Vulnerability analysis

License

Contents

General notes about the labs

Often the lab instructions are intentionally open ended, and you will have to figure some things out for yourselves. This module is designed to be challenging, as well as fun!

However, we aim to provide a well planned and fluent experience. If you notice any mistakes in the lab instructions or you feel some important information is missing, please feel free to add a comment to the document by highlighting the text and click the comment icon (▤), and I (Cliffe) will try to address any issues. Note that your comments are public.

If you notice others are also reading the lab document, you can click the chat icon (💬) to discuss the lab with each other.

Preparation

As with all of the labs in this module, start by loading the latest version of the LinuxZ template from the IMS system. If you have access to this lab sheet, you can read ahead while you wait for the image to load.

> To load the image: press F12 during startup (on the blue boot screen) to access the IMS system, then login to IMS using your university password. Load the template image: LinuxZ.

Once your LinuxZ image has loaded, log in using the username and password allocated to you by your tutor.

The root password -- **which should NOT be used to log in graphically** -- is "tiaspbiqe2r" (**t**his **i**s **a** **s**ecure **p**assword **b**ut **i**s **q**uite **e**asy **2** **r**emember). Again, never log in to the desktop environment using the root account -- that is bad practice, and should always be avoided.

Using the VM download script (as described in the previous lab), download and **start** these VMs:

- Kali Linux - with Armitage and Nessus (Bridged and Host Only)
- Vulnerable Win2K server (Host Only)
- Metasploitable (Host Only)

Feel free to read ahead while the VMs are downloading.

Note the IP address of the Kali Linux system, using "ifconfig". Ensure that the VMs are networked as indicated above: that is, all share a "host only" network, and the Kali Linux VM also has a "bridged" network.

Introduction to vulnerability scanning and analysis

Identifying vulnerabilities via ethical hacking and penetration testing requires careful research and planning, and testing the exploits against vulnerabilities typically results in a compromise of the remote system. The advantage of a penetration test (hiring ethical hackers to test security by hacking) is that there are very few false positives (that is, vulnerabilities “discovered” that are false alarms), since the security tester can actually attempt exploits and report whether they were successful.

However, there is always a risk that an exploit may cause unintentional damage, or that the ethical hacker will miss something obvious when they are checking things manually.

An alternative, shallower and automated approach, is to use *vulnerability scanning* (also known as vulnerability analysis or vulnerability assessment). Vulnerability scanners typically start by performing (or importing) network scans such as port scans and service identification, then automatically checks whether each of the identified services are known to contain vulnerabilities.

The way the security tests are conducted are often simply by comparing the service version that has been detected with the versions known to have vulnerabilities (similar to what you did manually using Security Focus). Vulnerability scanners will often also probe the software further to confirm that the system really does appear to be vulnerable. Some probes can potentially cause crashes, so a safe-mode is typically offered to avoid the more dangerous checks.

There are lots of different vulnerability scanners on the market, many of which are extremely expensive for commercial use (although arguably a necessity for efficient security testing). No-cost evaluation versions are often available for home use.

Nmap scripting engine (NSE) and advanced scanning

The Nmap scanner has a powerful feature known as the Nmap scripting engine (NSE). In addition to the scanning features that are built into Nmap, Nmap can be extended with scripts that add other capabilities. Nmap is distributed with a number of scripts (developed by various people), and these add more types of version detection and even does some vulnerability detection.

On the host OS (LinuxZ):

Enable VMware player VMs to put the NIC into promiscuous mode... From the host OS (the LinuxZ image) run the following in a console (such as Konsole from KDEMenu → System → Terminal → Konsole):

```
sudo chmod a+rw /dev/vmnet*
```

On the Kali Linux (security tester) VM:

Look at the list of files contained in:

/usr/share/nmap/scripts/

For example, “`ls /usr/share/nmap/scripts/`”, or browse using a file browser, such as Dolphin.

View the contents of “http-iis-webdav-vuln.nse”. Hint: consider using vi.

This script is written in the Lua programming language, and it checks for a specific WebDav vulnerability.

Open the Nmap man page, and read the description under the heading “NMAP SCRIPTING ENGINE (NSE)”. Note that “*-sC Performs a script scan using the default set of scripts. [...] Some of the scripts in this category are considered intrusive and should not be run against a target network without permission.*"

Launch an Nmap scan using the default set of scripts (where IP address is the Metaploitable VM):

```
nmap -sC IP-address
```

Launch an Nmap scan using vulnerability scanning scripts (where IP address is the Metaploitable VM):

```
nmap --script vuln IP-address
```

Note this can take a long time to complete (roughly 10 minutes); you may wish to leave this running and *continue on with other tasks while it runs*.

When this completes read through the output. What vulnerabilities did it detect?

Nmap scripts have a lot of potential; however, the current set of scripts only check for a limited number of vulnerabilities.

Based on what you have learned:

1. Use the man page to answer: what does the -A Nmap flag do?

Run an Nmap vulnerability scan against the Win2k server VM.

Extra challenge: exploit a vulnerability detected by the Nmap script scan.

Nessus

Nessus, by Tenable Network Security, is one of the most popular commercial vulnerability scanners. Vulnerability tests are written using NASL (the Nessus Attack Scripting Language), and subscriptions to “feeds” of vulnerability checks are available. The “HomeFeed” is available for noncommercial home and educational use for no cost, while the “ProfessionalFeed” receives updates sooner and can be used in commercial settings.

Nessus is based on a client/server architecture, where a client (such as the web interface) connects to the server, which does the scanning. Results can be imported into Metasploit.

In addition to vulnerability scanning, Nessus can be used for compliance checks (such as checking the security policies on networked systems by giving Nessus credentials to manage them).

Open a terminal, and run:

```
service nessusd start
```

Start Iceweasel, and visit:

https://localhost:8834

Confirm the security exception. (“I Understand the Risks”, “Add Exception”.) The warning is shown because the site is secured using a self-signed certificate.

Login with username: “nessusadmin”, password: “toor”.

Note that there are various scanning profiles available, and depending on your selection Nessus will check the target(s) for different types of security issues.

Click on “Policies”, and review the various scan types that are preconfigured. Click on “External Network Scan”, and browse the Plugins that are enabled for this profile.

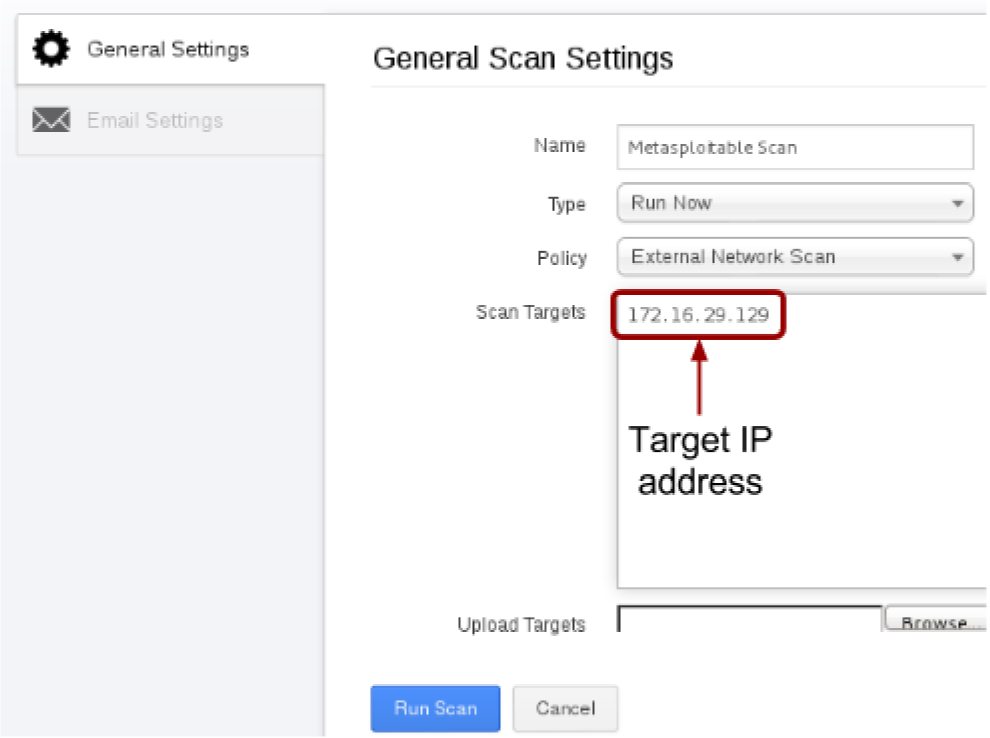
Lets use Nessus to scan Metasploitable for vulnerabilities:

Click “Scan Queue”.

The Nessus Scan Queue

Click “New Scan”.

Configure a scan, by entering a name for the scan, such as “Metasploitable Scan”, and enter the IP address of the system you wish to perform a vulnerability scan of. In this case the IP address of the Metasploitable VM. Note that you could instead enter an IP address range.



General Scan Settings

Name: Metasploitable Scan

Type: Run Now

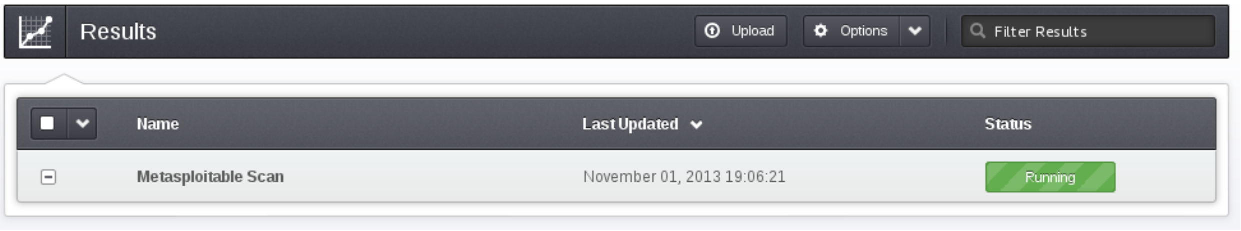
Policy: External Network Scan

Scan Targets: 172.16.29.129

Adding and starting a new scan

Click “Run Scan”, to run a vulnerability scan against the Metasploitable target VM.

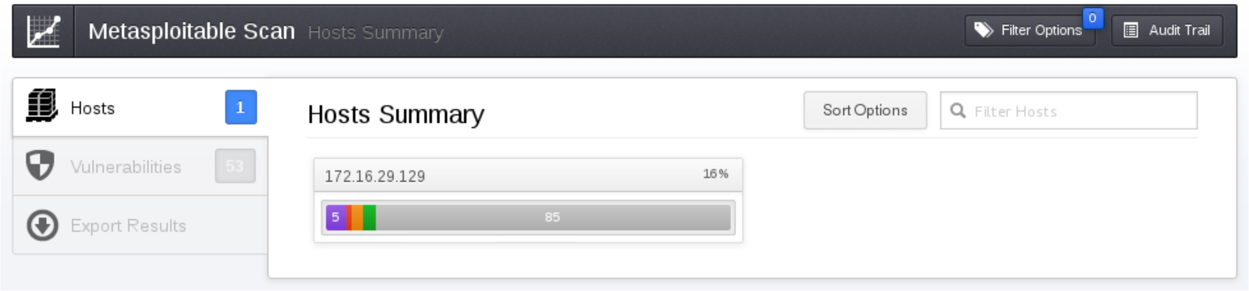
Click “Results”. You will see that the vulnerability analysis scan is currently running.



Name	Last Updated	Status
Metasploitable Scan	November 01, 2013 19:06:21	Running

Nessus scan in progress

Click the ongoing scan (in this case “Metasploitable Scan”), and view the progress. The Nessus scan is quite detailed, and will take some time to complete.



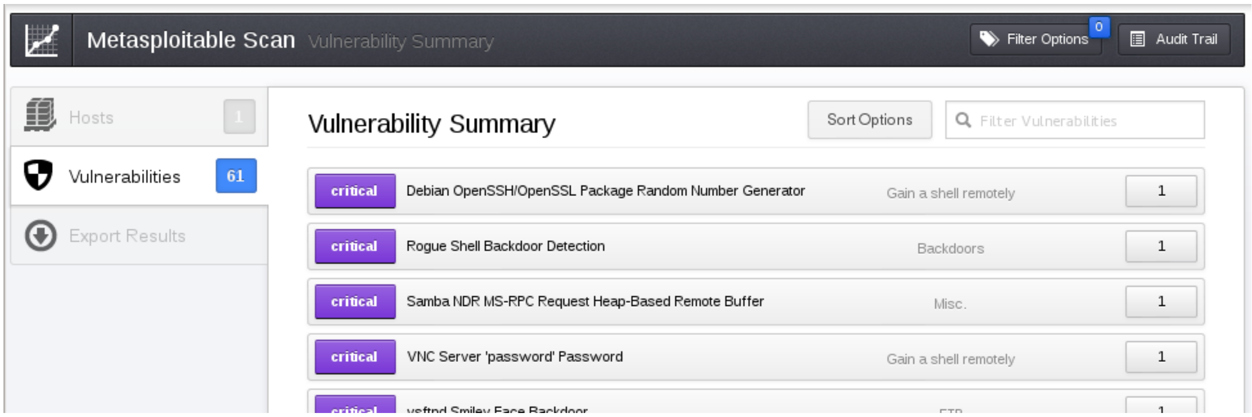
Hosts Summary

172.16.29.129 16%

5 85

Nessus scan in progress, some vulnerabilities

Click “Vulnerabilities”, to view the security vulnerabilities that have been detected.

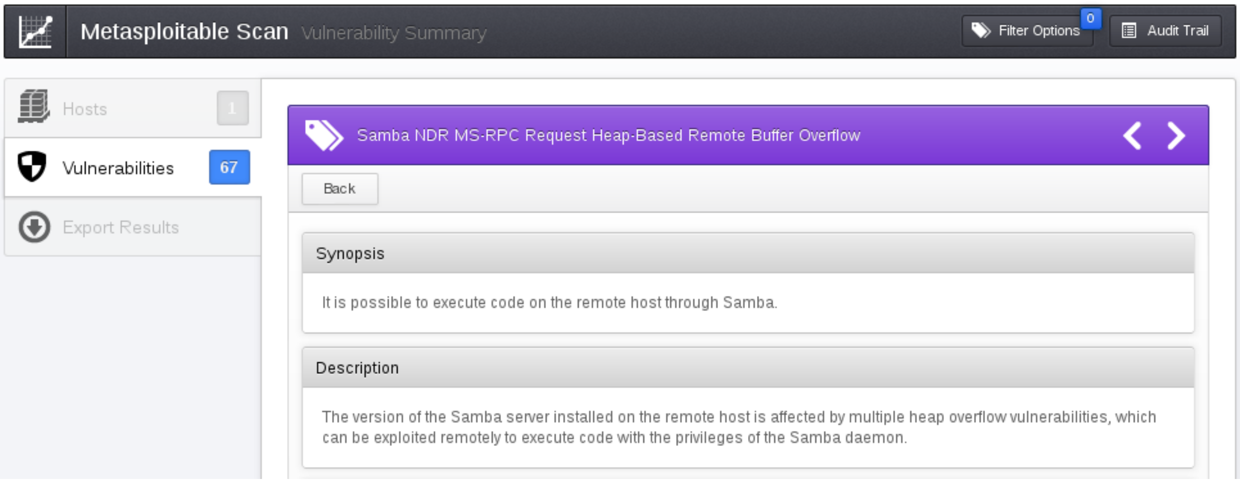


Vulnerability Summary

critical	Debian OpenSSH/OpenSSL Package Random Number Generator	Gain a shell remotely	1
critical	Rogue Shell Backdoor Detection	Backdoors	1
critical	Samba NDR MS-RPC Request Heap-Based Remote Buffer	Misc.	1
critical	VNC Server 'password' Password	Gain a shell remotely	1
critical	vsftpd Smiley Face Backdoor	FTP	1

Browsing the detected vulnerabilities

Browse through the list of detected vulnerabilities (if there are not any yet, just wait a while), and click on one of the issues to view more detailed information.



Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow

Synopsis

It is possible to execute code on the remote host through Samba.

Description

The version of the Samba server installed on the remote host is affected by multiple heap overflow vulnerabilities, which can be exploited remotely to execute code with the privileges of the Samba daemon.

Vulnerability details

Read through the information for the vulnerability and answer the following:

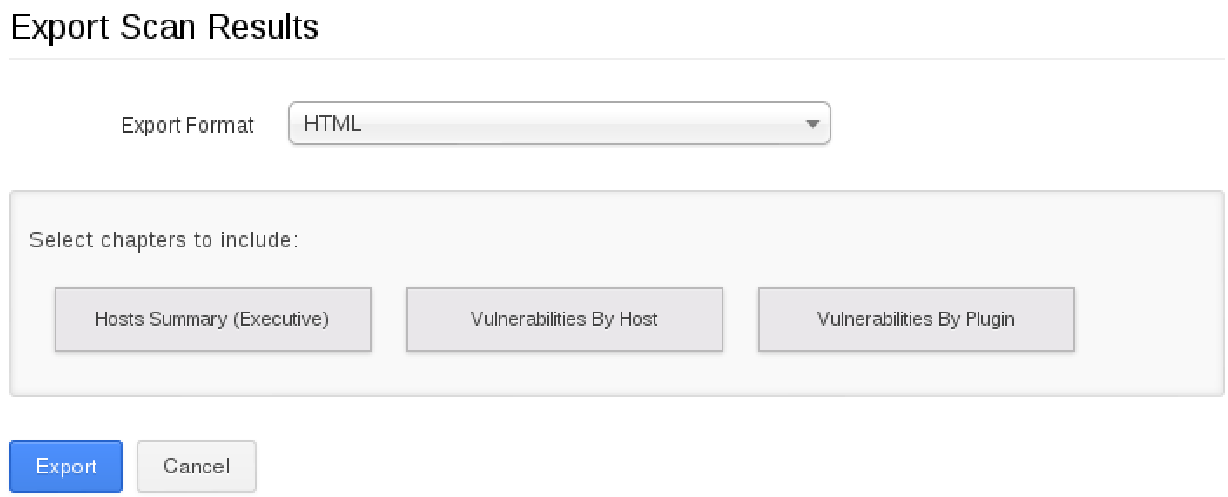
- What is the CVE for this vulnerability?
- Are exploits available? What kind? (Stand alone, MSF, etc)
- What would be the likely result of an attack on this vulnerability?
- How would you fix this issue?

Once the scan is complete:

How many vulnerabilities did it detect?

- How many of the vulnerabilities did you miss when you have previously scanned these systems using Nmap, MSF, and Armitage?
- How many vulnerabilities that were detected are “critical”, “high”, and so on? (Make a note of the number of vulnerabilities)

Click “Export Results”, and generate various HTML reports. View the output of these reports.



Export Scan Results

Export Format: HTML

Select chapters to include:

Generating Nessus reports

What information from these reports do you think a you would use:

- During a penetration test?
- When writing a report for the management of a company that hired you to test their systems?

- When writing a report for the IT department of the company?

Extra challenge: save and import the results into MSF.

Exploit a vulnerability detected by the Nessus vulnerability scan, to confirm the system is vulnerable.

OPTIONAL TASK: run a scan against the Win2k VM.

OpenVAS

Nessus was originally free and open source software (FOSS); however, in 2005 they closed the source code and removed the permission to use the software for commercial use without a paying for a license. In response to this, the community forked the last version of Nessus that had been released as FOSS, and started the OpenVAS (Open Vulnerability Assessment System) project, a free product. Due to a smaller developer team, OpenVAS's database of vulnerability checks may be less complete. As with Nessus, results can be imported into Metasploit.

OPTIONAL TASK: Comparison with OpenVAS

Note that using OpenVAS on Kail Linux may involve some troubleshooting to get it working. Consider this an open-ended optional task. If you identify any steps that are missing, please leave a comment.

Setup OpenVAS on Kali Linux:

If you are in the Leeds Met IMS labs, run:

```
export http_proxy=192.168.208.51:3128
```

```
openvas-setup
```

This will take quite some time, to download and install all the plugins.

Note that the default account is named "admin", and you will set a password while the above runs.

Once the install is complete:

```
openvas-start
```

Open another Iceweasel tab, and visit:

https://localhost:9392

Confirm the security exception.

Login with username: “admin”, password: (as you have configured it).

Run a vulnerability scan against the Metasploitable target VM, using the most complete scanning profile that you think is appropriate.

> Tip: if you need a guide, try this tutorial.

How many critical vulnerabilities did it detect? How does this compare with the earlier Nessus scan? What are the differences?

Retina Network Security Scanner

Retina, was developed by eEye Digital Security and acquired by BeyondTrust, and is similar in purpose to Nessus. It scans a network or host, and produces a report on the vulnerabilities it discovers. Includes some integration with Metasploit.

OPTIONAL TASK: download a trial version, install, setup, and run Retina Network Security Scanner. Run a vulnerability scan against the Metasploitable target VM, using the most complete scanning profile that you think is appropriate.

> How many critical vulnerabilities did it detect? How does this compare with the earlier scans? What are the differences?

NeXpose

NeXpose is developed by Rapid7, who also now manage the Metasploit project. Again, the purpose of NeXpose is similar to the above, although due to the relationship, there is extensive integration with Metasploit to pen-test detected vulnerabilities.

OPTIONAL TASK: download a trial version, install, setup, and run NeXpose. Run a vulnerability scan against the Metasploitable target VM, using the most complete scanning profile that you think is appropriate.

> How many critical vulnerabilities did it detect? How does this compare with the earlier scans? What are the differences?

Web vulnerability analysis

In addition to tests to look for vulnerable software running as remote services (and compliance checks regarding client system configuration), security testers often have to test the security of web servers. While the above vulnerability scanners will do some testing of web servers that are detected, there are also a number of vulnerability scanners that exclusively scan web servers for software and misconfiguration vulnerabilities.

Nikto is a command line web vulnerability scanner. Nikto scans for over 6000 security issues, such as dangerous CGI scripts and permissions.

Use Nikto to scan the Metasploitable VM, then the Win2k VM.

```
nikto -host Target-IP-Address
```

Take some time to read and understand the output.

- How many critical vulnerabilities did Nikto detect?
- Did it detect any that the above scanners missed?

Based on one of the detected vulnerabilities:

- Can you identify the CVE for the vulnerability?
- How could you exploit this vulnerability? (With what attack software/exploit?)
- What would be the likely result of an attack on this vulnerability?
- How would you fix this issue?

Exploit a vulnerability detected by the Nikto vulnerability scan, to confirm the system is vulnerable.

Conclusion

At this point you have:

- Learned about vulnerability assessment
- Run vulnerability scans using various industry standard tools, including Nessus and Nikto
- Understood that different tools will detect different security issues, and that it is important to consider which tests (and scan profiles) to run

Well done.