Chapter 06
Finding Vulnerabilities

1

Outline

- From Nmap Version Scan to Potential Vulnerability
- Nessus
- The Nmap Scripting Engine
- Running a Single NSE Script
- Metasploit Scanner Modules
- Metasploit Exploit Check Functions
- Web Application Scanning
- Manual Analysis

2

2

From Nmap Version Scan to Potential Vulnerability

- Intelligence Gathering about our target and the attack surface → Now we can develop scenarios to reach our pentest goals

3

3

Tenable Security's Nessus

- One of the most widely used commercial vulnerability scanners
- Nessus database includes vulnerabilities across platforms and protocols, and its scanner performs a series of checks to detect known issues
- # service nessusd start
- https://localhost:8834 (the Nessus web interface on TCP port)

- Get your Activation Code at:
  - http://www.tenable.com/products/nessus-home/

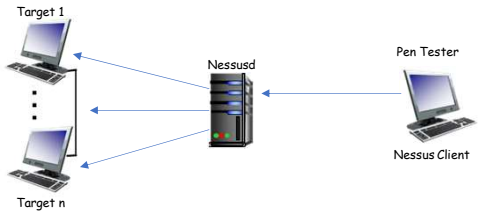
Nessus® vulnerability scanner

4

4

Nessus Architecture

- Nessus is a client server architecture
- Client: browser based. Used to configure and manage things
- Server: nessusd. It is used to perform the scan
- Client and nessud often run on the same machine
- Can run on Windows, Linux and macOS



5

5

Nessus Plugins

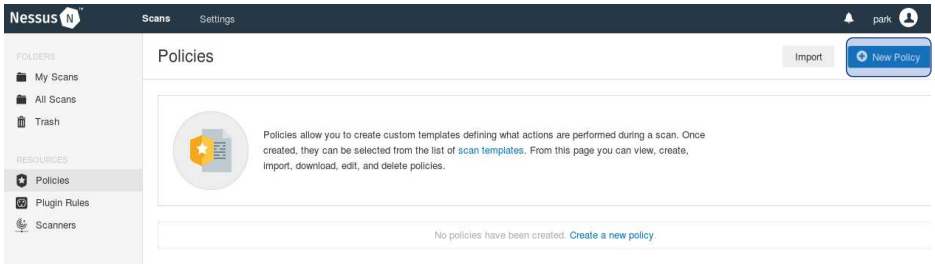
- Plugins are small programs that tell the scanning engine what to measure for each individual security issue on a target
- More than 181,537 plugins
- Nessus auto update plugins every 24 hours
- Update Nessus plugins at the start of the project
  - # sudo /opt/nessus/sbin/nessuscli update --plugins-only
- Record which plugins you used for scan
- Make a note of the particular plugin configuration (scan policy) you use for the test **so that your results will be repeatable**.
- By default, Nessus does not run dangerous plugins

6

6

Nessus – Policies

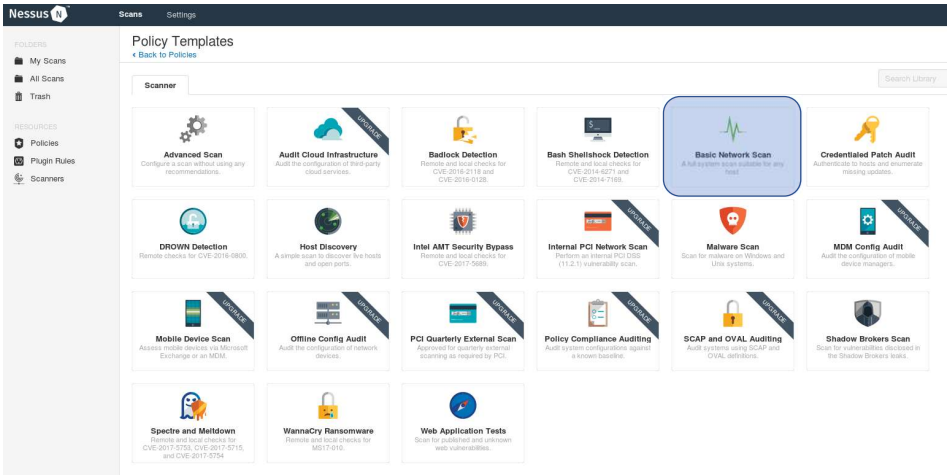
- Nessus policies are like configuration files that tell Nessus which vulnerability checks, port scanners, and so on to run in the vulnerability scan



7

7

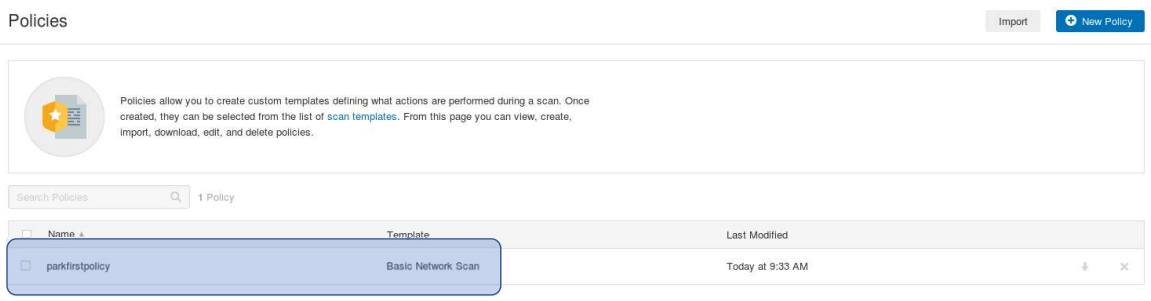
Nessus - Policies



8

8

Nessus – Policies

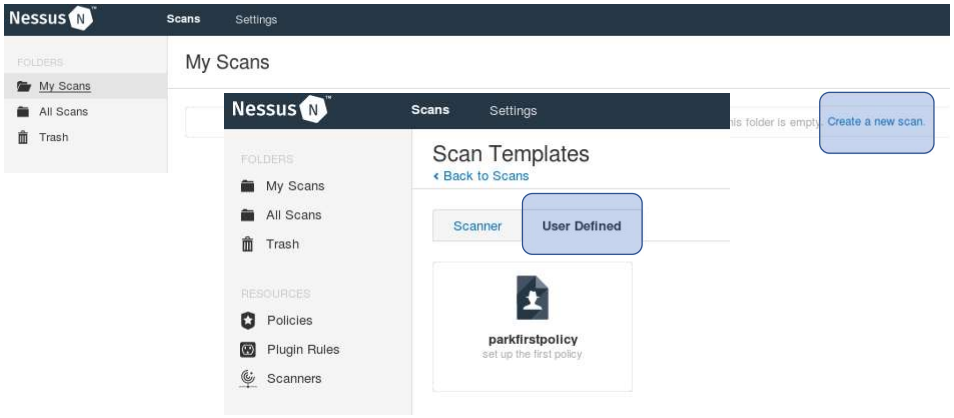


9

9

Scanning with Nessus

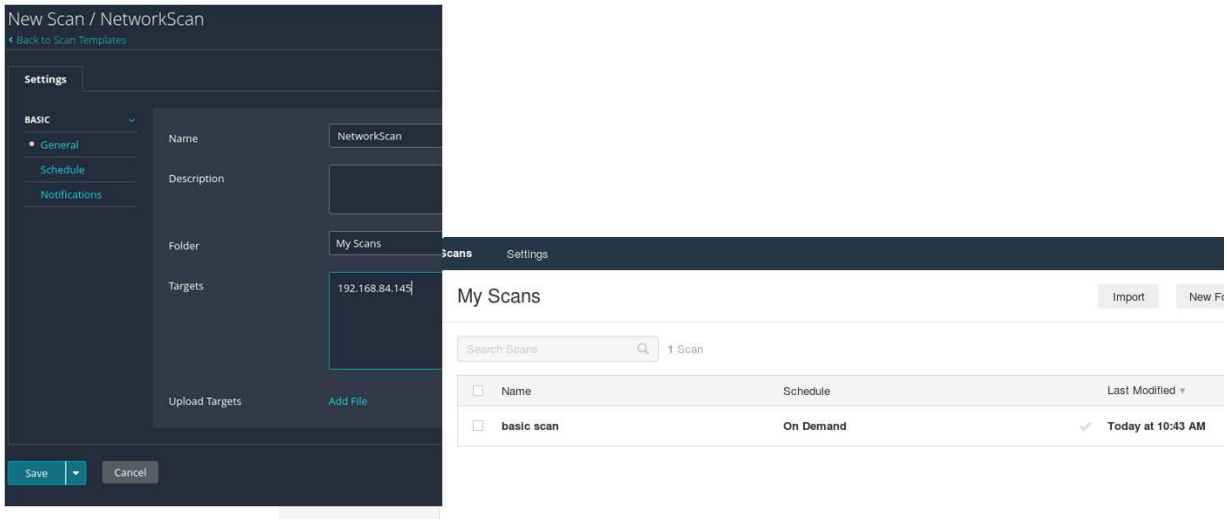
- Let's run Nessus against our target machines



10

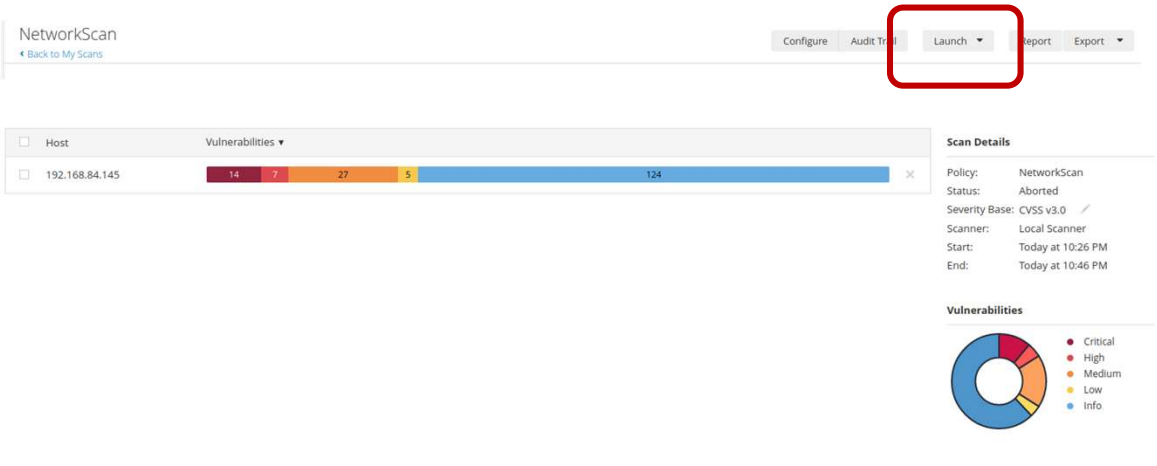
10

Scanning with Nessus



11

Scanning with Nessus



12

12

Scanning with Nessus

Nessus | Scans | Settings | park

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Scanners

SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

See Also

https://technet.microsoft.com/library/security/MS17-010
http://www.nessus.org/u?321523eb
http://www.nessus.org/u?7bec1941
http://www.nessus.org/u?d9f569cf
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
https://support.microsoft.com/en-us/kb/2696547
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?36fd3072
http://www.nessus.org/u?4c7e0cf3
https://github.com/stamparm/EternalRocks/
http://www.nessus.org/u?59db5b5b

Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: March 14, 2017
Vulnerability Pub Date: March 14, 2017
In the news: true

Exploitable With

Metasploit (MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption)
Core Impact

Reference Information

EDB-ID: 41891, 41987
MSFT: MS17-010
BID: 96703, 96704, 96705, 96706, 96707, 96709

13

13

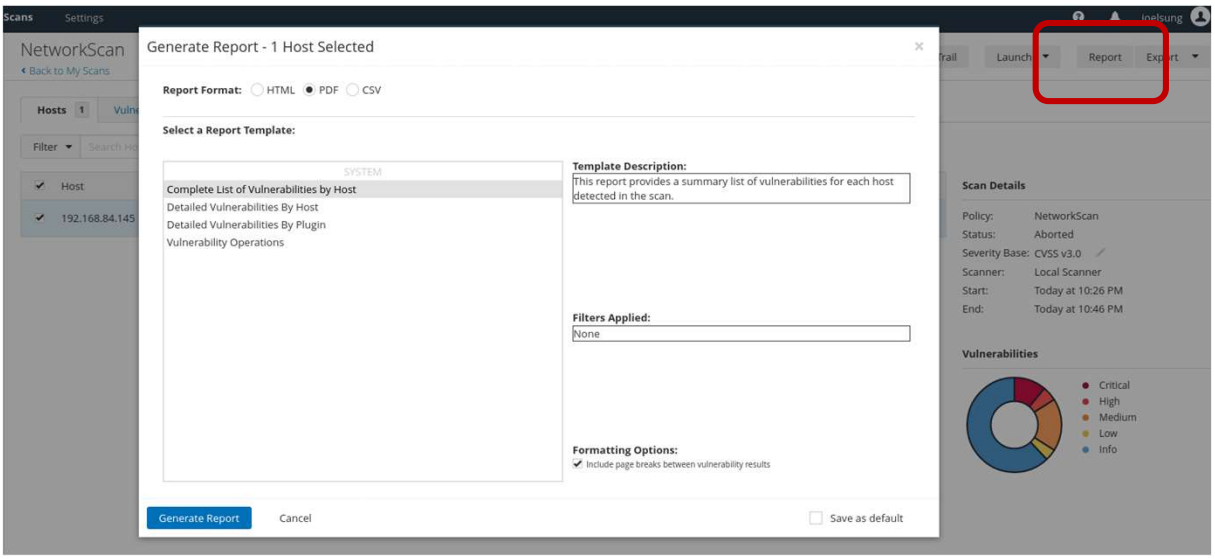
Nessus Rankings

- Nessus ranks vulnerabilities based on the **Common Vulnerability Scoring System (CVSS) version 3**, from the National Institute of Standards and Technology (NIST)
- Ranking is calculated based on the impact to the system if the issue is exploited
- **The actual risk of a vulnerability depends on the environment**

14

14

Exporting Nessus Results



15

Other Commercial Vulnerability Scanning Tools

- Nexpose by Rapid 7 https://www.rapid7.com/products/nexpose/
- Saint, http://www.saintcorporation.com/
- Retina, https://www.beyondtrust.com/resources/brochures/retina-network-security-scanner
- Acunetix, specialized in Web vulnerability scanning, https://www.acunetix.com/
- Qualys, a scanning service, https://www.qualys.com/

16

16

Methods for Discovering Vulnerabilities

- Check software version number
  - Red Hat Enterprise Linux (RHEL) often keeps old version number when a patch is released
- Check protocol version number
- Look at its behavior
- Check its configuration
  - Authenticated vulnerability scan
- Run exploit against it
  - Help reduce false positive but it doesn't help us manage false negative
- Not all vulnerabilities lead to exploit

17

17

Researching Vulnerabilities

- Security Focus
  - http://www.securityfocus.com/
- Packet Storm
  - http://www.packetstormsecurity.org/
- Exploit Database
  - http://www.exploit-db.org
- Common Vulnerabilities and Exposures
  - http://www.cve.mitre.org
- Open Sourced Vulnerability Database (OSVDB)
  - http://osvdb.com
- US-CERT
  - www.us-cert.gov/cas/techalerts
- HackerStorm
  - www.hackerstorm.co.uk

18

18

Nmap Scripting Engine (NSE)

- From Caterpillar to Butterfly …
  - **NSE** provides entirely new skill set and dimension to **Nmap**
  - Vulnerability scanning, advanced network discovery, detection of backdoor, and even exploitation become possible in Nmap
  - https://nmap.org/nsedoc/scripts/
  - NSE and its scripts are prebuilt into Nmap
  - **root@kali:~#** nmap --script banner 10.0.2.5

19

NSE examples: banner

- Banner script
  - https://nmap.org/nsedoc/scripts/banner.html
  - A simple banner grabber which connects to an open TCP port and prints out anything sent by the listening service **within five seconds**

```
root@kali:~# nmap -sV --script=banner 10.0.2.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-27 15:27 EST
Nmap scan report for 10.0.2.5
Host is up (0.00014s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_banner: 220 (vsFTPd 2.3.4)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp   open  telnet      Linux telnetd
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
25/tcp   open  smtp        Postfix smtpd
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

20

Nmap at Defcon 2010

- Defcon 18 - Mastering the Nmap Scripting Engine
  - https://www.youtube.com/watch?v=M-Uq7YSfZ4I
  - (00:00~04:00) + (9:55~10:30) + (11:40~16:00) + (28:00~36:00)

21

The Nmap Scripting Engine

- Let you run publicly available scripts and write your own
- Extremely useful for scanning for and measuring a relative small number of specific items across a large number of target systems
- Categories of the available scripts
  - # gedit /usr/share/nmap/scripts/script.db
- Search for script in a specific category
  - # grep safe /usr/share/nmap/scripts/script.db
- Count the number of scripts in a specific category
  - # cat /usr/share/nmap/scripts/script.db | grep discovery | wc -l

22

22

The Nmap Scripting Engine

Open | script.db /usr/share/nmap/scripts | Save

```
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-methods.nse", categories = { "default", "safe", } }
Entry { filename = "ajp-request.nse", categories = { "discovery", "safe", } }
Entry { filename = "allseeingeye-info.nse", categories = { "discovery", "safe", "version", } }
Entry { filename = "amqp-info.nse", categories = { "default", "discovery", "safe", "version", } }
Entry { filename = "asn-query.nse", categories = { "discovery", "external", "safe", } }
Entry { filename = "auth-owners.nse", categories = { "default", "safe", } }
Entry { filename = "auth-spoof.nse", categories = { "malware", "safe", } }
Entry { filename = "backorifice-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "backorifice-info.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "bacnet-info.nse", categories = { "discovery", "version", } }
Entry { filename = "banner.nse", categories = { "discovery", "safe", } }
Entry { filename = "bitcoin-getaddr.nse", categories = { "discovery", "safe", } }
Entry { filename = "bitcoin-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "bitcoinrpc-info.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "bittorrent-discovery.nse", categories = { "discovery", "safe", } }
Entry { filename = "bjnp-discover.nse", categories = { "discovery", "safe", } }
Entry { filename = "broadcast-ataoe-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-avahi-dos.nse", categories = { "broadcast", "dos", "intrusive",
"vuln", } }
Entry { filename = "broadcast-bjnp-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-db2-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-dhcp-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-dhcp6-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-dns-service-discovery.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-dropbox-listener.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-eigrp-discovery.nse", categories = { "broadcast", "discovery",
"safe", } }
Entry { filename = "broadcast-igmp-discovery.nse", categories = { "broadcast", "discovery"
```

Plain Text | Tab Width: 8 | Ln 1, Col 1 | INS

23

23

The Nmap Scripting Engine

- Categories of the available scripts
  - ❖ Information gathering
  - ❖ Active vulnerability assessment
  - ❖ Searches for signs of previous compromises, and so on
- Currently defined categories are auth, broadcast, brute, default. discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version, and vuln. Category names are not case sensitive
- To get more information about a particular script or category of scripts
  - ❖ # nmap --script-help default
- Run all the scripts in the *default* category, ***-sC***
  - ❖ # nmap -sC <target IP address(es)>

Categories
auth
broadcast
brute
default
discovery
dos
exploit
external
fuzzer
intrusive
malware
safe
version
vuln

24

24

Running NSE Scripts

- To run NSE
  - ❖nmap --script=[all, category, dir, script] [target] –p [ports]
  - ❖Add --script-args=[arguments] to pass arguments to a script
  - ❖Do not run all scripts since NSE contains Dos scripts which may harm target systems

Categories
auth
broadcast
brute
default
discovery
dos
exploit
external
fuzzer
intrusive
malware
safe
version
vuln

25

25

Running a Single NSE Script

- The NSE script **nfs-ls**.nse
  - ❖Connects to NFS and audit shares
  - ❖**Mounts the remote shares, audits their permissions, and lists the files included in the share**
  - ❖# nmap --script=nfs-ls <target IP address>
- More information about a script?
  - ❖# nmap --script-help nfs-ls
- --script-trace: detailed output from each script

26

26

Metasploit Scanner Modules

- msf > use scanner/ftp/anonymous
- msf auxiliary(anonymous) > set RHOSTS <target IP address(es)>
- msf auxiliary(anonymous) > exploit

- Anonymous FTP login credentials
  - User: anonymous
  - Password: guest

27

27

Metasploit Exploit Check Functions

- "**check**" functions
  - Connects to a target to see if it is vulnerable, rather than attempting to exploit a vulnerability

- msf > use windows/smb/ms08_067_netapi
  msf exploit(ms08_067_netapi) > set RHOST <target IP address>
  msf exploit(ms08_067_netapi) > check

28

28