test Description: Are Guest VMs Prevented from writing name/value pairs to config file?
# Null returns indicate the default (false)

echo "<b>Test Commands - for each VM:</b>"
echo "cat $vm | grep tools.setinfo.disable"
echo "<b>Validation Criteria: </b> these should be set to true. Null returns indicate the default (false)"
```

for vm in `vmware-cmd -l`
   do
     echo `vmware-cmd "$vm" getconfig displayname -q`
     val1=`cat $vm | grep tools.setinfo.disable | grep -i true | wc -l`
     if [ $val1 -eq 0 ]; then
       echo "<FONT COLOR=Red>NONCOMPLIANT</FONT>"
       echo ""tools.setinfo.disable=true" is required"
       echo "Noncompliant settings:"
       cat $vm | grep tools.setinfo.disable
     else
       echo "<FONT COLOR=Lime>COMPLIANT</FONT>"
     fi
   done

for vm in `vmware-cmd -l`
   do
     echo `vmware-cmd "$vm" getconfig displayname -q`
     cat $vm | grep log.rotate
     cat $vm | grep log.keep
     cat $vm | grep sizeLimit
   done

This test is against VMware's numbers – different organizations may elect to use different values. This script is against VMware's documentation.

for vm in `vmware-cmd -l`
   do
     echo `vmware-cmd "$vm" getconfig displayname -q`
     val1=`cat $vm | grep scsi | grep .mode | grep -iv independant-persisent | wc -l`
     if [ $val1 -eq 0 ]; then
       echo "<FONT COLOR=Lime>COMPLIANT</FONT>"
     else
       echo "<FONT COLOR=Red>NONCOMPLIANT</FONT>"
     fi
     cat $vm | grep scsi | grep .mode
   done

Rob VandenBrink. rvandenbrink@metafore.ca
<table>
<thead>
<tr>
<th>echo &quot;&lt;H3&gt;&lt;HR&gt;&lt;p style=&quot;background-color: #C0C0C0;&quot;&gt;Test Description: Guest Unauthorized device connection&lt;/p&gt;&lt;/H3&gt;&quot;</th>
<th>Test Description: Guest Unauthorized device connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>echo &quot;&lt;b&gt;Test Detail:&lt;/b&gt; Ensure that unauthorized devices are not currently connected to guest VMs&quot;</td>
<td>Test Detail: Ensure that unauthorized devices are not currently connected to guest VMs</td>
</tr>
<tr>
<td>echo &quot;&lt;b&gt;Test Command:&lt;/b&gt; cat guestvmxfile.vmx</td>
<td>grep .present&quot;</td>
</tr>
<tr>
<td>echo &quot;&lt;b&gt;Verify values:&lt;/b&gt; Varies by organization&quot;</td>
<td>Verify values: Varies by organization</td>
</tr>
</tbody>
</table>
| for vm in `vmware-cmd -l`  
do  
echo `vmware-cmd "$vm" getconfig displayname -q`  
cat $vm | grep .present  
done | for vm in `vmware-cmd -l`  
do  
echo `vmware-cmd "$vm" getconfig displayname -q`  
cat $vm | grep .present  
done |
| echo "<H3><HR><p style="background-color: #C0C0C0;">Test Description: Guest Prevent Unauthorized Removal or Connection of Devices</p></H3>" | Test Description: Guest Prevent Unauthorized Removal or Connection of Devices |
| echo "<b>Test Command:</b> For each VM: cat <vmname>.vmx | grep isolation.tools.disable " | Test Command: For each VM: cat <vmname>.vmx | grep isolation.tools.disable |
| echo "<b>Verify Values:</b> should be set to \"true\". "false" or blank indicates non-compliance." | Verify Values: should be set to \"true\". "false" or blank indicates non-compliance. |
| for vm in `vmware-cmd -l`  
do  
echo `vmware-cmd "$vm" getconfig displayname -q`  
cat $vm | grep isolation.tools.disable  
if [ $val1 -eq 0 ] ; then  
echo "<FONT COLOR=Red>NONCOMPLIANT</FONT>"  
echo "Noncompliant settings (blank line indicates noncompliance):"  
cat $vm | grep isolation.tools.disable  
else  
echo "<FONT COLOR=Lime>COMPLIANT</FONT>"  
fi  
done | for vm in `vmware-cmd -l`  
do  
echo `vmware-cmd "$vm" getconfig displayname -q`  
cat $vm | grep isolation.tools.disk  
done |
| echo "<H3><HR><p style="background-color: #C0C0C0;">Test Description: Guest Denied Disk Operations D.O.S.</p></H3>" | Test Description: Guest Denied Disk Operations D.O.S. |
| echo "<b>Test Command:</b> cat $vm | grep isolation\:tools\:disk" | Test Command: cat $vm | grep isolation\:tools\:disk |
| echo "<b>Verify Values:</b>: should be set to \"true\". "false" or blank indicates non-compliance." | Verify Values: should be set to \"true\". "false" or blank indicates non-compliance. |
| for vm in `vmware-cmd -l`  
do  
echo `vmware-cmd "$vm" getconfig displayname -q`  
cat $vm | grep guestOS | sort -r  
done | for vm in `vmware-cmd -l`  
do  
echo `vmware-cmd "$vm" getconfig displayname -q`  
cat $vm | grep guestOS | sort -r  
done |
| echo "<H3><HR><p style="background-color: #C0C0C0;">Test Description: Verify that Guest OS Maches ESX Configuration</p></H3>" | Test Description: Verify that Guest OS Maches ESX Configuration |
| echo "<b>Test Command:</b> cat <guestname>.vmx | grep guestOS | sort -r" | Test Command: cat <guestname>.vmx | grep guestOS | sort -r |
| echo "<b>Verify Values:</b>: should be the same value as the actual OS of the Guest VM." | Verify Values: should be the same value as the actual OS of the Guest VM. |
| for vm in `vmware-cmd -l`  
do  
echo `vmware-cmd "$vm" getconfig displayname -q`  
cat $vm | grep guestOS | sort -r  
done | for vm in `vmware-cmd -l`  
do  
echo `vmware-cmd "$vm" getconfig displayname -q`  
cat $vm | grep guestOS | sort -r  
done |

Rob VandenBrink. rvandenbrink@metafore.ca
Rob VandenBrink, rvandenbrink@metafore.ca
<table>
<thead>
<tr>
<th>Processes</th>
<th>ps -efw --forest</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Command:</td>
<td>Cat /etc/sshd/sshd_config</td>
</tr>
<tr>
<td>Verify Values:</td>
<td>PermitRootLogin should be set to no</td>
</tr>
<tr>
<td>Test Command:</td>
<td>cat /etc/sshd/sshd_config</td>
</tr>
<tr>
<td>Test Command:</td>
<td>Is -l /etc/xinetd.d</td>
</tr>
<tr>
<td>Verify Values:</td>
<td>output should be blank</td>
</tr>
<tr>
<td>Test Command:</td>
<td>cat /etc/securetty</td>
</tr>
<tr>
<td>Verify Values:</td>
<td>this listing should be empty</td>
</tr>
<tr>
<td>Test Command:</td>
<td>cat /etc/pam.d/su</td>
</tr>
<tr>
<td>Test Command:</td>
<td>cat /etc/group</td>
</tr>
<tr>
<td>Verify Values:</td>
<td>root only, or authorized users only</td>
</tr>
<tr>
<td>Test Command:</td>
<td>cat /etc/group</td>
</tr>
<tr>
<td>Verify Values:</td>
<td>who has access to the “su” command</td>
</tr>
</tbody>
</table>

Rob VandenBrink, rvandenbrink@metafore.ca
ITDOCS: One Admin’s Documentation is their Hacker’s Pentest

Rob VandenBrink, rvandenbrink@metafore.ca

© 2010 The SANS Institute Author retains full rights.
ITDOCS: One Admin’s Documentation is their Hacker’s Pentest

Rob VandenBrink. rvandenbrink@metafore.ca

if [ $val1 -gt 0 ] ; then
  echo "<FONT COLOR=Lime>COMPLIANT</FONT>"
else
  echo "<FONT COLOR=Red>NONCOMPLIANT</FONT>"
fi

echo "Raw Data:"<br>
cat /etc/pam.d/system-auth | grep pam_tally.so

if [ $val1 -gt 0 ] ; then
  echo "<FONT COLOR=Red>NONCOMPLIANT</FONT>"
else
  echo "<FONT COLOR=Lime>COMPLIANT</FONT>"
fi

echo "Are failed logins logged?"

val=`ls /var/log/faillog | wc -l`
if [ $val1 -gt 0 ] ; then
  echo "<FONT COLOR=Red>NONCOMPLIANT</FONT>"
else
  echo "<FONT COLOR=Lime>COMPLIANT</FONT>"
fi

echo "Is NTP running?"

val1=`ps -efw | grep ntpd | wc -l`
if [ $val1 -gt 0 ] ; then
  echo "<FONT COLOR=Lime>COMPLIANT</FONT>"
else
  echo "<FONT COLOR=Red>NONCOMPLIANT</FONT>"
fi

echo "Is NTP associated with a trusted timesource? (manual verify)"

ntp.conf server settings:
cat /etc/ntp.conf | grep i server
echo "ntp/step-ticker server settings:"
cat /etc/ntp/step-tickers
echo

Service Startup Settings
chkconfig --list | grep ntp
echo
Firewall Settings
esxcfg-firewall | grep ntpClient
echo
"NTP Associations:"
ntpq -p
echo
echo "<H3><HR><p style="background-color: #C0C0C0;">Test Description: are local logs being written?</p></H3>"

echo "<H3><HR><p style="background-color: #C0C0C0;">Test Description: Verify that log file growth is controlled</p></H3>"

echo "<H3><HR><p style="background-color: #C0C0C0;">Test Description: is remote syslog running?</p></H3>"

for fn in vmkernel vmksummary vmkwarning
do
  echo -n "Size limit: " ; cat /etc/logrotate.d/$fn | grep size | grep -v # | grep -v compress
  echo -n "Filename $fn Compression Check: "
  cat /etc/logrotate.d/$fn | grep size | grep -v # | grep compress | grep -v nocompres
  cat /etc/logrotate.d/$fn
  if [ -n " cat /etc/logrotate.d/$fn | grep size | grep -v # | grep compress | grep -v nocompres | wc -l -gt 1 ] ; then
    echo Noncompliant
  else
    echo Compliant
  fi
done

echo "<H3><HR><p style="background-color: #C0C0C0;">Test Description: is remote syslog running?</p></H3>"

if [ -n " cat /etc/syslog.conf | grep @ | wc -l -gt 0 ] ; then
  echo "<FONT COLOR=Lime><FONT COLOR=Lime>COMPLIANT</FONT></FONT>"
else
  echo "<FONT COLOR=Red><FONT COLOR=Red>NONCOMPLIANT</FONT></FONT>"
fi

echo "<H3><HR><p style="background-color: #C0C0C0;">Test Description: Verify correct permissions on VMware utility file permissions</p></H3>"

if [ -n "ls -lh /usr/sbin/esxcfg-* | grep -v esxcfg-auth | grep -v 'r-x------' |" ]; then
  echo "<H3><HR><p style="background-color: #C0C0C0;">Test Results: </p></H3>"
  echo "<HR>
  echo "<HR>
  echo "<HR>
else
  echo "<H3><HR><p style="background-color: #C0C0C0;">Test Results: </p></H3>"
fi

Rob VandenBrink rvandenbrink@metafore.ca
wc -l -gt 0 ]; then
  echo "<FONT COLOR=Red>NONCOMPLIANT</FONT>"
else
  echo "<FONT COLOR=Lime>COMPLIANT</FONT>"
fi

echo -n "<b>Test Results: </b>"

echo -n "<b>esxcfg-auth permissions - "
if [ `ls -lh /usr/sbin/esxcfg-auth | grep -v "^-rwxr-x---" | wc -l` -gt 0 ]; then
  echo "<FONT COLOR=Red>NONCOMPLIANT</FONT>"
else
  echo "<FONT COLOR=Lime>COMPLIANT</FONT>"
fi

echo

echo "<b>Test Raw Data: </b>"

ls -lh /usr/sbin/esxcfg-*

Do log files have the correct permissions?

Test Description: Verify correct file permissions on logs

Test Commands:<b>/</b> ls -lh /var/log

Is -lh /var/log

Is -lh /var/log/vmware

Is -Rlh /vmfs/volumes/

Verify Values:<b>/</b>: all log files have permissions of -rw------- (600)*

except: /var/log/vmware/webAccess/* -rw-r--r-- (755)*

and: Individual Virtual Machine log files -rw-r--r-- (644)*

Do log files have the correct permissions?

Lots more grep !!

Non Compliant Files:

ls -lh /var/log | grep -v drw | grep -v txt | grep -v html | grep -v wtmp | grep -v rpmpkgs | grep -v dme | grep -v lastlog | grep -v "^-rwxr-x---" | grep -v total | wc -l -gt 0 ]; then

This might be better in octal, but is more understandable in ascii

Rob VandenBrink. rvandenbrink@metafore.ca
ITDOCS: One Admin’s Documentation is their Hacker’s Pentest

Rob VandenBrink. rvandenbrink@metafore.ca

© 2010 The SANS Institute    Author retains full rights.
1. Compliance Report for ESX Host -

1.1.1. Test Description: Inventory ESX Version and Patch Levels

**Test Commands**
cat /etc/vmware-release
esxupdate -l query

**Test Results**

VMware ESX Server 3

<table>
<thead>
<tr>
<th>Installed software bundles:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5.0-64607</td>
<td>19:34:53 10/10/08 Full bundle of ESX 3.5.0-64607</td>
</tr>
<tr>
<td>ESX350-200802303-SG</td>
<td>19:34:54 10/10/08 perl security update</td>
</tr>
<tr>
<td>ESX350-200802304-SG</td>
<td>19:34:54 10/10/08 util-linux security update</td>
</tr>
<tr>
<td>ESX350-200802305-SG</td>
<td>19:34:55 10/10/08 openssl security update</td>
</tr>
<tr>
<td>ESX350-200802306-BG</td>
<td>19:34:55 10/10/08 t泽da update</td>
</tr>
<tr>
<td>ESX350-200802408-SG</td>
<td>19:34:55 10/10/08 Security Updates to the Python Package.</td>
</tr>
<tr>
<td>ESX350-200803210-UG</td>
<td>19:34:55 10/10/08 Update to the ESX Server Service Console</td>
</tr>
<tr>
<td>ESX350-200803212-UG</td>
<td>19:34:56 10/10/08 Update VMware qla4010/qla4022 drivers</td>
</tr>
<tr>
<td>ESX350-200803213-UG</td>
<td>19:34:56 10/10/08 Driver Versioning Method Changes</td>
</tr>
<tr>
<td>ESX350-200803214-UG</td>
<td>19:34:57 10/10/08 Update to Third Party Code Libraries</td>
</tr>
<tr>
<td>ESX350-200804404-BG</td>
<td>19:34:57 10/10/08 Update to VMware-esx-drivers-scsi-vmkisc</td>
</tr>
<tr>
<td>ESX350-200804405-BG</td>
<td>19:34:57 10/10/08 Update to VMware-esx-drivers-scsi-megara</td>
</tr>
<tr>
<td>ESX350-200805504-SG</td>
<td>19:34:57 10/10/08 Security Update to Cyrus SASL</td>
</tr>
<tr>
<td>ESX350-200805505-SG</td>
<td>19:34:58 10/10/08 Security Update to unzip</td>
</tr>
<tr>
<td>ESX350-200805506-SG</td>
<td>19:34:58 10/10/08 Security Update to Tcl/Tk</td>
</tr>
<tr>
<td>ESX350-200805507-SG</td>
<td>19:34:58 10/10/08 Security Update to krb5</td>
</tr>
<tr>
<td>ESX350-200805514-BG</td>
<td>19:34:59 10/10/08 Update to VMware-esx-drivers-net-e1000</td>
</tr>
<tr>
<td>ESX350-200808201-UG</td>
<td>19:34:59 10/10/08 Updates VMkernel, Service Console, hostd</td>
</tr>
<tr>
<td>ESX350-200808202-UG</td>
<td>19:34:59 10/10/08 Update to ESX Scripts</td>
</tr>
<tr>
<td>ESX350-200808203-UG</td>
<td>19:34:59 10/10/08 Update to Backup Tools</td>
</tr>
<tr>
<td>ESX350-200808205-UG</td>
<td>19:35:00 10/10/08 Updates to CIM and Pegasus</td>
</tr>
<tr>
<td>ESX350-200808206-UG</td>
<td>19:35:00 10/10/08 Update to vmware-hwdata</td>
</tr>
<tr>
<td>ESX350-200808207-UG</td>
<td>19:35:00 10/10/08 Update to VMware-esx-lnxcfg</td>
</tr>
<tr>
<td>ESX350-200808209-UG</td>
<td>19:35:01 10/10/08 Update to VMware-esx-srvrmgmt</td>
</tr>
<tr>
<td>ESX350-200808210-UG</td>
<td>19:35:01 10/10/08 Update to VMware-esx-drivers-net-ixgbe</td>
</tr>
<tr>
<td>ESX350-200808211-UG</td>
<td>19:35:01 10/10/08 Update to the tg3 Driver</td>
</tr>
</tbody>
</table>

Rob VandenBrink. rvandenbrink@metafore.ca
### 1.1.2.

#### Test Description: Inventory Guests on this ESX Host

**Test Command:** `Vmware-cmd -l`  
**Test Results:**

VM Displayname VM04  
VM Path `/vmfs/volumes/4907c9e2-e2e30320-806d-000c29dba8b9/VM04/VM04.vmx`

VM Displayname VM03  
VM Path `/vmfs/volumes/4907c9e2-e2e30320-806d-000c29dba8b9/VM03/VM03.vmx`

VM Displayname SRV01  
VM Path `/vmfs/volumes/4907c9e2-e2e30320-806d-000c29dba8b9/SRV01/SRV01.vmx`

VM Displayname FW01  
VM Path `/vmfs/volumes/4907c9e2-e2e30320-806d-000c29dba8b9/FW01/FW01.vmx`

### 1.1.3.

#### Test Description: Inventory Virtual Switches on each ESX Host

**Test Commands** `esxcfg-vswitch -l`

<table>
<thead>
<tr>
<th>Switch Name</th>
<th>Num Ports</th>
<th>Used Ports</th>
<th>Configured Ports</th>
<th>MTU</th>
<th>Uplinks</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSwitch0</td>
<td>64</td>
<td>4</td>
<td>64</td>
<td>1500</td>
<td>vmnic0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PortGroup Name</th>
<th>VLAN ID</th>
<th>Used Ports</th>
<th>Uplinks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine Network0</td>
<td>0</td>
<td>vmnic0</td>
<td></td>
</tr>
<tr>
<td>Service Console</td>
<td>0</td>
<td>1</td>
<td>vmnic0</td>
</tr>
</tbody>
</table>

Rob VandenBrink. rvandenbrink@metafore.ca
### Test Description: Inventory Guest VM Virtual Switch Connectivity

**Test Commands:**
```
cat /pathspec/guestname.vmx | grep networkName
```

**Test Results:**

VM04  
ethernet0.networkName = "Public Internet Trust Zone"

VM03  
ethernet0.networkName = "Internal Trust Zone"

SRV01  
ethernet0.networkName = "DMZ Trust Zone"

FW01  
ethernet0.networkName = "Virtual Machine Network"  
ethernet1.networkName = "Virtual Machine Network"  
ethernet2.networkName = "Virtual Machine Network"
1.1.5.

Test Description: Verify Guest VM Cut / Paste Restrictions

Test Detailed Description: Disable copy and paste operations for the guest operating system between the guest OS and the Remote Console

Commands to Test (for each VM):
cat vmname.vmx | grep isolation\tools\copy
cat vmname.vmx | grep isolation\tools\paste
cat vmname.vmx | grep isolation\tools\setGUI

Blank Output indicates default settings (cut/paste permitted)

VM04 NONCOMPLIANT
Non Compliant settings:
"isolation.tools.copy=true" is required
"isolation.tools.paste=true" is required
"isolation.tools.setGUI=true" is required

VM03 NONCOMPLIANT
Non Compliant settings:
"isolation.tools.copy=true" is required
"isolation.tools.paste=true" is required
"isolation.tools.setGUI=true" is required

SRV01 NONCOMPLIANT
Non Compliant settings:
"isolation.tools.copy=true" is required
"isolation.tools.paste=true" is required
"isolation.tools.setGUI=true" is required

FW01 NONCOMPLIANT
Non Compliant settings:
"isolation.tools.copy=true" is required
"isolation.tools.paste=true" is required
"isolation.tools.setGUI=true" is required

1.1.6.

Test Description: Are Guest VMs Prevented from writing name/value pairs to config file?

Test Commands - for each VM
cat /vmfs/volumes/4907c9e2-e2e30320-806d-000c29dba8b9/FW01/FW01.vmx | grep tools.setinfo.disable

Validation Criteria: these should be set to true. Null returns indicate the default (false)

Rob VandenBrink. rvandenbrink@metafore.ca
Test Description: Guest log Size and Rotation

Test Detail
Logs should be rotated when they reach a specific size (100k), rotated to keep old logs (10).
These are the values recommended in the VMware hardening guide, some organizations may elect to set different values as standards.

Validation Criteria:
log.rotateSize = 100000
log.keepOld = 10

tools.setinfo.sizeLimit = 1048576

1.1.7.

Test Description: Verify Guest Non-Persistent Disks

Test Command: cat guestvmxfile.vmx | grep scsi | grep .mode

Verify values:
Default Value (blank) indicates independant-nonpersistent mode
Blank or "independant-nonpersistent" indicates compliance.

1.1.8.
1.1.9. **Test Description: Guest Unauthorized device connection**

**Test Detail:** Ensure that unauthorized devices are not currently connected to guest VMs

**Test Command:** cat guestvmxfile.vmx | grep .present

**Verify values:** Varies by organization

VM04
floppy0.present = "false"
ide0:0.present = "true"
ethernet0.present = "true"

VM03
floppy0.present = "false"
ide0:0.present = "true"
ethernet0.present = "true"

SRV01
floppy0.present = "true"
ethernet0.present = "true"

FW01
floppy0.present = "true"
ethernet0.present = "true"
ethernet1.present = "true"
ethernet2.present = "true"

1.1.10. **Test Description: Guest Prevent Unauthorized Removal or Connection of Devices**

**Test Command:** For each VM: cat | grep isolation.tools.disable

**Verify Values:** should be set to "true". false or blank indicates non-compliance.

VM04
NONCOMPLIANT
Noncompliant settings (blank line indicates noncompliance):

VM03
NONCOMPLIANT
Noncompliant settings (blank line indicates noncompliance):

Rob VandenBrink. rvandenbrink@metafore.ca
SRV01  
NONCOMPLIANT
Noncompliant settings (blank line indicates noncompliance):
FW01  
NONCOMPLIANT
Noncompliant settings (blank line indicates noncompliance):

1.1.11.

Test Description: Guest Denied Disk Operations D.O.S.

Test Command: cat /vmfs/volumes/4907c9e2-e2e30320-806d-000c29dbab8b9/FW01/FW01.vmx | grep isolation\.tools\.disk
Verify Values: should be set to "true". "false" or blank indicates non-compliance.

VM04  
VM03  
SRV01  
FW01

1.1.12.

Test Description: Verify that Guest OS Matches ESX Configuration

Test Command: cat .vmx | grep guestOS | sort -r
Verify Values: should be the same value as the actual OS of the Guest VM.

VM04  
guestOS = "linux"
guestOSAltName = "Other Linux (32-bit)"
VM03  
guestOS = "linux"
guestOSAltName = "Other Linux (32-bit)"
SRV01  
guestOS = "linux"
guestOSAltName = "Other Linux (32-bit)"
FW01  
guestOS = "linux"
guestOSAltName = "Other Linux (32-bit)"

1.1.13.

Test Description: Guest File Permissions

Rob VandenBrink. rvandenbrink@metafore.ca
Test Command: ls -lh .vmx  
Verify Values: user and group should be root and root  
permissions should be -rwxr-xr-x (755)  

VM04  
-rwxr-xr-x  1 root  root  2.1K Mar 2  2009 /vmfs/volumes/4907c9e2e2e30320-806d-000c29dba8b9/VM04/VM04.vmx  
VM03  
-rwxr-xr-x  1 root  root  2.0K Mar 2  2009 /vmfs/volumes/4907c9e2e2e30320-806d-000c29dba8b9/VM03/VM03.vmx  
SRV01  
-rwxr-xr-x  1 root  root  1.8K Mar 2  2009 /vmfs/volumes/4907c9e2e2e30320-806d-000c29dba8b9/SRV01/SRV01.vmx  
FW01  
-rwxr-xr-x  1 root  root  2.2K Mar 2  2009 /vmfs/volumes/4907c9e2e2e30320-806d-000c29dba8b9/FW01/FW01.vmx  

list VMDK file permissions  
Verify Values: user and group should be root and root  
permissions should be -rw------  

VM04  
VM03  
SRV01  
FW01  

1.2. SERVICE CONSOLE checks  

1.2.1.  

Test Description: Firewall Checks  

Test Command: esxcsfg-firewall -q  
Verify Values: Firewall settings should meet corporate standards  

Chain INPUT (policy DROP 1033 packets, 99877 bytes)  
pkts bytes target prot opt in out source  destination  
316K  218M ACCEPT all -- lo * 0.0.0.0/0 0.0.0.0/0  
66486 5989K valid-tcp-flags tcp -- * * 0.0.0.0/0  
0.0.0.0/0  
66486 5989K valid-source-address !udp -- * * 0.0.0.0/0  
0.0.0.0/0  
1033 99877 valid-source-address-udp udp -- * * 0.0.0.0/0  
0.0.0.0/0  
12 576 valid-source-address tcp -- * * 0.0.0.0/0  
0.0.0.0/0  
0 icmp-in tcp flags:0x16/0x02  
0 0 icmp-in icmp -- * * 0.0.0.0/0 0.0.0.0/0  
66474 5988K ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0  
state RELATED,ESTABLISHED  

Rob VandenBrink. rvandenbrink@metafore.ca
ITDOCS: One Admin’s Documentation is their Hacker’s Pentest

<table>
<thead>
<tr>
<th>Chain</th>
<th>policy</th>
<th>(policy DROP 0 packets, 0 bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FORWARD</td>
<td>DROP</td>
<td>ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:902 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:80 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:443 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>udp spts:67:68 dpts:67:68</td>
</tr>
<tr>
<td></td>
<td></td>
<td>udp dpt:427</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:427 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:5989 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:22 state NEW</td>
</tr>
<tr>
<td>OUTPUT</td>
<td>DROP</td>
<td>ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all -- * lo 0.0.0.0/0 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>icmp-out tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp spts:1024:65535 dpt:53</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:1024:65535 dpt:53</td>
</tr>
<tr>
<td></td>
<td></td>
<td>69644 8959K valid-tcp-flags tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>316K 218M ACCEPT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6408 ACCEPT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>udp -- * * 0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>udp spts:1024:65535 dpt:53</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp spts:1024:65535 dpt:53</td>
</tr>
<tr>
<td></td>
<td></td>
<td>state RELATED,ESTABLISHED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 0 ACCEPT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:902 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:902 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:443 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:902 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:27000 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:27010 state NEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:514</td>
</tr>
<tr>
<td></td>
<td></td>
<td>189 14426 ACCEPT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>udp dpt:514</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:514</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tcp dpt:514</td>
</tr>
</tbody>
</table>

Rob VandenBrink. rvandenbrink@metafore.ca
ITDOCS: One Admin’s Documentation is their Hacker’s Pentest

0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0
tcp dpt:12345
0 0 REJECT all -- * * 0.0.0.0/0 0.0.0.0/0
reject-with icmp-port-unreachable

Chain icmp-in (1 references)

<table>
<thead>
<tr>
<th>pkts</th>
<th>bytes</th>
<th>target prot opt in</th>
<th>out</th>
<th>source</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>DROP all -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Chain icmp-out (1 references)

<table>
<thead>
<tr>
<th>pkts</th>
<th>bytes</th>
<th>target prot opt in</th>
<th>out</th>
<th>source</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>DROP all -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Chain log-and-drop (7 references)

<table>
<thead>
<tr>
<th>pkts</th>
<th>bytes</th>
<th>target prot opt in</th>
<th>out</th>
<th>source</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>LOG all -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOG flags 6 level 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>DROP all -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Chain valid-source-address (2 references)

<table>
<thead>
<tr>
<th>pkts</th>
<th>bytes</th>
<th>target prot opt in</th>
<th>out</th>
<th>source</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>DROP all -- * * 127.0.0.1 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>DROP all -- * * 0.0.0.0/8 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>DROP all -- * * 0.0.0.0/0 255.255.255.255</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Chain valid-source-address-udp (1 references)

<table>
<thead>
<tr>
<th>pkts</th>
<th>bytes</th>
<th>target prot opt in</th>
<th>out</th>
<th>source</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>DROP all -- * * 127.0.0.1 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>DROP all -- * * 0.0.0.0/8 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Chain valid-tcp-flags (2 references)

<table>
<thead>
<tr>
<th>pkts</th>
<th>bytes</th>
<th>target prot opt in</th>
<th>out</th>
<th>source</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>log-and-drop tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp flags:0x3F/0x00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>log-and-drop tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp flags:0x11/0x01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>log-and-drop tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp flags:0x10/0x08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>log-and-drop tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp flags:0x30/0x20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>log-and-drop tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp flags:0x03/0x03</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>log-and-drop tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp flags:0x06/0x06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>log-and-drop tcp -- * * 0.0.0.0/0 0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp flags:0x05/0x05</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Incoming and outgoing ports blocked by default.
Enabled services: CIMSLP ntpClient VCB CIMHttpPostClient vpxHeartbeats LicenseClient sshServer

Opened ports:
- **syslog**: port 514 tcp.out udp.out
- **SEC557Backdoor**: port 12345 tcp.out

1.2.2.

Test Description: Running Service Checks

**Test Command:** `chkconfig --list`

**Verify Values:** Running Services should meet corporate standards

<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdisc</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>gpm</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>vmware-webAccess</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>ntpd</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>kudzu</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>syslog</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>microcode_ctl</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>netsfs</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>network</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>random</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>rawdevices</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>ssdlauthd</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>irqbalance</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>iptables</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>smartd</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>snmpdtrpd</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>sshd</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>portmap</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>nfs</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>nfslock</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>winbind</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>crond</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>xinetd</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>snmpd</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>firewall</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>ym</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>ipmi</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>vmware</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>vmware-vmkauthd</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>vmware-late</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>mptctlnode</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>megaraid_sas_ioclt</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>pegasus</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>wsman</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
<tr>
<td>mgmt-vmware</td>
<td></td>
<td>0:off</td>
<td>1:off</td>
<td>2:off</td>
<td>3:off</td>
<td>4:off</td>
<td>5:off</td>
<td>6:off</td>
</tr>
</tbody>
</table>
vmware-autostart 0:off 1:off 2:off 3:on 4:off 5:off 6:off
vmware-vpxa 0:off 1:off 2:off 3:on 4:off 5:on 6:off

xinetd based services:
  chargen-udp: off
  chargen: off
  daytime-udp: off
  daytime: off
  echo-udp: off
  echo: off
  vmware-authd: on
  services: off
  time: off
  time-udp: off

1.2.3.

Test Description: List Running Processes

Test Command: ps -efw --forest
Verify Values: Check process list for unexpected processes

<table>
<thead>
<tr>
<th>UID</th>
<th>PID</th>
<th>PPID</th>
<th>C</th>
<th>STIME</th>
<th>TTY</th>
<th>TIME</th>
<th>CMD</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:04</td>
<td>init</td>
</tr>
<tr>
<td>root</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[keventd]</td>
</tr>
<tr>
<td>root</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[ksoftirqd/0]</td>
</tr>
<tr>
<td>root</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[bdflush]</td>
</tr>
<tr>
<td>root</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[kswapd]</td>
</tr>
<tr>
<td>root</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:03</td>
<td>[kscand]</td>
</tr>
<tr>
<td>root</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[kupdated]</td>
</tr>
<tr>
<td>root</td>
<td>19</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[vmkmsgd]</td>
</tr>
<tr>
<td>root</td>
<td>20</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[vmnixhbd]</td>
</tr>
<tr>
<td>root</td>
<td>24</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[vmkdevd]</td>
</tr>
<tr>
<td>root</td>
<td>25</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[scsi_eh_0]</td>
</tr>
<tr>
<td>root</td>
<td>558</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[scsi_eh_1]</td>
</tr>
<tr>
<td>root</td>
<td>614</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:20</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>root</td>
<td>701</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>root</td>
<td>1213</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:03</td>
<td>syslogd -m 0</td>
</tr>
<tr>
<td>root</td>
<td>1217</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>klogd -x</td>
</tr>
<tr>
<td>root</td>
<td>1282</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>/usr/sbin/sshd</td>
</tr>
<tr>
<td>root</td>
<td>3327</td>
<td>1282</td>
<td>0</td>
<td>Sep09</td>
<td>?</td>
<td>0:00:15</td>
<td>_ sshd: root@pts/0</td>
</tr>
<tr>
<td>root</td>
<td>3329</td>
<td>3327</td>
<td>0</td>
<td>Sep09</td>
<td>pts/0</td>
<td>0:00:09</td>
<td>_ bash</td>
</tr>
<tr>
<td>root</td>
<td>27202</td>
<td>3329</td>
<td>0</td>
<td>02:11</td>
<td>pts/0</td>
<td>0:00:00</td>
<td>_ /bin/bash /vm9e.sh</td>
</tr>
<tr>
<td>root</td>
<td>27568</td>
<td>27202</td>
<td>0</td>
<td>02:11</td>
<td>pts/0</td>
<td>0:00:00</td>
<td>_ /usr/sbin/sshd --forest</td>
</tr>
<tr>
<td>root</td>
<td>3598</td>
<td>1282</td>
<td>0</td>
<td>Sep09</td>
<td>?</td>
<td>0:00:05</td>
<td>_ sshd: root@pts/1</td>
</tr>
<tr>
<td>root</td>
<td>3600</td>
<td>3598</td>
<td>0</td>
<td>Sep09</td>
<td>pts/1</td>
<td>0:00:05</td>
<td>_ bash</td>
</tr>
<tr>
<td>root</td>
<td>1337</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>/usr/sbin/vmklogger</td>
</tr>
<tr>
<td>root</td>
<td>1381</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:03</td>
<td>xinetd -stayalive -pidfile</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/run/xinetd.pid</td>
</tr>
<tr>
<td>ntp</td>
<td>1396</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:02</td>
<td>ntpd -U ntp -p /var/run/ntpd.pid -g</td>
</tr>
<tr>
<td>root</td>
<td>1405</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>gpm -t imps2 -m /dev/mouse</td>
</tr>
<tr>
<td>root</td>
<td>1426</td>
<td>1</td>
<td>0</td>
<td>Sep08</td>
<td>?</td>
<td>0:00:00</td>
<td>/bin/sh /usr/bin/vmware-watchdog -s webAccess -u 30 -q 5 /usr/lib/vmware/webAccess/j</td>
</tr>
</tbody>
</table>

Rob VandenBrink. rvandenbrink@metafore.ca
ITDOCS: One Admin’s Documentation is their Hacker’s Pentest

Rob VandenBrink, rvandenbrink@metafore.ca

© 2010 The SANS Institute Author retains full rights.
Test Description: Control of SSH Root Privileges

Test Command: `cat /etc/ssh/sshd_config | grep Root`
Verify Values: `PermitRootLogin` should be set to `no`

PermitRootLogin yes

Test Description: Verify that ftp is disabled by port

Test Command: `netstat -na | grep LIST | grep \:21`
Verify Values: Output should be blank

Test Description: Verify that ftp is disabled by configuration

Test Command: `ls -l /etc/xinetd.d | grep ftp`
Verify Values: Output should be blank

Test Description: Verify that root cannot login directly to the console

Test Command: `cat /etc/securetty`
Verify Values: This listing should be empty

Test Results: COMPLIANT
Raw Data:

console
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11

1.2.8.

Test Description

: verify su permissions are restricted
   enumerate members of the wheel group

Test Command: cat /etc/group | grep wheel
Verify Value: root only, or authorized users only

wheel:x:10:root

1.2.9.

Test Description: Verify that only the wheel group members
have access to su

Test Command: cat /etc/pam.d/su | grep auth | grep pam_wheel.so | grep -v \\

Test Results:
COMPLIANT

Raw Data:

Rob VandenBrink. rvandenbrink@metafore.ca
1.2.10.

Test Description
: verify that directory service is used for sudo authentication

Test Command: cat /etc/pam.d/sudo

Verify Value: should read "service=system-auth"

COMPLIANT

Raw Data:

<table>
<thead>
<tr>
<th>Service</th>
<th>Required</th>
<th>Module</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth</td>
<td>required</td>
<td>pam_stack.so</td>
<td>service=system-auth</td>
</tr>
<tr>
<td>account</td>
<td>required</td>
<td>pam_stack.so</td>
<td>service=system-auth</td>
</tr>
<tr>
<td>password</td>
<td>required</td>
<td>pam_stack.so</td>
<td>service=system-auth</td>
</tr>
</tbody>
</table>

1.2.11.

Test Description: verify that password aging is enabled

Test Command: 
cat /etc/passwd | cust -d : -f 1
chage -l

==========
Userid = root
Minimum: 0
Maximum: -1
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

==========
Userid = bin
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

==========
Userid = daemon
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

==========

Rob VandenBrink. rvandenbrink@metafore.ca
Userid = adm
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = lp
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = sync
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = shutdown
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = mail
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Rob VandenBrink. rvandenbrink@metafore.ca
Password Inactive: Never
Account Expires: Never

Userid = news
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = uucp
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = operator
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = gopher
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = ftp
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = nobody
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = nsd
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = vcsa
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = ntp
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = sshd
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = rpc
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

Userid = rpcuser
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

---------------------
Userid = nfsnobody
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

---------------------
Userid = pcap
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

---------------------
Userid = rpm
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

---------------------
Userid = vimuser
Minimum: 0
Maximum: 99999
Warning: 7
Inactive: -1
Last Change: Oct 10, 2008
Password Expires: Never
Password Inactive: Never
Account Expires: Never

---------------------
Userid = vpxuser
Minimum: 0
Maximum: -1
Warning: 7
Inactive: -1
Last Change: May 28, 2009
Password Expires: Never
Password Inactive: Never
1.2.12. **Test Description: Verify Account Lockout**

**Test Command:** cat /etc/pam.d/system-auth | grep pam_tally
**Verify Values:**
- echo for auth required: /lib/security/pam_tally.so no_magic_root
- echo for account required: /lib/security/pam_tally.so deny=3 no_magic_root
No returned value indicates non-compliance

**Noncompliant**

**Raw Data:**

1.2.13. **Test Description: Verify logging of failed logins**

**Test Command:** ls /var/log/faillog | wc -l
**Verify Values:**
- 1 file exists, compliant
- 0 file does not exist, noncompliant

**Compliant**

1.3. **MAINTAINING PROPER LOGGING**

1.3.1. **Test Description: Verify that NTP is running?**

**Test Command:** ps -efw | grep ntpd | wc -l
**Verify Values:**
- 1 = ntpd is running, compliant
- 0 = ntpd is not running, noncompliant

**Compliant**
1.3.2.

**Test Description:** Verify that NTP is associated with a trusted timesource?

**Test Command:** ntpq associations
**Verify Value:** trusted timesource(s) configured
active ntp associations
firewall permissions show ntpClient

ntp.conf server settings:
server 192.168.206.204

ntp/step-tickers server settings:
server 192.168.206.204

Service Startup Settings
ntpd 0:off 1:off 2:on 3:on 4:on 5:on 6:off

Firewall Settings
NTP Associations:

<table>
<thead>
<tr>
<th>remote</th>
<th>refid</th>
<th>st</th>
<th>t</th>
<th>when</th>
<th>poll</th>
<th>reach</th>
<th>delay</th>
<th>offset</th>
<th>jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntp01</td>
<td>0.0.0.0</td>
<td>16</td>
<td>u</td>
<td>-</td>
<td>1024</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
<td>4000.00</td>
</tr>
</tbody>
</table>

1.3.3.

**Test Description:** are local logs being written?

**Test Command:** date ; echo ; ls -lhst /var/log | head -25
**Verify Values:** Compare file date against current date
Compare file dates against current date

Current Date is: Thu Sep 10 02:11:48 EDT 2009

```
total 2.8M
248K -rw------- 1 root root 240K Sep 10 02:11 secure
60K -rw------- 1 root root 53K Sep 10 02:11 messages
32K -rw------- 1 root root 31K Sep 10 02:04 vmkernel
76K -rw------- 1 root root 69K Sep 10 02:01 vmksyslog
4.0K -rw------- 1 root root 2.6K Sep 10 02:01 cron
4.0K -rw------- 1 root root 4.0K Sep 9 23:36 vmware
48K -rw-rw-r-- 1 root utmp 44K Sep 9 21:11 wtmp
28K -r-------- 1 root root 143K Sep 9 13:29 lastlog
0 -rw-r--r-- 1 root root 0 Sep 9 05:01 rpmpkgs
4.0K -rw-r--r-- 1 root root 1.3K Sep 9 04:02 vmksyslog.txt
8.0K -rw-r--r-- 1 root root 7.9K Sep 9 04:02 rpmpkgs.1
4.0K -rw-r--r-- 1 root root 1.7K Sep 9 04:02 vmksyslog.html
8.0K -r-------- 1 root root 7.5K Sep 8 19:59 boot.log
4.0K -rw-r--r-- 1 root root 4.0K Sep 8 19:58 oldconf
76K -rw------- 1 root root 68K Sep 8 19:58 ksymns.0
20K -rw-r--r-- 1 root root 17K Sep 8 19:58 dmesg
```
Test Description:

Verify that log file growth is controlled

Test Command: cat /etc/logrotate.conf

Test Results:

Size limit: size 200k
Filename vmkkernel Compression Check: /var/log/vmkernel{
    create 0600 root root
    missingok
    nocompress
    # keep a history over 3 years.
    monthly
    rotate 36
    # max log size of 200k (thus limiting total disk usage to under 8megs)
    size 200k
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null ||
        true
    endscript
}
Noncompliant
Size limit: size 200k
Filename vmksummary Compression Check: /var/log/vmksummary{
    create 0600 root root
    missingok
    nocompress
    # keep a history over 3 years.
    monthly
    rotate 36
    # max log size of 200k (thus limiting total disk usage to under 8megs)
    size 200k
    olddir /var/log/vmksummary.d
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null ||
        true
    endscript
}
Noncompliant
Size limit: Filename vmkwarning Compression Check: /var/log/vmkwarning{
    create 0600 root root
}
missingok
sharedscripts
postrotate
/bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null ||
true
endscript
}
Noncompliant

1.3.5.

**Test Description: is remote syslog running?**

**Test Command:** cat/etc/syslog.conf | grep @

**Test Verify:** view syslog.conf, verify remote logging (@ symbol)

**Test Results:**

**COMPLIANT**

**Test Raw Output:**

```
*.info;mail.none;authpriv.none;cron.none;local6.none;local5.none
@192.168.206.204
```

1.3.6.

**Test Description: Verify correct permissions on VMware utility file permissions**

**Test Command:** ls -lh /usr/sbin/esxcfg-*

**Verify Value:** all /usr/sbin/esxcfg-* commands are set to -r-x------- (500) except esxcfg-auth which should be -r-xr--r-- (544)

**Test Results:**

esxcfg* permissions - COMPLIANT

**Test Results: - n esxcfg-auth permissions - COMPLIANT**

**Test Raw Data:**

```
-r-x------ 1 root root 48K Aug 12 2008 /usr/sbin/esxcfg-advcfg
-r-xr--r-- 1 root root 26K Aug 12 2008 /usr/sbin/esxcfg-auth
-r-x------ 1 root root 19K Aug 12 2008 /usr/sbin/esxcfg-boot
-r-x------ 1 root root 7.6K Aug 12 2008 /usr/sbin/esxcfg-configcheck
-r-x------ 1 root root 51K Aug 12 2008 /usr/sbin/esxcfg-dumpart
-r-x------ 1 root root 29K Aug 12 2008 /usr/sbin/esxcfg-firewall
-r-x------ 1 root root 2.9K Aug 12 2008 /usr/sbin/esxcfg-hwiscsi
-r-x------ 1 root root 42K Aug 12 2008 /usr/sbin/esxcfg-info
-r-x------ 1 root root 19K Aug 12 2008 /usr/sbin/esxcfg-init
```

Rob VandenBrink. rvandenbrink@metafore.ca
## Test Description: Verify correct file permissions on logs

**Test Commands**
- `ls -lh /var/log`
- `ls -lh /var/log/vmware`
- `ls -lh /var/log`
- `ls -Rlh /vmfs/volumes/`

**Verify Values:**
- all log files have permissions of `-rw-------` (600)
- except: `/var/log/vmware/webAccess/* -rw-r--r--` (755)
- and: Individual Virtual Machine log files `-rw-r---r--` (644)

### Test Results:

#### in /var/log:

**Test Raw Data:**

<table>
<thead>
<tr>
<th>Permissions</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date/Time</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>7.5K</td>
<td>Sep 8 19:59</td>
<td>boot.log</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>24K</td>
<td>Sep 8 15:47</td>
<td>boot.log.1</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>8.2K</td>
<td>Sep 4 14:00</td>
<td>boot.log.2</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>34K</td>
<td>May 27 20:10</td>
<td>boot.log.3</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>16K</td>
<td>Apr 5 00:58</td>
<td>boot.log.4</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>2.6K</td>
<td>Sep 10 02:01</td>
<td>cron</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>846</td>
<td>Sep 8 16:01</td>
<td>cron.1</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>2.0K</td>
<td>Sep 4 14:01</td>
<td>cron.2</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>1.3K</td>
<td>May 27 21:01</td>
<td>cron.3</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>414</td>
<td>Apr 5 01:01</td>
<td>cron.4</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>68K</td>
<td>Sep 8 19:58</td>
<td>ksysms.0</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>68K</td>
<td>Sep 8 15:46</td>
<td>ksysms.1</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>68K</td>
<td>Sep 5 19:37</td>
<td>ksysms.2</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>68K</td>
<td>Sep 4 17:56</td>
<td>ksysms.3</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>68K</td>
<td>Sep 4 13:59</td>
<td>ksysms.4</td>
</tr>
<tr>
<td>-rw---------</td>
<td>root</td>
<td>root</td>
<td>68K</td>
<td>May 27 20:08</td>
<td>ksysms.5</td>
</tr>
</tbody>
</table>
In /var/log/vmware/webAccess:

NONCOMPLIANT

Noncompliant files:
total 12K
-rw-r--r-- 1 root root 0 Oct 28 2008 objectMonitor.log
-rw-r--r-- 1 root root 9.7K Oct 28 2008 proxy.log
-rw-r--r-- 1 root root 0 Sep 8 19:59 timer.log
-rw-r--r-- 1 root root 0 Sep 8 19:59 unitTest.log
-rw-r--r-- 1 root root 0 Oct 28 2008 updateThread.log
-rw-r--r-- 1 root root 0 Oct 28 2008 v1ghthelper.log

Test Raw Data:
total 12K
-rw-r--r-- 1 root root 0 Oct 28 2008 objectMonitor.log
-rw-r--r-- 1 root root 9.7K Oct 28 2008 proxy.log
-rw-r--r-- 1 root root 0 Sep 8 19:59 timer.log
-rw-r--r-- 1 root root 0 Sep 8 19:59 unitTest.log

Rob VandenBrink. rvandenbrink@metafore.ca
Individual VM Logs
NONCOMPLIANT
Noncompliant files:

Test Description: Is root filesystem protected from filling up?

verify that /home, /tmp and /var/log are in 3 separate, non-root partitions
Test Command: vdf -lh
Verification Value: verify a separate entry for each critical partition: /var/log, /home, tmp

Test Results
/var/log partition is **COMPLIANT**
/home partition is **NONCOMPLIANT**
/tmp partition is **NONCOMPLIANT**

**Test Raw Data:**

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Use%</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sda1</td>
<td>2.2G</td>
<td>1.6G</td>
<td>457M</td>
<td>78%</td>
<td>/</td>
</tr>
<tr>
<td>none</td>
<td>124M</td>
<td>0</td>
<td>124M</td>
<td>0%</td>
<td>/dev/shm</td>
</tr>
<tr>
<td>/dev/sda2</td>
<td>496M</td>
<td>8.1M</td>
<td>462M</td>
<td>2%</td>
<td>/var/logs</td>
</tr>
<tr>
<td>/vmfs/devices</td>
<td>11G</td>
<td>0</td>
<td>11G</td>
<td>0%</td>
<td>/vmfs/devices</td>
</tr>
<tr>
<td>/vmfs/volumes/4907c9e2-e2e30320-806d-000c29dba8b9</td>
<td>768M</td>
<td>178M</td>
<td>590M</td>
<td>23%</td>
<td>/vmfs/volumes/LABVMFS</td>
</tr>
<tr>
<td>/vmfs/volumes/4912fc0b-4723c25b-f882-000c29dba8b9</td>
<td>768M</td>
<td>659M</td>
<td>109M</td>
<td>85%</td>
<td>/vmfs/volumes/LABVMFS2</td>
</tr>
</tbody>
</table>
2. Appendix - Windows Scripts

2.1. Master Inventory Script (invent-list.cmd)

The master script is simply a series of calls, one per server, to invent-host.cmd. Invent-host.cmd is the master inventory script for Windows servers.

call inven-host mail.somecompany.com 10.19.1.4
call inven-host dc01.somecompany.com 10.19.1.5
call inven-host finance2.somecompany.com 10.19.1.6
call inven-host dc02.somecompany.com 10.19.1.7
call inven-host auth1.somecompany.com 10.19.1.8

The script calls using both the hostname and ip address. The hostname is used in report titles and the like, the ip address is generally used for host access. This approach is used so that DNS is not required to successfully complete a documentation run.

2.2. Windows Server Detail Inventory Script (invent-host.cmd)

```
set HOST=%1
set IP=%2

if _%2==_ set IP=%1

set DIRNAME=%HOST%

if NOT %HOST%==%IP% set DIRNAME=%HOST%_%IP%

set DOM=somecompany.com
set UID=%DOM%\adminaccount
set PWD=AdminPassword

ping -w 1000 -n 2 %IP% | find "TTL=" || goto HOSTDOWN
net use * /d /y
net use %IP% c$ /user:%UID% %PWD% && goto HOSTOK

:HOSTOK
md %DIRNAME%
rem combine some, add systemenclosure stuff
rem wmic startup list full (malware)
rem printers
wmic /output:%DIRNAME%\patches.htm /user:%UID% /password:%PWD% /node:%IP% qfe list brief /format:htable
wmic /output:%DIRNAME%\os.htm /user:%UID% /password:%PWD% /node:%IP% os list full /format:htable
wmic /output:%DIRNAME%\bios.htm /user:%UID% /password:%PWD% /node:%IP% bios list brief /format:htable
wmic /output:%DIRNAME%\computersystem.htm /user:%UID% /password:%PWD% /node:%IP% computersystem
goto BADCREDS

:HOSTDOWN
```

Rob VandenBrink, rvandenbrink@metafore.ca
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>computersystem list /format:hform</code></td>
<td>Disk partition info</td>
</tr>
<tr>
<td><code>wmi /output:%DIRNAME%partitions.htm /user:%UID% /password:%PWD% /node:%IP% logicaldisk list brief /format:htable</code></td>
<td>Local Groups (Domain groups if target is a DC)</td>
</tr>
<tr>
<td><code>wmi /output:%DIRNAME%sysaccounts.htm /user:%UID% /password:%PWD% /node:%IP% sysaccount list /format:htable</code></td>
<td>System account list</td>
</tr>
<tr>
<td><code>wmi /output:%DIRNAME%shares.htm /user:%UID% /password:%PWD% /node:%IP% share list /format:htable</code></td>
<td>Local shares</td>
</tr>
<tr>
<td><code>wmi /output:%DIRNAME%NICs.htm /user:%UID% /password:%PWD% /node:%IP% nicconfig list /format:htable</code></td>
<td>NIC Configurations</td>
</tr>
<tr>
<td><code>wmi /output:%DIRNAME%ACTIVENICs.htm /user:%UID% /password:%PWD% /node:%IP% nicconfig where IPEnabled='true' /format:htable</code></td>
<td>NIC Configurations of live NICs only</td>
</tr>
<tr>
<td><code>wmi /output:%DIRNAME%products.htm /user:%UID% /password:%PWD% /node:%IP% product get vendor, name, version, installdate, packagecache, description, identifyingnumber /format:htable</code></td>
<td>Installed Program List</td>
</tr>
<tr>
<td><code>wmi /output:%DIRNAME%services.htm /user:%UID% /password:%PWD% /node:%IP% service list /format:htable</code></td>
<td>Windows Services</td>
</tr>
<tr>
<td><code>rem list out share permissions</code></td>
<td>Share permissions (using dumpsec)</td>
</tr>
<tr>
<td><code>rem &quot;c:\program files\systemtools\dumpsec&quot; /computer=%1 /rpt=allsharedirs /outfile=d:\support\www\scripts\win\reports\acls\%1_shares.txt /saveas=fixed</code></td>
<td></td>
</tr>
<tr>
<td><code>rem &quot;c:\program files\systemtools\dumpsec&quot; /computer=%1 /rpt=dir=\%1\c$ /showaudit /outfile=d:\support\www\scripts\win\reports\acls\%1_c.txt /saveas=fixed</code></td>
<td></td>
</tr>
<tr>
<td><code>rem &quot;c:\program files\systemtools\dumpsec&quot; /computer=%1 /rpt=dir=\%1\d$ /showaudit /outfile=d:\support\www\scripts\win\reports\acls\%1_d.txt /saveas=fixed</code></td>
<td></td>
</tr>
<tr>
<td><code>goto ENDEND</code></td>
<td></td>
</tr>
<tr>
<td><code>:HOSTDOWN</code></td>
<td>Maintain an error file for down hosts</td>
</tr>
<tr>
<td><code>date /t &gt;&gt; hosts.err</code></td>
<td></td>
</tr>
<tr>
<td><code>time /t &gt;&gt; hosts.err</code></td>
<td></td>
</tr>
<tr>
<td><code>echo %1 - host down (no icmp echo reply) &gt;&gt; hosts.err</code></td>
<td></td>
</tr>
<tr>
<td><code>goto ENDEND</code></td>
<td></td>
</tr>
<tr>
<td><code>:BADCREDS</code></td>
<td>Also indicate errors for bad credentials</td>
</tr>
<tr>
<td><code>date /t &gt;&gt; hosts.err</code></td>
<td></td>
</tr>
<tr>
<td><code>time /t &gt;&gt; hosts.err</code></td>
<td></td>
</tr>
<tr>
<td><code>echo %1 - bad credentials or no SMB services &gt;&gt; hosts.err</code></td>
<td></td>
</tr>
<tr>
<td><code>goto ENDEND</code></td>
<td></td>
</tr>
</tbody>
</table>
3. Appendix - Novell Scripts

The novell script takes a more monolithic approach – data is collected on the NDS directory in this script. The server-specific calls simply collect the config.nlm output from each server.

3.1. Novell Detail List

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cx /r</code></td>
<td>Go to the root of NDS Tree</td>
</tr>
<tr>
<td><code>rem list NDS tree</code></td>
<td></td>
</tr>
<tr>
<td><code>cx /t /c &gt;report/indstreelist.txt</code></td>
<td>List NDS Tree</td>
</tr>
<tr>
<td><code>rem list objects within NDS tree</code></td>
<td></td>
</tr>
<tr>
<td><code>cx /t/a /c &gt;report/indsoloblist.txt</code></td>
<td>List all objects in nds in tree format</td>
</tr>
<tr>
<td><code>rem list all users, with expire on logins and passwords</code></td>
<td></td>
</tr>
<tr>
<td><code>nlist user=* /s &gt; report/userids.txt</code></td>
<td>List all users</td>
</tr>
<tr>
<td><code>rem list accounts that don't require a password</code></td>
<td></td>
</tr>
<tr>
<td><code>NLIST User = * WHERE &quot;Require a Password&quot; NEXISTS /s &gt; report/userids.nopassword.txt</code></td>
<td>Users who don't require a password.</td>
</tr>
<tr>
<td><code>rem list accounts that haven't logged in for an extended period of time</code></td>
<td></td>
</tr>
<tr>
<td><code>NLIST User = * WHERE &quot;Last Login Time&quot; LT 1/11/2008 /s &gt; report/userids.inactive.txt</code></td>
<td>List inactive accounts</td>
</tr>
<tr>
<td><code>rem list disabled accounts</code></td>
<td></td>
</tr>
<tr>
<td><code>nlist user=* where &quot;Account Disabled&quot; EQ &quot;Yes&quot; /s &gt; report/userids.disabled.txt</code></td>
<td>List disabled accounts</td>
</tr>
<tr>
<td><code>NLIST Organization SHOW &quot;Object Trustees (ACL)&quot; /S /c &gt; report/trustees.o.txt</code></td>
<td>Show object trustees</td>
</tr>
<tr>
<td><code>NLIST &quot;Organizational Unit&quot; SHOW &quot;Object Trustees (ACL)&quot; /S /c &gt; report/trustees.ou.txt</code></td>
<td>Show trustees of organizational units</td>
</tr>
<tr>
<td><code>Rem collect config.txt reports</code></td>
<td></td>
</tr>
<tr>
<td><code>call getconfig fileserver</code></td>
<td>Collect config.txt from each netware server</td>
</tr>
<tr>
<td><code>call getconfig firewall</code></td>
<td></td>
</tr>
<tr>
<td><code>call getconfig webhost</code></td>
<td></td>
</tr>
<tr>
<td><code>call getconfig zendeploy</code></td>
<td></td>
</tr>
<tr>
<td><code>call getconfig zenmaster</code></td>
<td></td>
</tr>
<tr>
<td><code>rem show volumes (used by other scripts)</code></td>
<td></td>
</tr>
<tr>
<td><code>rem nlist volume /s /c &gt; volumes.txt</code></td>
<td>Volume list (disabled, it's in the config.txt output)</td>
</tr>
<tr>
<td><code>rem show groups and group members</code></td>
<td></td>
</tr>
<tr>
<td><code>nlist group show MEMBER /c/s &gt; report/grouplist.txt</code></td>
<td>Group member list</td>
</tr>
<tr>
<td><code>rem volume reports</code></td>
<td></td>
</tr>
<tr>
<td><code>call vol1</code></td>
<td></td>
</tr>
</tbody>
</table>
3.2. Getconfig.cmd

This script collects config.txt files from Netware Servers.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>net use r: /d</td>
<td>Remove any existing drive map</td>
</tr>
<tr>
<td>net use r: %1.sys</td>
<td>Map the drive</td>
</tr>
<tr>
<td>xcopy r:\system\config.txt %1_config.txt /y</td>
<td></td>
</tr>
<tr>
<td>call txt2html fileserver_volumes &quot;Server FILESERVER - Volume ACL Report&quot;</td>
<td>Change all TXT files to HTML</td>
</tr>
<tr>
<td>call txt2html fileserver_config &quot;Server FILESERVER - CONFIG.NLM Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html firewall_config &quot;Server FIREWALL - CONFIG.NLM Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html FIREWALL_volumes &quot;Server FIREWALL - Volume ACL Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html grouplist &quot;NDS Group Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html WEBHOST_volumes &quot;Server WEBHOST - Volume ACL Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html ndsobjlist &quot;NDS Object ACL Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html WEBHOST_config &quot;Server WEBHOST - CONFIG.NLM ACL Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html ndstreenlist &quot;DNS Tree Listing&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html trustees.o &quot;NDS Object Trustee Assignments&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html trustees.ou &quot;NDS OU Trustee Assignments&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html userids.disabled &quot;NDS - Disabled Accounts Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html userids.inactive &quot;NDS - Inactive Accounts Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html userids.nopassword &quot;NDS - Accounts with no Password Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html userids &quot;NDS - USERID Detail Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html zendeploy_config &quot;Server ZENDEPLOY - CONFIG.NLM Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html ZENDEPLOY_volumes &quot;Server ZENDEPLOY - Volume ACL Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html zensmaster_config &quot;Server ZENMASTER - CONFIG.NLM Report&quot;</td>
<td></td>
</tr>
<tr>
<td>call txt2html ZENMASTER_volumes &quot;Server ZENMASTER - Volume ACL Report&quot;</td>
<td></td>
</tr>
</tbody>
</table>
3.3. Convert Text Data to HTML

This script relies heavily on sed. First the sed file is created, then it is called:

```
sed s/"Insert Title Here"%/2/g dst2html.sed >work1.sed
sed -f work1.sed report\%1.txt >report\%1.html
```

<table>
<thead>
<tr>
<th>sed s/&quot;Insert Title Here&quot;%/2/g dst2html.sed &gt;work1.sed</th>
<th>Take the sed skeleton file and update the Title text</th>
</tr>
</thead>
<tbody>
<tr>
<td>sed -f work1.sed report%1.txt &gt;report%1.html</td>
<td>Now run the SED using the input file and resulting SED file</td>
</tr>
</tbody>
</table>

3.4. An example WORK1.SED file

```
s/&/</g
s/&>/</g

1 i
<head>
<title>
Server FILESERVER - CONFIG.NLM Report
<title>
<head>
<body>
2 p<font size="4">Server FILESERVER - CONFIG.NLM Report</font>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p><font face="monospace">$ a</font></p>
</pre>
$ a
</html>
```

Rob VandenBrink. rvandenbrink@metafore.ca
4. Appendix - Front-end Web Page

As mentioned, all IT-DOCS reports are front-ended with a simple website. At the client’s request, the main page matches the customer rack layout, and server hyperlinks are made off the network and rack diagrams.

UPS PDU documentation is currently manual, it will be automated using data collection via telnet and/or ssh (depending on the PDU) in a future version.

The “Directories” hyperlink has sub-pages for Active Directory and NDS. The Firewall, Switch Topology and VLAN pages are diagrams with further links.
# Upcoming SANS Penetration Testing

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mentor Session - SEC504</td>
<td>Des Moines, IA</td>
<td>Jun 24, 2019 - Jul 24, 2019</td>
<td>Mentor</td>
</tr>
<tr>
<td>SANS Munich July 2019</td>
<td>Munich, Germany</td>
<td>Jul 01, 2019 - Jul 06, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defence Japan 2019</td>
<td>Tokyo, Japan</td>
<td>Jul 01, 2019 - Jul 13, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Madison SEC504</td>
<td>Madison, WI</td>
<td>Jul 08, 2019 - Jul 13, 2019</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Pittsburgh 2019</td>
<td>Pittsburgh, PA</td>
<td>Jul 08, 2019 - Jul 13, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rocky Mountain 2019</td>
<td>Denver, CO</td>
<td>Jul 15, 2019 - Jul 20, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Summer 2019</td>
<td>Boston, MA</td>
<td>Jul 29, 2019 - Aug 03, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>Mentor Session - SEC504</td>
<td>Oklahoma City, OK</td>
<td>Aug 03, 2019 - Aug 31, 2019</td>
<td>Mentor</td>
</tr>
<tr>
<td>SANS Prague August 2019</td>
<td>Prague, Czech Republic</td>
<td>Aug 12, 2019 - Aug 19, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Minneapolis 2019</td>
<td>Minneapolis, MN</td>
<td>Aug 12, 2019 - Aug 17, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2019</td>
<td>Virginia Beach, VA</td>
<td>Aug 19, 2019 - Aug 30, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam August 2019</td>
<td>Amsterdam, Netherlands</td>
<td>Aug 19, 2019 - Aug 24, 2019</td>
<td>Live Event</td>
</tr>
</tbody>
</table>