

HARSHIT SRIVASTAVA

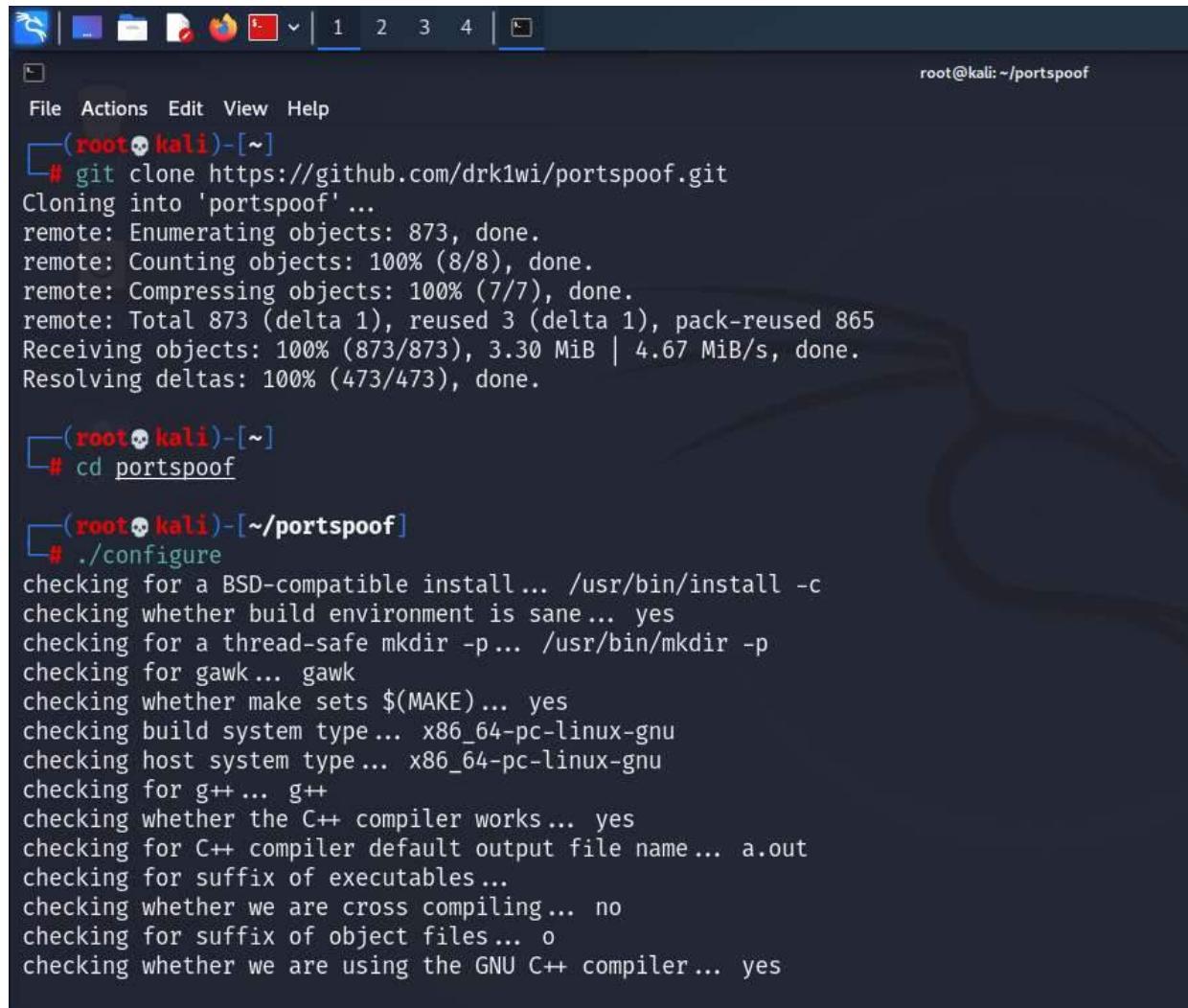
19BCE0382

LAB ASSIGNMENT- 2

28/02/2022 WINTER SEM 2021-22 [SLOT: L5+L6]

1. Port Spoof Install

Download and Configure



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title bar says '(root㉿kali)-[~]'. The command history shows:

```
# git clone https://github.com/drk1wi/portspoof.git
Cloning into 'portspoof' ...
remote: Enumerating objects: 873, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 873 (delta 1), reused 3 (delta 1), pack-reused 865
Receiving objects: 100% (873/873), 3.30 MiB | 4.67 MiB/s, done.
Resolving deltas: 100% (473/473), done.

[root@kali ~]# cd portspoof
[root@kali ~]# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking for g++... g++
checking whether the C++ compiler works... yes
checking for C++ compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C++ compiler... yes
```

Make and Install

```
root@kali:~/portspoof# make
Making all in src
make[1]: Entering directory '/root/portspoof/src'
make all-am
make[2]: Entering directory '/root/portspoof/src'
g++ -DHAVE_CONFIG_H -I. -DConfDir="/usr/local/etc" -g -O2 -MT portspoof-Configuration.o -MD -MP -MF .deps/portspoof-Configuration.Tpo -c -o portspoof-Configuration.o `test -f 'Configuration.cpp' || echo './Configuration.cpp'
mv -f .deps/portspoof-Configuration.Tpo .deps/portspoof-Configuration.Po
g++ -DHAVE_CONFIG_H -I. -DConfDir="/usr/local/etc" -g -O2 -MT portspoof-connection.o -MD -MP -MF .deps/portspoof-connection.Tpo -c -o portspoof-connection.o `test -f 'connection.cpp' || echo './connection.cpp'
mv -f .deps/portspoof-connection.Tpo .deps/portspoof-connection.Po
g++ -DHAVE_CONFIG_H -I. -DConfDir="/usr/local/etc" -g -O2 -MT portspoof-Fuzzer.o -MD -MP -MF .deps/portspoof-Fuzzer.Tpo -c -o portspoof-Fuzzer.o `test -f 'Fuzzer.cpp' || echo './Fuzzer.cpp'
mv -f .deps/portspoof-Fuzzer.Tpo .deps/portspoof-Fuzzer.Po
g++ -DHAVE_CONFIG_H -I. -DConfDir="/usr/local/etc" -g -O2 -MT portspoof-Portspoof.o -MD -MP -MF .deps/portspoof-Portspoof.Tpo -c -o portspoof-Portspoof.o `test -f 'Portspoof.cpp' || echo './Portspoof.cpp'
mv -f .deps/portspoof-Portspoof.Tpo .deps/portspoof-Portspoof.Po
g++ -DHAVE_CONFIG_H -I. -DConfDir="/usr/local/etc" -g -O2 -MT portspoof-Server.o -MD -MP -MF .deps/portspoof-Server.Tpo -c -o portspoof-Server.o `test -f 'Server.cpp' || echo './Server.cpp'
Server.cpp: In constructor 'Server::Server(Configuration*)':
Server.cpp:51:76: warning: cast to pointer from integer of different size [Wint-to-pointer-cast]
  51 |     pthread_create(&threads[i].tid, NULL, &process_connection, (void *) i);
      |                                     ^~~~~~
mv -f .deps/portspoof-Server.Tpo .deps/portspoof-Server.Po
g++ -DHAVE_CONFIG_H -I. -DConfDir="/usr/local/etc" -g -O2 -MT portspoof-Revregex.o -MD -MP -MF .deps/portspoof-Revregex.Tpo -c -o portspoof-Revregex.o `test -f 'Revregex.cpp' || echo './Revregex.cpp'
mv -f .deps/portspoof-Revregex.Tpo .deps/portspoof-Revregex.Po
```

```
root@kali:~/portspoof# make install
Making install in src
make[1]: Entering directory '/root/portspoof/src'
make[2]: Entering directory '/root/portspoof/src'
test -z "/usr/local/bin" || /usr/bin/mkdir -p "/usr/local/bin"
 /usr/bin/install -c portspoof '/usr/local/bin'
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/root/portspoof/src'
make[1]: Leaving directory '/root/portspoof/src'
Making install in tools
make[1]: Entering directory '/root/portspoof/tools'
make[2]: Entering directory '/root/portspoof/tools'
test -z "/usr/local/etc" || /usr/bin/mkdir -p "/usr/local/etc"
 /usr/bin/install -c -m 644 portspoof.conf portspoof_signatures '/usr/local/etc'
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/root/portspoof/tools'
make[1]: Leaving directory '/root/portspoof/tools'
make[1]: Entering directory '/root/portspoof'
make[2]: Entering directory '/root/portspoof'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/root/portspoof'
make[1]: Leaving directory '/root/portspoof'
```

2. Information gathering techniques

WhoIs

Whois Record for Vit.ac.in

Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Country	: in
Registrar	ERNET India IANA ID: 800068 URL: http://www.ernet.in Whois Server: -
Registrar Status	ok
Dates	6,818 days old Created on 2003-06-29 Expires on 2028-06-29 Updated on 2019-05-17
Name Servers	NS-1067.AWSDNS-05.ORG (has 50,971 domains) NS-1772.AWSDNS-29.CO.UK (has 352 domains) NS-389.AWSDNS-48.COM (has 271 domains) NS-865.AWSDNS-44.NET (has 19 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p x {) x

IP Address: 136.233.9.13 - 1 other site is hosted on this server

DomainTools Iris: More data. Better context. Faster response. Learn More. Preview the Full Domain Report.

Tools: Hosting History, Monitor Domain Properties, Visit Website, Upcoming Events, Recent News.

5:18 PM 2/27/2022 ENG IN

Whois Record | last updated on 2022-02-27

Domain Name: vit.ac.in
Registry Domain ID: D8480-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2019-05-18T05:44:08Z
Creation Date: 2003-06-30T04:00:00Z
Registry Expiry Date: 2028-06-30T04:00:00Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registrar Registration ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Tamil Nadu
Registrant Postal Code: REDACTED FOR PRIVACY

Available TLDs: General TLDs, Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

- Taken domain.
- Available domain.
- Deleted previously owned domain.

Vit.com	View Whois
Vit.net	View Whois
Vit.org	View Whois
Vit.info	View Whois
Vit.biz	Buy Domain
Vit.us	View Whois

5:19 PM 2/27/2022 ENG IN

Netcraft

Site report for https://vit.ac.in

Look up another site?

Share: [Email](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Print](#)

Background

Site title	VIT No.1 Private Institution for Innovation	Date first seen	June 2002
Site rank	91791	Netcraft Risk Rating	0/10
Description	Established in 1984, VIT is a No.1 Progressive Educational institution & Top Ranking University in India. Its a dedicated to the pursuit of excellence.	Primary language	English

Network

Site	https://vit.ac.in	Domain	vit.ac.in
Netblock Owner	Reliance Jio Infocomm Limited	Nameserver	ns-389.awsdns-48.com
Hosting company	Reliance Industries	Domain registrar	registry.in
Hosting country	IN	Nameserver organisation	whois.markmonitor.com

Site report for https://vit.ac.in

Look up another site?

Share: [Email](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Print](#)

Network

Site	https://vit.ac.in	Domain	vit.ac.in
Netblock Owner	Reliance Jio Infocomm Limited	Nameserver	ns-389.awsdns-48.com
Hosting company	Reliance Industries	Domain registrar	registry.in
Hosting country	IN	Nameserver organisation	whois.markmonitor.com

IP delegation

IPv4 address (136.233.9.13)

IP range	Country	Name	Description
0.0.0.0-255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 136.0.0.0-136.255.255.255	United States	NET136	Various Registries (Maintained by ARIN)
↳ 136.232.0.0-136.233.255.255	India	RELIANCEJIO-IN	Reliance Jio Infocomm Limited
↳ 136.233.9.13	India	RELIANCEJIO-IN	Reliance Jio Infocomm Limited

SSL/TLS Report for vit.ac.in

Assurance: Perfect Forward Secrecy (No)

Common name: *.vit.ac.in (Supported TLS Extensions: RFC5746, RFC5077)

Organisation: Not Present (Application-Layer Protocol Negotiation: Not Present)

State: Not Present (Next Protocol Negotiation: Not Present)

Country: Not Present (Issuing organisation: Sectigo Limited)

Organisational unit: Not Present (Issuer common name: Sectigo RSA Domain Validation Secure Server CA)

Subject Alternative Name: *.vit.ac.in, vit.ac.in (Issuer unit: Not Present)

Validity period: From Aug 10 2020 to Aug 10 2022 (24 months) (Issuer location: Salford)

Matches hostname: Yes (Issuer country: GB)

Server: Apache (Issuer state: Greater Manchester)

Public key algorithm: RSAEncryption (Certificate Revocation Lists: Not Present)

Protocol version: TLSv1.2 (Certificate Hash: PWwdIGql+tljr88W2lwma+Dkiv/g)

Public key length: 2048 (Public Key Hash: 9e0cba5e248da709507dee5d2ec2805b2f9d80ee828835c367338caeb76)

Certificate check: OK (OCSP servers: http://ocsp.sectigo.com - 100% uptime in the past 24 hours) (Performance Graph)

Robtex

ANALYSIS

This section shows a quick analysis of the given host name or ip number.

Google name servers

The name servers are ns1.google.com, ns2.google.com, ns3.google.com and ns4.google.com.

Google mail servers

The mail servers are aspmx.l.google.com, alt1.aspmx.l.google.com, alt2.aspmx.l.google.com, alt3.aspmx.l.google.com and alt4.aspmx.l.google.com.

IP numbers

The IP numbers are 2404:6800:4003:c02::8b, 2404:6800:4004:807::200e, 2404:6800:4006:803::200e, 2607:f8b0:4004:811::200e, 2607:f8b0:4005:802::200e, 2607:f8b0:4009:809::200e, 2800:3f0:4001:803::200e, 2a00:1450:4009:821::200e, 2a00:1450:400b:805::200e, 74.125.68.100, 74.125.68.101, 74.125.68.102, 74.125.68.113, 74.125.68.138, 172.217.0.46, 172.217.15.110, 172.217.16.238, 172.217.27.78, 172.217.29.14, 172.217.171.14, 216.58.194.174 and 216.58.199.46. The PTRs of the IP numbers are sc-in-f139.1e100.net, sc-in-x8b.1e100.net, nrt12s15-in-x0e.1e100.net, syd09s12-in-x0e.1e100.net, iad30s21-in-x0e.1e100.net, nup04s44-in-x0e.1e100.net, sfo07s26-in-x0e.1e100.net, sea15s12-in-x0e.1e100.net, lhr48s28-in-x0e.1e100.net, dub16s02-in-x0e.1e100.net, sc-in-f100.1e100.net, sc-in-f101.1e100.net, sc-in-f102.1e100.net, sc-in-f113.1e100.net, iad66s02-in-f14.1e100.net, lg15s43-in-f14.1e100.net, sfo07s26-in-f14.1e100.net, iad10s21-in-f14.1e100.net, lhr48s28-in-f14.1e100.net, mar08s04-in-f14.1e100.net, nrt12s15-in-f14.1e100.net, nrt12s15-in-f78.1e100.net, era03s04-in-f14.1e100.net, am14s06-in-f14.1e100.net.

Shodan

TOTAL RESULTS: 6

TOP PORTS:

Port	Count
25	2
80	2
443	2

TOP ORGANIZATIONS:

Organization	Count
Reliance Jio Infocomm Limited	4
Bharti Airtel Limited	2

TOP PRODUCTS:

Product	Count
Apache httpd	2
Microsoft Exchange smtpd	1

Vellore Institute of Technology | A Place to Learn, Chance to grow

SSL Certificate

Issued By: Sectigo RSA Domain Validation Secure Server CA

Issued To: Reliance Jio Infocomm Limited

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

136.233.9.13

HTTP/1.1 302 Object Moved

Location: https://vit.ac.in/

Content-type: text/html

Cache-Control: private

Connection: close

Dirb

```
DIRB v2.22
By The Dark Raver

dirb <url_base> [<wordlist_file(s)>] [options]

===== NOTES =====
<url_base> : Base URL to scan. (Use -resume for session resuming)
<wordlist_file(s)> : List of wordfiles. (wordfile1,wordfile2,wordfile3 ... )

===== HOTKEYS =====
'n' → Go to next directory.
'q' → Stop scan. (Saving state for resume)
'r' → Remaining scan stats.

===== OPTIONS =====
-a <agent_string> : Specify your custom USER_AGENT.
-b : Use path as is.
-c <cookie_string> : Set a cookie for the HTTP request.
-E <certificate> : path to the client certificate.
-f : Fine tuning of NOT_FOUND (404) detection.
-H <header_string> : Add a custom header to the HTTP request.
-i : Use case-insensitive search.
```

```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | || | ↻ | ☰ | X
S | D | F | R | E | ↻ | 1 2 3 4 | ☰
File Actions Edit View Help
(root💀kali)-[~]
# dirb https://inspiring-visvesvaraya-faa643.netlify.app/
_____
DIRB v2.22
By The Dark Raver
_____
START_TIME: Mon Feb 28 09:17:48 2022
URL_BASE: https://inspiring-visvesvaraya-faa643.netlify.app/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
_____
GENERATED WORDS: 4612
_____
— Scanning URL: https://inspiring-visvesvaraya-faa643.netlify.app/ —
^[
→ Testing: https://inspiring-visvesvaraya-faa643.netlify.app/admissions
```

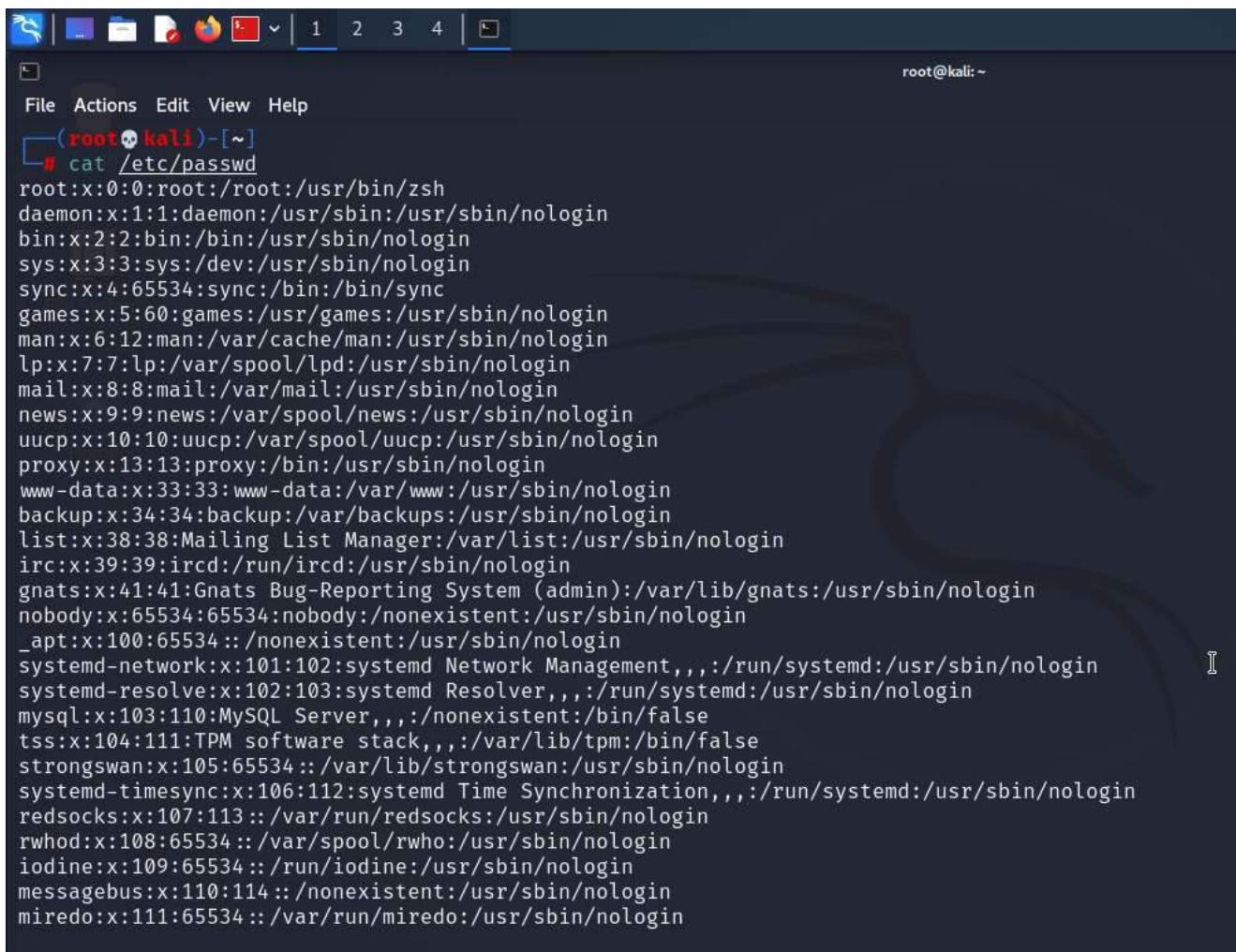
NMAP

```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | || | ↻ | ☰ | X
S | D | F | R | E | ↻ | 1 2 3 4 | ☰
File Actions Edit View Help
(root💀kali)-[~]
# nmap -Pn 192.168.1.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-28 09:21 EST
Nmap scan report for 192.168.1.6
Host is up (0.013s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
2869/tcp   open  icslap
3306/tcp   open  mysql

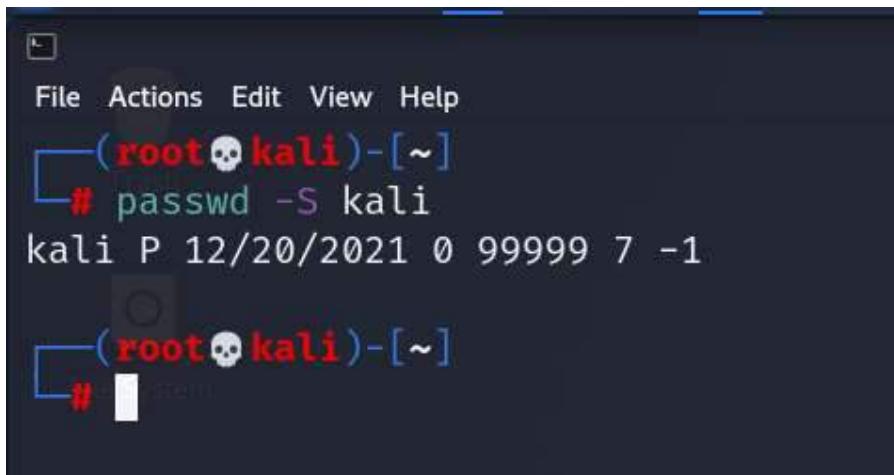
Nmap done: 1 IP address (1 host up) scanned in 10.30 seconds
(root💀kali)-[~]
#
```

3. Incident Response Linux

USER ACCOUNTS



```
root@kali:~# cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:103:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:104:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:105:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:106:112:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
redsocks:x:107:113::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:108:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:109:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:110:114::/nonexistent:/usr/sbin/nologin
miredo:x:111:65534::/var/run/miredo:/usr/sbin/nologin
```



```
root@kali:~# passwd -S kali
kali P 12/20/2021 0 99999 7 -1

root@kali:~#
```

```
[root💀kali㉿kali:~]
# grep :0: /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh

[root💀kali㉿kali:~]
# find / -nouser -print
find: '/proc/1956/task/1956/fd/5': No such file or directory
find: '/proc/1956/task/1956/fdinfo/5': No such file or directory
find: '/proc/1956/fd/6': No such file or directory
find: '/proc/1956/fdinfo/6': No such file or directory
find: '/run/user/1000/gvfs': Permission denied
```

File Actions Edit View Help

```
[root💀kali㉿kali:~]
# cat /etc/shadow
root!:18981:0:99999:7:::
daemon:*:18981:0:99999:7:::
bin:*:18981:0:99999:7:::
sys:*:18981:0:99999:7:::
sync:*:18981:0:99999:7:::
games:*:18981:0:99999:7:::
man:*:18981:0:99999:7:::
lp:*:18981:0:99999:7:::
mail:*:18981:0:99999:7:::
news:*:18981:0:99999:7:::
uucp:*:18981:0:99999:7:::
proxy:*:18981:0:99999:7:::
www-data:*:18981:0:99999:7:::
backup:*:18981:0:99999:7:::
list:*:18981:0:99999:7:::
irc:*:18981:0:99999:7:::
gnats:*:18981:0:99999:7:::
nobody:*:18981:0:99999:7:::
_apt:*:18981:0:99999:7:::
systemd-network:*:18981:0:99999:7:::
systemd-resolve:*:18981:0:99999:7:::
mysql!:18981:0:99999:7:::
tss:*:18981:0:99999:7:::
strongswan:*:18981:0:99999:7:::
systemd-timesync:*:18981:0:99999:7:::
redsocks!:18981:0:99999:7:::
rwhod:*:18981:0:99999:7:::
iodine:*:18981:0:99999:7:::
messagebus:*:18981:0:99999:7:::
```

```
(root💀kali)-[~]
# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:kali,root
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:kali,root
fax:x:21:
voice:x:22:
cdrom:x:24:kali
floppy:x:25:kali
tape:x:26:
sudo:x:27:kali
audio:x:29:pulse,kali
dip:x:30:kali
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
```

```
(root💀kali)-[~]
# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

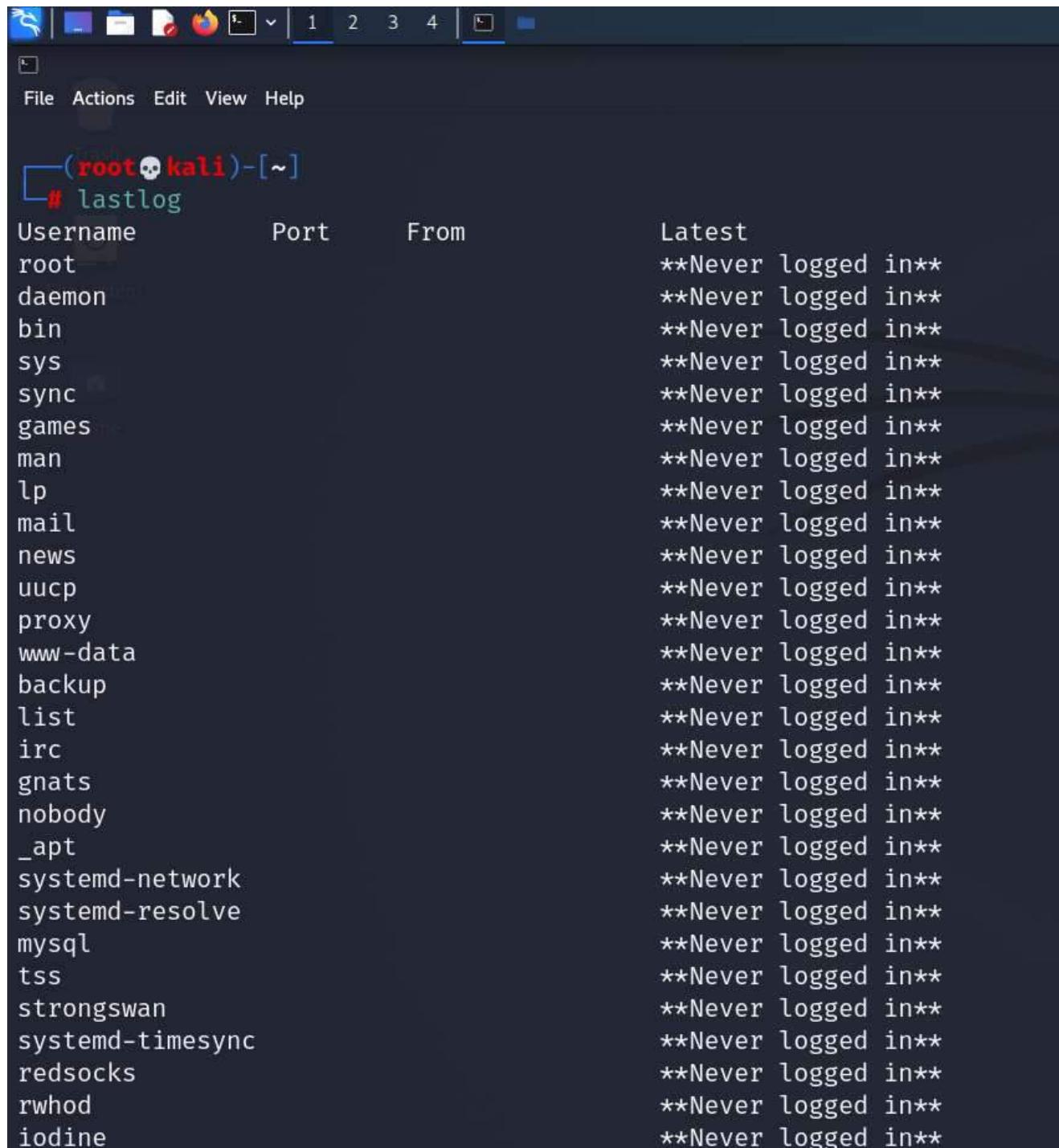
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:
@includedir /etc/sudoers.d
```

LOG ENTRIES



The screenshot shows a terminal window titled '(root💀kali)-[~]' running on a Kali Linux system. The window displays the output of the 'lastlog' command, which lists various system users and their login status. The columns in the table are 'Username', 'Port', 'From', and 'Latest'. Most users have a 'Latest' entry of '**Never logged in**', indicating they have not logged in recently.

Username	Port	From	Latest
root			**Never logged in**
daemon			**Never logged in**
bin			**Never logged in**
sys			**Never logged in**
sync			**Never logged in**
games			**Never logged in**
man			**Never logged in**
lp			**Never logged in**
mail			**Never logged in**
news			**Never logged in**
uucp			**Never logged in**
proxy			**Never logged in**
www-data			**Never logged in**
backup			**Never logged in**
list			**Never logged in**
irc			**Never logged in**
gnats			**Never logged in**
nobody			**Never logged in**
_apt			**Never logged in**
systemd-network			**Never logged in**
systemd-resolve			**Never logged in**
mysql			**Never logged in**
tss			**Never logged in**
strongswan			**Never logged in**
systemd-timesync			**Never logged in**
redsocks			**Never logged in**
rwhod			**Never logged in**
iodine			**Never logged in**

```
(root㉿kali)-[~]
# cd var

(root㉿kali)-[/var]
# ls
backups cache lib local lock log mail opt run spool tmp www

(root㉿kali)-[/var]
# cd log

(root㉿kali)-[/var/log]
# tail auth.log
Feb 27 11:08:39 kali systemd: pam_unix(systemd-user:session): session opened for user kali(uid=1000) by (uid=0)
Feb 27 11:08:39 kali lightdm: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Feb 27 11:08:41 kali polkitd(authority=local): Registered Authentication Agent for unix-session:2 (system bus name :1.41 [/usr/lib/policykit-1-gnome/polkit-gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Feb 27 11:09:01 kali CRON[1291]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Feb 27 11:09:01 kali CRON[1291]: pam_unix(cron:session): session closed for user root
Feb 27 11:09:02 kali polkitd(authority=local): Operator of unix-session:2 successfully authenticated as unix-user:kali to gain ONE-SHOT authorization for action org.kali.pkexec.x-terminal-emulator for unix-process:979:3018 [/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libwhiskermenu.so 1 16777223 whiskermenu Whisker Menu Show a menu to easily access installed applications] (owned by unix-user:kali)
Feb 27 11:09:02 kali pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by (uid=1000)
Feb 27 11:09:02 kali pkexec[1269]: kali: Executing command [USER=root] [TTY=unknown] [CWD=/home/kali] [COMMAND=/usr/bin/x-terminal-emulator]
Feb 27 11:15:01 kali CRON[3083]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Feb 27 11:15:01 kali CRON[3083]: pam_unix(cron:session): session closed for user root
```

```
1  clear
2  tor
3  ifconfig
4  who -a
5  nmap
6  clear
7  nmap 192.168.1.1-255
8  cleat
9  clear
10 nmap -Pn 192.168.1.1
11 nmap -Pn 192.168.1.0
12 nmap -Pn 192.168.1.9
13 who -a
14 clear
15 git clone https://github.com/drk1wi/portspoof.git
16 cd portspoof
17 ./configure
18 make
19 clear
20 make
21 make install
22 clear
23 iptables -A PREROUTING -i eth0 -p tcp -m tcp --dport 1:65535 -j REDIRECT --to-ports 4444
24 ifconfig
25 clear
26 ping 192.168.1.9
27 clear
28 nmap -Pn 192.168.1.9
29 ifconfig
30 nmap -Pn 192.168.16.129
31 nmap -Pn 192.168.1.9
:
```

SYSTEM RESOURCES

root@kali:/var/log

```
(root💀kali)-[~/var/log]
# uptime
11:18:46 up 10 min,  1 user,  load average: 0.13, 0.15, 0.09

(root💀kali)-[~/var/log]
# free
              total        used        free      shared  buff/cache   available
Mem:       4016560     710988    2191696        20504    1113876    2987824
Swap:      998396          0     998396
```

File Actions Edit View Help

```
(root💀kali)-[~/var/log]
# cat /proc/meminfo

MemTotal:      4016560 kB
MemFree:       2202824 kB
MemAvailable:  2998808 kB
Buffers:        194484 kB
Cached:         378408 kB
SwapCached:     0 kB
Active:         313200 kB
Inactive:      758104 kB
Active(anon):   1088 kB
Inactive(anon): 517824 kB
Active(file):   312112 kB
Inactive(file): 240280 kB
Unevictable:    96 kB
Mlocked:        96 kB
SwapTotal:     998396 kB
SwapFree:      998396 kB
Dirty:          456 kB
Writeback:      0 kB
AnonPages:     482432 kB
Mapped:         202148 kB
Shmem:          20500 kB
KReclaimable:  540836 kB
Slab:           588700 kB
SReclaimable:  540836 kB
SUnreclaim:    47864 kB
KernelStack:    5792 kB
PageTables:    9520 kB
NFS_Unstable:   0 kB
```

```

root@kali:/var/log
# cat /proc/mounts
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
udev /dev devtmpfs rw,nosuid,relatime,size=1965976k,nr_inodes=491494,mode=755,inode64 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /run tmpfs rw,nosuid,nodev,noexec,relatime,size=401656k,mode=755,inode64 0 0
/dev/sda1 / ext4 rw,relatime,errors=remount-ro 0 0
securityfs /sys/kernel/security securityfs rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev/shm tmpfs rw,nosuid,nodev,inode64 0 0
tmpfs /run/lock tmpfs rw,nosuid,nodev,noexec,relatime,size=5120k,inode64 0 0
cgroup2 /sys/fs/cgroup cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
pstore /sys/fs/pstore pstore rw,nosuid,nodev,noexec,relatime 0 0
none /sys/fs/bpf bpf rw,nosuid,nodev,noexec,relatime,mode=700 0 0
systemd-1 /proc/sys/fs/binfmt_misc autofs rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=10206 0 0
hugetlbfs /dev/hugepages hugetlbfs rw,relatime,pagesize=2M 0 0
mqqueue /dev/mqueue mqqueue rw,nosuid,nodev,noexec,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,nosuid,nodev,noexec,relatime 0 0
tracefs /sys/kernel/tracing tracefs rw,nosuid,nodev,noexec,relatime 0 0
sunrpc /run/rpc_pipefs rpc_pipefs rw,relatime 0 0
configfs /sys/kernel/config configfs rw,nosuid,nodev,noexec,relatime 0 0
fusectl /sys/fs/fuse/connections fusectl rw,nosuid,nodev,noexec,relatime 0 0
none /run/credentials/systemd-susers.service ramfs ro,nosuid,nodev,noexec,relatime,mode=700 0 0
vmware-vmblock /run/vmblock-fuse fuse.vmware-vmblock rw,relatime,user_id=0,group_id=0,default_permissions,allow_other 0 0
binfmt_misc /proc/sys/fs/binfmt_misc binfmt_misc rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /run/user/1000 tmpfs rw,nosuid,nodev,relatime,size=401656k,nr_inodes=100414,mode=700,uid=1000,gid=1000,inode64 0 0
gvfsd-fuse /run/user/1000/gvfs fuse.gvfsd-fuse rw,nosuid,nodev,relatime,user_id=1000,group_id=1000 0 0
tracefs /sys/kernel/debug/tracing tracefs rw,nosuid,nodev,noexec,relatime 0 0

```

PROCESSES

TOP:

```

root@kali:/var/log
top - 11:21:19 up 13 min, 1 user, load average: 0.09, 0.11, 0.09
Tasks: 200 total, 1 running, 199 sleeping, 0 stopped, 0 zombie
%Cpu(s): 3.1 us, 1.0 sy, 0.0 ni, 95.1 id, 0.7 wa, 0.0 hi, 0.1 si, 0.0 st
MiB Mem : 3922.4 total, 2144.0 free, 688.6 used, 1089.8 buff/cache
MiB Swap: 975.0 total, 975.0 free, 0.0 used. 2922.7 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
718 root 20 0 474548 152164 62076 S 11.3 3.8 0:23.95 Xorg
4874 kali 20 0 469676 42124 32824 S 2.7 1.0 0:00.43 xfce4-screensho
933 kali 20 0 1220616 94192 66584 S 2.0 2.3 0:05.46 xfwm4
191 root -51 0 0 0 0 S 0.3 0.0 0:00.35 irq/16-vmwgfx
251 root 20 0 0 0 0 I 0.3 0.0 0:00.27 kworker/1:2-events
980 kali 20 0 215308 32556 17432 S 0.3 0.8 0:02.52 panel-13-cpugra
1070 kali 20 0 289836 40020 28820 S 0.3 1.0 0:01.40 vmtoolsd
1269 root 20 0 411492 86032 68416 S 0.3 2.1 0:02.12 x-terminal-emul
1 root 20 0 164544 10580 7788 S 0.0 0.3 0:01.09 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.01 kthreadd
3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
6 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker/0:0H-events_highpri
7 root 20 0 0 0 0 I 0.0 0.0 0:01.93 kworker/u64:0-flush-8:0
8 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu_wq
9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_tasks_rude_
10 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_tasks_trace
11 root 20 0 0 0 0 S 0.0 0.0 0:00.01 ksoftirqd/0
12 root 20 0 0 0 0 I 0.0 0.0 0:00.28 rcu_sched
13 root rt 0 0 0 0 S 0.0 0.0 0:00.00 migration/0
14 root 20 0 0 0 0 I 0.0 0.0 0:00.04 kworker/0:1-events
15 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/0
16 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/1
17 root rt 0 0 0 0 0 S 0.0 0.0 0:00.29 migration/1
18 root 20 0 0 0 0 S 0.0 0.0 0:00.03 ksoftirqd/1

```

```
root@kali:/var/log
File Actions Edit View Help
( root💀kali )-[ /var/log ]
# ps aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.1 0.2 164544 10580 ? Ss 11:08 0:01 /sbin/init splash
root 2 0.0 0.0 0 0 ? S 11:08 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? I< 11:08 0:00 [rcu_gp]
root 4 0.0 0.0 0 0 ? I< 11:08 0:00 [rcu_par_gp]
root 6 0.0 0.0 0 0 ? I< 11:08 0:00 [kworker/0:0H-events_highpri]
root 7 0.2 0.0 0 0 ? I 11:08 0:01 [kworker/u64:0-events_unbound]
root 8 0.0 0.0 0 0 ? I< 11:08 0:00 [mm_percpu_wq]
root 9 0.0 0.0 0 0 ? S 11:08 0:00 [rcu_tasks_rude_]
root 10 0.0 0.0 0 0 ? S 11:08 0:00 [rcu_tasks_trace]
root 11 0.0 0.0 0 0 ? S 11:08 0:00 [ksoftirqd/0]
root 12 0.0 0.0 0 0 ? I 11:08 0:00 [rcu_sched]
root 13 0.0 0.0 0 0 ? S 11:08 0:00 [migration/0]
root 14 0.0 0.0 0 0 ? I 11:08 0:00 [kworker/0:1-events]
root 15 0.0 0.0 0 0 ? S 11:08 0:00 [cpuhp/0]
root 16 0.0 0.0 0 0 ? S 11:08 0:00 [cpuhp/1]
root 17 0.0 0.0 0 0 ? S 11:08 0:00 [migration/1]
root 18 0.0 0.0 0 0 ? S 11:08 0:00 [ksoftirqd/1]
root 20 0.0 0.0 0 0 ? I< 11:08 0:00 [kworker/1:0H-events_highpri]
root 21 0.0 0.0 0 0 ? S 11:08 0:00 [cpuhp/2]
root 22 0.0 0.0 0 0 ? S 11:08 0:00 [migration/2]
root 23 0.0 0.0 0 0 ? S 11:08 0:00 [ksoftirqd/2]
root 25 0.0 0.0 0 0 ? I< 11:08 0:00 [kworker/2:0H-events_highpri]
root 26 0.0 0.0 0 0 ? S 11:08 0:00 [cpuhp/3]
root 27 0.0 0.0 0 0 ? S 11:08 0:00 [migration/3]
root 28 0.0 0.0 0 0 ? S 11:08 0:00 [ksoftirqd/3]
root 30 0.0 0.0 0 0 ? I< 11:08 0:00 [kworker/3:0H-events_highpri]
root 32 0.0 0.0 0 0 ? R 11:08 0:00 [kworker/u64:1-events_unbound]
root 35 0.0 0.0 0 0 ? S 11:08 0:00 [kdevtmpfs]
```

SERVICES

```
(root💀kali)-[~]
# service --status-all

[ - ] apache-htcacheclean
[ - ] apache2
[ - ] apparmor
[ - ] atftpd
[ - ] avahi-daemon
[ + ] binfmt-support
[ - ] bluetooth
[ - ] console-setup.sh
[ + ] cron
[ - ] cryptdisks
[ - ] cryptdisks-early
[ + ] dbus
[ - ] dns2tcp
[ + ] haveged
[ - ] hwclock.sh
[ - ] inetsim
[ - ] iodined
[ - ] ipsec
[ - ] keyboard-setup.sh
[ + ] kmod
[ + ] lightdm
[ - ] mariadb
[ - ] miredo
[ + ] networking
[ - ] nfs-common
[ - ] nginx
[ - ] nmbd
```

```
File Actions Edit View Help
root@kali: ~
# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab` command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# ┌───────── minute (0 - 59)
# ┌───────── hour (0 - 23)
# ┌───────── day of month (1 - 31)
# ┌───────── month (1 - 12) OR jan,feb,mar,apr ...
# ┌───────── day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# * * * * * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

```
root@kali: ~
File Actions Edit View Help
└──(root💀kali)-[~]
    └──# more /etc/resolv.conf
        # Generated by NetworkManager
        search localdomain
        nameserver 192.168.16.2

└──(root💀kali)-[~]
    └──# more /etc/hosts
        127.0.0.1      localhost
        127.0.1.1      kali

        # The following lines are desirable for IPv6 capable hosts
        ::1      localhost ip6-localhost ip6-loopback
        ff02::1  ip6-allnodes
        ff02::2  ip6-allrouters

└──(root💀kali)-[~]
    └──# iptables -L -n

        Chain INPUT (policy ACCEPT)
        target     prot opt source          destination

        Chain FORWARD (policy ACCEPT)
        target     prot opt source          destination

        Chain OUTPUT (policy ACCEPT)
        target     prot opt source          destination
```

FILES

```
root@kali: ~
File Actions Edit View Help
└──(root💀kali)-[~]
    └──# find /home/ -type f -size +512k -exec ls -lh {} \;
        -rw-r--r-- 1 kali kali 5.0M Feb 27 06:40 /home/kali/.mozilla/firefox/oomnrqj6.default-esr/places.sqlite
        -rw-r--r-- 1 kali kali 928K Feb 27 06:40 /home/kali/.mozilla/firefox/oomnrqj6.default-esr/storage/permanent/chrome/idb/3870112724rsegmnnoittet-es.sqlite
        -rw-r--r-- 1 kali kali 5.0M Feb 27 06:40 /home/kali/.mozilla/firefox/oomnrqj6.default-esr/favicons.sqlite
        -rw-r--r-- 1 kali kali 778K Feb 27 11:17 /home/kali/Documents/LinuxIncident/8.png
        -rw-r--r-- 1 kali kali 518K Feb 27 11:25 /home/kali/Documents/LinuxIncident/16.png
        -rw-r--r-- 1 kali kali 594K Feb 27 11:22 /home/kali/Documents/LinuxIncident/14.png
        -rw-r--r-- 1 kali kali 651K Feb 27 11:21 /home/kali/Documents/LinuxIncident/13.png
        -rw-r--r-- 1 kali kali 756K Feb 27 11:20 /home/kali/Documents/LinuxIncident/12.png
        -rw-r--r-- 1 kali kali 7.6M Feb 27 06:40 /home/kali/.cache/mozilla/firefox/oomnrqj6.default-esr/startupCache/scriptCache.bin
        -rw-r--r-- 1 kali kali 2.4M Feb 27 06:40 /home/kali/.cache/mozilla/firefox/oomnrqj6.default-esr/startupCache/scriptCache-child.bin
        -rw-r--r-- 1 kali kali 4.9M Feb 27 06:40 /home/kali/.cache/mozilla/firefox/oomnrqj6.default-esr/startupCache/startupCache.8.little
        -rw-r--r-- 1 kali kali 1.5M Feb 27 06:40 /home/kali/.cache/mozilla/firefox/oomnrqj6.default-esr/safebrowsing/google-trackwhite-digest256.vlpset
        -rw-r--r-- 1 kali kali 1.3M Feb 3 06:45 /home/kali/.cache/mesa_shader_cache/index
        -rw----- 1 kali kali 1.1M Feb 27 11:08 /home/kali/.cache/gstreamer-1.0/registry.x86_64.bin
```



File Actions Edit View Help

```
[root💀kali㉿kali: ~]
# find /etc/ -readable -type f 2>/dev/null
/etc/crypttab
/etc/bash_completion
/etc/perl/Net/libnet.cfg
/etc/strongswan.d/starter.conf
/etc/strongswan.d/charon-logging.conf
/etc/strongswan.d/charon/pgp.conf
/etc/strongswan.d/charon/sha2.conf
/etc/strongswan.d/charon/pkcs12.conf
/etc/strongswan.d/charon/xcbc.conf
/etc/strongswan.d/charon/bypass-lan.conf
/etc/strongswan.d/charon/drbg.conf
/etc/strongswan.d/charon/md5.conf
/etc/strongswan.d/charon/fips-prf.conf
/etc/strongswan.d/charon/attr.conf
/etc/strongswan.d/charon/sha1.conf
/etc/strongswan.d/charon/hmac.conf
/etc/strongswan.d/charon/revocation.conf
/etc/strongswan.d/charon/constraints.conf
/etc/strongswan.d/charon/aes.conf
/etc/strongswan.d/charon/pem.conf
/etc/strongswan.d/charon/stroke.conf
/etc/strongswan.d/charon/pkcs8.conf
/etc/strongswan.d/charon/socket-default.conf
/etc/strongswan.d/charon/counters.conf
/etc/strongswan.d/charon/pkcs7.conf
/etc/strongswan.d/charon/updown.conf
/etc/strongswan.d/charon/mgf1.conf
/etc/strongswan.d/charon/dnskey.conf
```

```
root@kali:~#
File Actions Edit View Help
[root@kali ~]# find / -mtime -2 -ls
1    0 dr-xr-xr-x 13 root      root      0 Feb 27 11:08 /sys
772   0 drwxr-xr-x 17 root      root      0 Feb 27 11:08 /sys/kernel
782   0 -r--r--r-- 1 root      root      532 Feb 27 11:11 /sys/kernel/notes
1009  0 drwxr-xr-x  6 root      root      0 Feb 27 11:08 /sys/kernel/mm
2404  0 drwxr-xr-x  3 root      root      0 Feb 27 11:08 /sys/kernel/mm/hugepages
2405  0 drwxr-xr-x  2 root      root      0 Feb 27 11:11 /sys/kernel/mm/hugepages/hugepages-2048kB
2408  0 -r--r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/hugepages/hugepages-2048kB/free_hugepages
2409  0 -r--r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/hugepages/hugepages-2048kB/resv_hugepages
2410  0 -r--r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/hugepages/hugepages-2048kB/surplus_hugepages
2411  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages_mempolicy
2406  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
2407  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/hugepages/hugepages-2048kB/nr_overcommit_hugepages
2432  0 drwxr-xr-x  3 root      root      0 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage
2434  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/defrag
2438  0 drwxr-xr-x  2 root      root      0 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/khugepaged
2439  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/khugepaged/defrag
2442  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/khugepaged/max_ptes_shared
2446  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/khugepaged/scan_sleep_millisecs
2440  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/khugepaged/max_ptes_none
2443  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/khugepaged/pages_to_scan
2441  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/khugepaged/max_ptes_swap
2447  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/khugepaged/alloc_sleep_millisecs
2444  0 -r--r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/khugepaged/pages_collapsed
2445  0 -r--r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/khugepaged/full_scans
2433  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/enabled
2435  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/use_zero_page
2437  0 -rw-r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/shmem_enabled
2436  0 -r--r--r--  1 root      root      4096 Feb 27 11:11 /sys/kernel/mm/transparent_hugepage/hpage_pmd_size
```

NETWORK SETTINGS

```
File Actions Edit View Help
root@kali:~#
[root@kali ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.16.129  netmask 255.255.255.0  broadcast 192.168.16.255
          inet6 fe80::20c:29ff:fe80:4cd5  prefixlen 64  scopeid 0x20<link>
            ether 00:0c:29:80:4c:d5  txqueuelen 1000  (Ethernet)
              RX packets 54  bytes 5333 (5.2 KiB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 78  bytes 6380 (6.2 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 8  bytes 400 (400.0 B)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 8  bytes 400 (400.0 B)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

[root@kali ~]#
```

```
root@kali:~#
File Actions Edit View Help
[root@kali ~]# lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
NetworkMa 537 root 23u IPv4 15953      0t0  UDP 192.168.16.129:bootpc→192.168.16.254:bootps

[root@kali ~]# netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address          State      PID/Program name
udp        0      0 192.168.16.129:68       192.168.16.254:67      ESTABLISHED 537/NetworkManager
raw6       0      0 ::*:58                 :::*                           7          537/NetworkManager
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State     I-Node PID/Program name   Path
unix    2      [ ACC ]     STREAM    LISTENING  15202  1/init           /run/dbus/system_bus_socket
unix    2      [ ACC ]     STREAM    LISTENING  19630  911/dbus-daemon   /tmp/dbus-st0Hl7S9jH
unix    2      [ ACC ]     STREAM    LISTENING  19234  1305/dbus-daemon  @/tmp/dbus-kn08u5zECY
unix    3      [ ]          DGRAM     LISTENING  10192  1/init           /run/systemd/notify
unix    2      [ ACC ]     STREAM    LISTENING  10195  1/init           /run/systemd/private
unix    2      [ ACC ]     STREAM    LISTENING  10197  1/init           /run/systemd/userdb/io.systemd.DynamicUser
unix    2      [ ACC ]     STREAM    LISTENING  10198  1/init           /run/systemd/io.system.ManagedOOM
unix    2      [ ]          DGRAM     LISTENING  10209  1/init           /run/systemd/journal/syslog
unix    2      [ ACC ]     STREAM    LISTENING  10211  1/init           /run/systemd/fsck.progress
unix   12      [ ]          DGRAM     LISTENING  10215  1/init           /run/systemd/journal/dev-log
unix    7      [ ]          DGRAM     LISTENING  10217  1/init           /run/systemd/journal/socket
unix    2      [ ACC ]     STREAM    LISTENING  10219  1/init           /run/systemd/journal/stdout
unix    2      [ ACC ]     STREAM    LISTENING  13213  718/Xorg         @/tmp/.X11-unix/X0
unix    2      [ ACC ]     SEQPACKET LISTENING 10221  1/init           /run/udev/control
unix    2      [ ]          DGRAM     LISTENING  19465  816/systemd      /run/user/1000/systemd/notify
unix    2      [ ACC ]     STREAM    LISTENING  19468  816/systemd      /run/user/1000/systemd/private
unix    2      [ ACC ]     STREAM    LISTENING  19473  816/systemd      /run/user/1000/bus
```

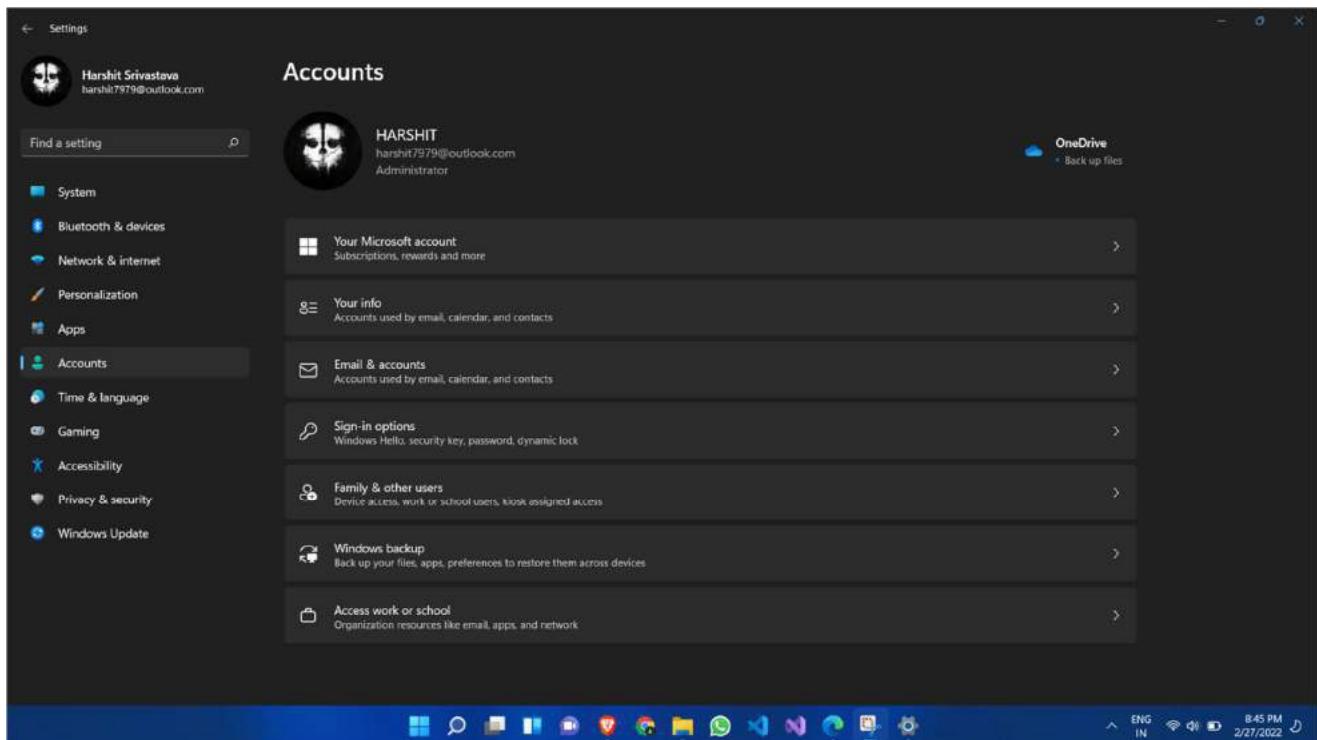
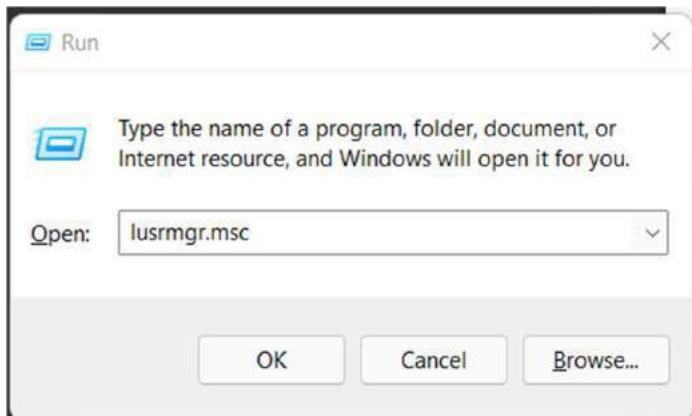
```
root@kali:~#
File Actions Edit View Help
[root@kali ~]# arp -a
? (192.168.16.2) at 00:50:56:e6:6d:78 [ether] on eth0
? (192.168.16.254) at 00:50:56:ed:d7:8e [ether] on eth0

[root@kali ~]# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games

[root@kali ~]#
```

4. Incident Response windows

USER ACCOUNTS



```
Command Prompt
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HARSHIT>net user

User accounts for \\LAPTOP-UE4331SF

-----
Administrator          DefaultAccount
HARSHIT                postgres
The command completed successfully.

C:\Users\HARSHIT>
```

A screenshot of the Windows Command Prompt window. It shows the output of the "net user" command, listing local user accounts: Administrator, DefaultAccount, HARSHIT, postgres, Guest, and WDAGUtilityAccount. The message "The command completed successfully." is also displayed. The prompt ends with "C:\Users\HARSHIT>".

```
Command Prompt  
C:\Users\HARSHIT>net localgroup administrators  
Alias name      administrators  
Comment          Administrators have complete and unrestricted access to the computer/domain  
Members  
  
Administrator  
HARSHIT  
The command completed successfully.  
  
C:\Users\HARSHIT>
```

```
Administrator: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows  
PS C:\WINDOWS\system32> Get-LocalUser  
Name           Enabled Description  
---  
Administrator   False  Built-in account for administering the computer/domain  
DefaultAccount  False  A user account managed by the system.  
Guest           False  Built-in account for guest access to the computer/domain  
HARSHIT         True   PostgreSQL service account  
postgres        True   PostgreSQL service account  
WDAGUtilityAccount False  A user account managed and used by the system for Windows Defender Application Guard scen...  
PS C:\WINDOWS\system32>
```

PROCESSES

Name		Status	12% CPU	55% Memory	0% Disk	0% Network
>	Windows PowerShell (2)		0.1%	45.0 MB	0 MB/s	0 Mbps
Background processes (125)						
>	Adobe Genuine Software Integri...		0%	0.1 MB	0 MB/s	0 Mbps
>	Adobe Genuine Software Servic...		0%	0.1 MB	0 MB/s	0 Mbps
>	Adobe Update Service (32 bit)		0%	0.2 MB	0 MB/s	0 Mbps
	AggregatorHost.exe		0%	0.6 MB	0 MB/s	0 Mbps
>	Antimalware Service Executable		1.2%	141.8 MB	0 MB/s	0 Mbps
	Antimalware Service Executable...		0%	69.1 MB	0 MB/s	0 Mbps
>	AppHelperCap.exe		0%	1.0 MB	0 MB/s	0 Mbps
	Application Frame Host		0%	8.6 MB	0 MB/s	0 Mbps
	Casting protocol connection list...		0%	1.6 MB	0 MB/s	0 Mbps
>	Clock	⌚	0%	0 MB	0 MB/s	0 Mbps
	COM Surrogate		0%	1.0 MB	0 MB/s	0 Mbps

^ Fewer details

End task

Command Prompt

Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HARSHIT>tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	7,264 K
Secure System	136	Services	0	41,564 K
Registry	208	Services	0	147,508 K
smss.exe	636	Services	0	1,068 K
csrss.exe	972	Services	0	4,396 K
wininit.exe	664	Services	0	4,548 K
services.exe	1056	Services	0	8,012 K
LsaIso.exe	1076	Services	0	3,016 K
lsass.exe	1084	Services	0	23,764 K
svchost.exe	1200	Services	0	49,020 K
fontdrvhost.exe	1228	Services	0	2,628 K
WUDFHost.exe	1284	Services	0	6,356 K
svchost.exe	1332	Services	0	28,936 K
svchost.exe	1384	Services	0	8,568 K
svchost.exe	1612	Services	0	3,628 K
svchost.exe	1620	Services	0	6,844 K
svchost.exe	1792	Services	0	6,908 K
svchost.exe	1864	Services	0	12,264 K
svchost.exe	1872	Services	0	7,728 K
svchost.exe	1880	Services	0	6,460 K
svchost.exe	1908	Services	0	6,348 K
svchost.exe	1992	Services	0	10,696 K
svchost.exe	1140	Services	0	14,384 K
svchost.exe	1136	Services	0	5,344 K
svchost.exe	1344	Services	0	13,616 K
svchost.exe	2192	Services	0	18,048 K
svchost.exe	2240	Services	0	5,604 K
svchost.exe	2264	Services	0	4,836 K
svchost.exe	2432	Services	0	4,216 K
svchost.exe	2504	Services	0	34,008 K
AppHelperCap.exe	2520	Services	0	13,392 K
NetworkCap.exe	2528	Services	0	5,680 K
DiagsCap.exe	2536	Services	0	5,268 K
svchost.exe	2696	Services	0	5,368 K
svchost.exe	2732	Services	0	7,120 K
TouchpointAnalyticsClient	2780	Services	0	29,524 K
svchost.exe	2900	Services	0	13,740 K
svchost.exe	2916	Services	0	4,604 K
svchost.exe	3044	Services	0	5,888 K
svchost.exe	2028	Services	0	6,108 K
svchost.exe	2716	Services	0	4,564 K

Administrator: Windows PowerShell

PS C:\WINDOWS\system32> get-process

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
160	11	2204	3728	3.13	4988	0	AdobeUpdateService
88	6	1644	4716	1.41	7216	0	AggregatorHost
242	15	3932	5028	0.81	5024	0	AGMService
446	18	7372	10940	10.84	5032	0	AGSService
454	19	9600	13372	20.23	2520	0	AppHelperCap
625	33	28252	45644	3.88	18384	24	ApplicationFrameHost
152	8	1624	6992	0.11	10668	0	AppVShNotify
205	11	6388	11828	55.83	19480	0	audiogd
3629	35	25904	30052	7.28	5380	24	backgroundTaskHost
250	28	7796	1956	0.20	8376	24	backgroundTaskHost
416	31	13608	29268	0.44	11064	24	backgroundTaskHost
249	26	11132	22680	0.14	24928	24	backgroundTaskHost
626	47	38516	1960	5.33	28008	24	backgroundTaskHost
383	22	70216	104676	316.30	824	24	brave
264	20	50784	82724	32.83	1952	24	brave
795	66	528660	245548	2,853.50	3064	24	brave
363	24	144304	119400	6,509.03	6480	24	brave
351	22	53688	75980	18.39	6712	24	brave
264	19	36100	63352	31.59	8004	24	brave
247	19	15632	28064	0.67	10408	24	brave
227	19	14036	29392	0.16	10512	24	brave
269	17	8328	19348	145.00	11816	24	brave
696	26	289944	316056	192.81	11852	24	brave
259	20	38128	70540	14.41	12636	24	brave
404	33	26548	43988	326.22	14136	24	brave
261	20	105648	91220	42.09	14156	24	brave
249	19	26984	50184	38.58	15156	24	brave
261	19	50560	65256	28.27	15240	24	brave
254	20	21508	45652	3.11	15984	24	brave
266	20	51496	83908	55.52	16716	24	brave
249	19	16988	35416	2.00	18560	24	brave
355	22	60556	98052	9.80	19376	24	brave
384	21	54336	74372	18.00	19488	24	brave
257	20	20880	49112	2.38	20300	24	brave
314	22	56856	62044	8.36	21732	24	brave
2404	76	346700	243680	1,048.56	21820	24	brave
256	19	15736	29380	1.23	22192	24	brave
249	19	17724	36568	2.16	23060	24	brave
249	19	17240	44260	0.17	23696	24	brave
190	14	7444	16428	7.72	24424	24	brave
249	19	20340	39736	2.34	26812	24	brave
204	14	33680	43120	13.72	27008	24	brave
249	19	16880	36160	2.03	28808	24	brave
326	10	2180	7320	0.31	29624	24	brave
238	14	14516	17288	5.89	29648	24	brave

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> wmic process get name,parentprocessid,processid
Name          ParentProcessId  ProcessId
System Idle Process      0            0
System          0            4
Secure System        4            136
Registry          4            208
smss.exe          4            636
csrss.exe         796           972
wininit.exe       796           664
services.exe       664           1056
LsaIso.exe        664           1076
lsass.exe         664           1084
svchost.exe       1056          1200
Fontdrvhost.exe   664           1228
WUDFHost.exe      1056          1284
svchost.exe       1056          1332
svchost.exe       1056          1384
svchost.exe       1056          1612
svchost.exe       1056          1620
svchost.exe       1056          1792
svchost.exe       1056          1864
svchost.exe       1056          1872
svchost.exe       1056          1880
svchost.exe       1056          1908
svchost.exe       1056          1992
svchost.exe       1056          1140
svchost.exe       1056          1136
svchost.exe       1056          1344
svchost.exe       1056          2192
svchost.exe       1056          2240
svchost.exe       1056          2264
svchost.exe       1056          2432
svchost.exe       1056          2504
AppHelperCap.exe  1056          2520
NetworkCap.exe    1056          2528
DiagsCap.exe     1056          2536
svchost.exe       1056          2696
svchost.exe       1056          2732
TouchpointAnalyticsClientService.exe 1056          2780
svchost.exe       1056          2900
svchost.exe       1056          2916
svchost.exe       1056          3044
svchost.exe       1056          2028
svchost.exe       1056          2716
svchost.exe       1056          3124
svchost.exe       1056          3316
svchost.exe       1056          3408
svchost.exe       1056          3480
svchost.exe       1056          3488
```

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> wmic process where 'ProcessID=1952' get CommandLine
CommandLine
"C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe" --type=renderer --extension-process --disable-client-side-phishing-detection --display-ca
pture-permissions-policy-allowed --origin-trial-public-key=bYUKPJOpNcxenVv72j4EmPUK7tr1PAC7SHn8jd9Mw3E=fMS4mp6buLQ/QMd+zJmzty/VQG81EUZqoCU04zorU= --brave_s
ession_token=13905483012887973638 --lang=en-US --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=14
--launch-time-ticks=911098193964 --mojo-platform-channel-handle=6016 --field-trial-handle=1860,8522214094988192311,5524789581673823291,131072 /prefetch:1
PS C:\WINDOWS\system32>
```

SERVICES

The screenshot shows the Windows Services snap-in window. The title bar reads "Services". The menu bar includes "File", "Action", "View", and "Help". Below the menu is a toolbar with icons for search, refresh, and navigation. The main area has two tabs: "Services (Local)" (selected) and "Services (Network)". A message box says "Select an item to view its description." A table lists various services with columns for Name, Description, Status, Startup Type, and Location. Most services are listed as "Running".

Name	Description	Status	Startup Type	Loc
ActiveX Installer (AxInstSV)	Provides Use...	Running	Manual	Loc
Adobe Genuine Monitor Ser...	Adobe Genu...	Running	Automatic	Loc
Adobe Genuine Software Int...	Adobe Genu...	Running	Automatic	Loc
AdobeUpdateService		Running	Automatic	Loc
Agent Activation Runtime_7...	Runtime for ...	Running	Manual	Loc
AllJoyn Router Service	Routes AllJo...		Manual (Trigg...	Loc
App Readiness	Gets apps re...		Manual	Loc
Application Identity	Determines ...		Manual (Trigg...	Loc
Application Information	Facilitates th...	Running	Manual (Trigg...	Loc
Application Layer Gateway S...	Provides sup...		Manual	Loc
AppX Deployment Service (A...	Provides infr...	Running	Manual (Trigg...	Loc
ASP.NET State Service	Provides sup...		Manual	Ne
Auto Time Zone Updater	Automaticall...		Disabled	Loc
AVCTP service	This is Audio...	Running	Manual (Trigg...	Loc
Background Intelligent Tran...	Transfers file...		Manual	Loc
Background Tasks Infrastruc...	Windows inf...	Running	Automatic	Loc
Base Filtering Engine	The Base Filt...	Running	Automatic	Loc
BattlEye Service			Manual	Loc
BitLocker Drive Encryption S...	BDESVC hos...		Manual (Trigg...	Loc
Block Level Backup Engine S...	The WBENGL...		Manual	Loc
Bluetooth Audio Gateway Se...	Service supp...		Manual (Trigg...	Loc

The screenshot shows a Command Prompt window. The title bar says "Command Prompt". The window displays the output of the "net start" command, listing numerous Windows services that are currently running. The services listed include Adobe Genuine Monitor Service, Adobe Genuine Software Integrity Service, AdobeUpdateService, Agent Activation Runtime_7ae38537, Application Information, AppX Deployment Service (AppXSVC), AVCTP service, Background Tasks Infrastructure Service, Base Filtering Engine, Capability Access Manager Service, CaptureService_7ae38537, Certificate Propagation, Clipboard User Service_7ae38537, CNG Key Isolation, COM+ Event System, Connected Devices Platform Service, Connected Devices Platform User Service_7ae38537, Connected User Experiences and Telemetry, Contact Data_7ae38537, CoreMessaging, Credential Manager, Cryptographic Services, Data Sharing Service, Data Usage, DbxSvc, DCOM Server Process Launcher, Delivery Optimization, Device Association Service, DevQuery Background Discovery Broker, DHCP Client, Diagnostic Policy Service, Diagnostic Service Host, Display Enhancement Service, Display Policy Service, Distributed Link Tracking Client, DNS Client, Docker Desktop Service, DtsApo4Service, ELAN Service, Encrypting File System (EFS), Function Discovery Provider Host, Function Discovery Resource Publication, and Geolocation Service.

```
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HARSHIT>net start
These Windows services are started:

Adobe Genuine Monitor Service
Adobe Genuine Software Integrity Service
AdobeUpdateService
Agent Activation Runtime_7ae38537
Application Information
AppX Deployment Service (AppXSVC)
AVCTP service
Background Tasks Infrastructure Service
Base Filtering Engine
Capability Access Manager Service
CaptureService_7ae38537
Certificate Propagation
Clipboard User Service_7ae38537
CNG Key Isolation
COM+ Event System
Connected Devices Platform Service
Connected Devices Platform User Service_7ae38537
Connected User Experiences and Telemetry
Contact Data_7ae38537
CoreMessaging
Credential Manager
Cryptographic Services
Data Sharing Service
Data Usage
DbxSvc
DCOM Server Process Launcher
Delivery Optimization
Device Association Service
DevQuery Background Discovery Broker
DHCP Client
Diagnostic Policy Service
Diagnostic Service Host
Display Enhancement Service
Display Policy Service
Distributed Link Tracking Client
DNS Client
Docker Desktop Service
DtsApo4Service
ELAN Service
Encrypting File System (EFS)
Function Discovery Provider Host
Function Discovery Resource Publication
Geolocation Service
```

Command Prompt

```
C:\Users\HARSHIT>sc query | more

SERVICE_NAME: AdobeUpdateService
DISPLAY_NAME: AdobeUpdateService
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 4   RUNNING
                           (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x0

SERVICE_NAME: AGMService
DISPLAY_NAME: Adobe Genuine Monitor Service
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 4   RUNNING
                           (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x0

SERVICE_NAME: AGSService
DISPLAY_NAME: Adobe Genuine Software Integrity Service
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 4   RUNNING
                           (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x0

SERVICE_NAME: Appinfo
DISPLAY_NAME: Application Information
    TYPE               : 30  WIN32
    STATE              : 4   RUNNING
                           (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x0

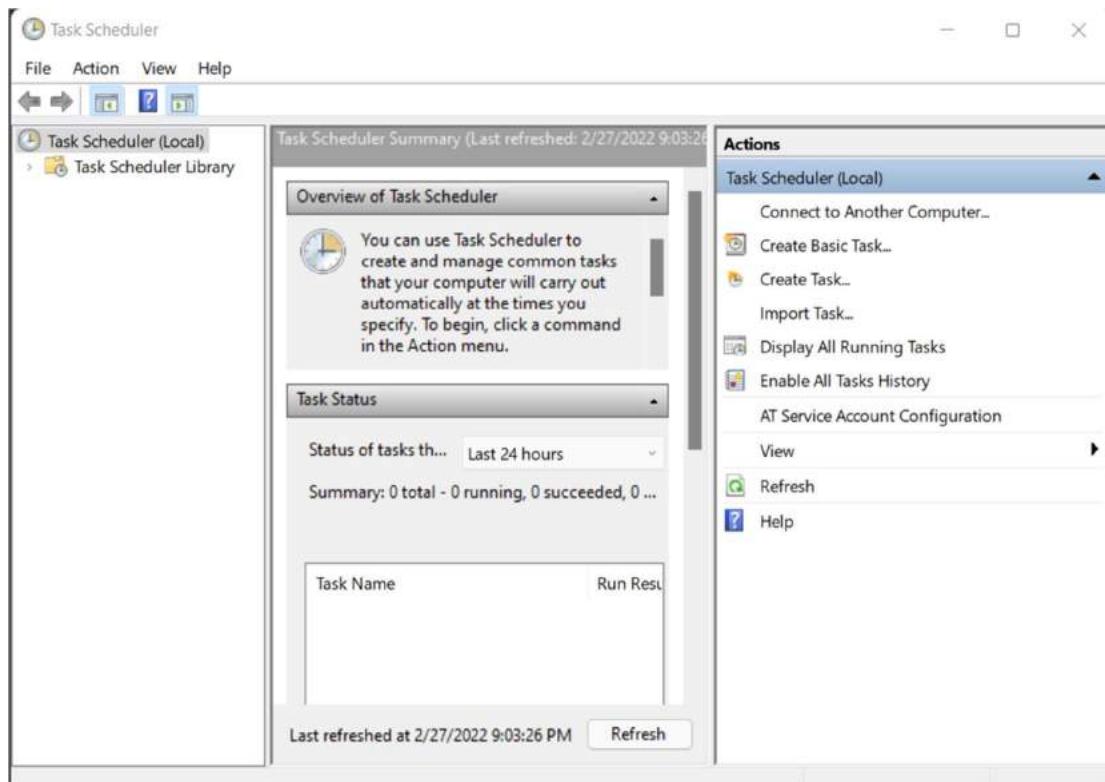
SERVICE_NAME: AppXSVC
DISPLAY_NAME: AppX Deployment Service (AppXSVC)
    TYPE               : 30  WIN32
    STATE              : 4   RUNNING
                           (NOT_STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
```

Command Prompt

```
C:\Users\HARSHIT>tasklist /svc

Image Name          PID Services
=====
System Idle Process      0 N/A
System                  4 N/A
Secure System            136 N/A
Registry                 208 N/A
smss.exe                636 N/A
csrss.exe                972 N/A
wininit.exe               664 N/A
services.exe              1056 N/A
LsaIso.exe                1076 N/A
Tsass.exe                1084 EFS, KeyIso, SamSs, VaultSvc
svchost.exe              1200 BrokerInfrastructure, DcomLaunch, PlugPlay,
                           Power, SystemEventsBroker
fontdrvhost.exe           1228 N/A
WUDFHost.exe              1284 N/A
svchost.exe                1332 RpcEptMapper, RpcSs
svchost.exe                1384 LSM
svchost.exe                1612 HvHost
svchost.exe                1620 TermService
svchost.exe                1792 NcbService
svchost.exe                1864 Schedule
svchost.exe                1872 ProfSvc
svchost.exe                1880 TimeBrokerSvc
svchost.exe                1908 DisplayEnhancementService
svchost.exe                1992 nsi
svchost.exe                1140 UserManager
svchost.exe                1136 TabletInputService
svchost.exe                1344 netprofm
svchost.exe                2192 camsvc
svchost.exe                2240 DevQueryBroker
svchost.exe                2264 CoreMessagingRegistrar
svchost.exe                2432 UmRdpService
svchost.exe                2504 Winmgmt
AppHelperCap.exe            2520 HPAppHelperCap
NetworkCap.exe              2528 HPNetworkCap
DiagsCap.exe                2536 HPDiagsCap
svchost.exe                2696 CertPropSvc
svchost.exe                2732 Dnscache
TouchpointAnalyticsClient    2780 HpTouchpointAnalyticsService
svchost.exe                2900 CryptSvc
svchost.exe                2916 LanmanWorkstation
svchost.exe                3044 Dhcp
svchost.exe                2028 HNS
svchost.exe                2716 DispBrokerDesktopSvc
svchost.exe                3124 SessionEnv
```

TASK SCHEDULER



```
C:\> Command Prompt
C:\> schtasks

Folder: \
TaskName          Next Run Time      Status
=====
AdobeGInvoker-1.0    2/27/2022 10:24:00 PM Ready
HPAudioSwitch        N/A                Running
JavaUpdateSched     N/A                Ready
LightstudioHelper   N/A                Running
MySQLNotifierTask   3/1/2022 9:11:00 PM Ready
NIUpdateServiceCheckTask 3/5/2022 5:49:00 PM Ready
NIUpdateServiceStartupTask N/A                Ready
NVBatteryBoostCheckOnLogon_{B2FE1952-0186-46C3-BAEC-N/A} N/A                Ready
NVDriverUpdateCheckDaily_{B2FE1952-0186-46C3-BAEC-N/A}    2/28/2022 12:25:07 PM Ready
NVIDIA GeForce Experience Selfupdate_{B2FE1952-0186-46C3-BAEC-N/A} N/A                Ready
NVNodeLauncher_{B2FE1952-0186-46C3-BAEC-N/A}             N/A                Ready
NvProfileUpdaterDaily_{B2FE1952-0186-46C3-BAEC-N/A}       2/28/2022 12:25:02 PM Ready
NvProfileUpdaterOnLogon_{B2FE1952-0186-46C3-BAEC-N/A}    N/A                Ready
NVtRep_CrashReport1_{B2FE1952-0186-46C3-BAEC-N/A}       2/28/2022 12:25:07 PM Ready
NVtRep_CrashReport2_{B2FE1952-0186-46C3-BAEC-N/A}       2/28/2022 6:25:07 PM Ready
NVtRep_CrashReport3_{B2FE1952-0186-46C3-BAEC-N/A}       2/28/2022 12:25:07 AM Ready
NVtRep_CrashReport4_{B2FE1952-0186-46C3-BAEC-N/A}       2/28/2022 6:25:07 AM Ready
OneDrive Reporting Task-S-1-5-21-3258786 2/27/2022 10:08:11 PM Ready
OneDrive Standalone Update Task-S-1-5-21 3/1/2022 12:39:31 AM Ready
Optimize Push Notification Data File-S-1 N/A                Disabled
User_Feed_Synchronization-{DF7C1BD4-683D} 2/28/2022 2:03:08 AM Ready

Folder: \Agent Activation Runtime
TaskName          Next Run Time      Status
=====
S-1-5-21-3258786884-371703526-3764206948 N/A                Disabled

Folder: \Hewlett-Packard
TaskName          Next Run Time      Status
=====
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Hewlett-Packard\HP Diagnostics
TaskName          Next Run Time      Status
=====
ABO              N/A                Ready
BatteryStatusError N/A                Ready
BatteryStatusTest 3/1/2022 8:00:00 AM Ready
BCF              N/A                Ready
BHM1             N/A                Ready
BHM2             N/A                Ready
LaunchUI         N/A                Ready
ShowUI           N/A                Ready
```

STARTUP

The screenshot shows the Windows Task Manager window with the 'Startup' tab selected. The table lists various startup items with columns for Name, Publisher, Status, and Startup impact.

Name	Publisher	Status	Startup impact
Adobe GC Invoker Utility	Adobe Systems, Incorp...	Disabled	None
Amazon Music	Amazon.com Services LLC	Disabled	None
Amazon Music Helper	Amazon.com Services LLC	Disabled	None
Brave Browser	Brave Software, Inc.	Disabled	None
CCXProcess.exe		Disabled	None
CCXProcess.exe		Disabled	None
Cortana	Microsoft Corporation	Enabled	Not measured
Creative Cloud Desktop	Adobe Inc.	Disabled	None
Docker Desktop	Docker Inc.	Disabled	None
Dropbox	Dropbox, Inc.	Disabled	None
EpicPen.exe	Tank Studios Ltd	Disabled	None
Figma Agent		Disabled	None
HpseuHostLauncher	HP Inc.	Enabled	Low

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> wmic startup get caption,command
Caption                               Command
OneDriveSetup                           C:\Windows\syswow64\OneDriveSetup.exe /thfirstsetup
OneDriveSetup                           C:\Windows\syswow64\OneDriveSetup.exe /thfirstsetup
Twitch                                Twitch.lnk
HPSEU_Host_Launcher                   C:\System.sav\util\HpseuHostLauncher.exe
OneDrive                               "C:\Users\HARSHIT\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
Steam                                  "C:\Program Files (x86)\Steam\steam.exe" -silent
Samsung DeX                            C:\Program Files (x86)\Samsung DeX\SamsungDeX.exe --autorun
CCXProcess                             "C:\Program Files (x86)\Adobe\Adobe Creative Cloud Experience\CCXProcess.exe"
com.squirrel.Teams.Teams              C:\Users\HARSHIT\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe" --process-start-args "--system-initiated"
Amazon Music Helper                     "C:\Users\HARSHIT\AppData\Local\Amazon Music\Amazon Music Helper.exe"
Amazon Music                           C:\Users\HARSHIT\AppData\Local\Amazon Music\Amazon Music.exe
Discord                                C:\Users\HARSHIT\AppData\Local\Discord\Update.exe --processStart Discord.exe
Figma Agent                            "C:\Users\HARSHIT\AppData\Local\FigmaAgent\figma_agent.exe"
MySQL Notifier                         C:\Program Files (x86)\MySQL\MySQL Notifier 1.1\MySQLNotifier.exe
Docker Desktop                         C:\Program Files\docker\docker\desktop.exe -Autostart
com.squirrel.slack.slack              "C:\Users\HARSHIT\AppData\Local\slack\slack.exe" --process-start-args --startup
GoogleChromeAutoLaunch_DE895F78ABEBF27A662AB411E57C477E  "C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe" --no-startup-window /prefetch:5
OneDriveSetup                           C:\Windows\syswow64\OneDrivesetup.exe /thfirstsetup
HPSEU_Host_Launcher                   C:\System.sav\util\HpseuHostLauncher.exe
SecurityHealth                         %windir%\system32\SecurityHealthsystray.exe
RtkAudUserService                     "C:\WINDOWS\System32\RtkAudUserService64.exe" -background
XboxStat                               "C:\Program Files\Microsoft Xbox 360 Accessories\XboxStat.exe" silentrun
AdobeGCInvoker-1.0                    "C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGCInvokerUtility.exe"
```

```

PS C:\WINDOWS\system32> Get-CimInstance Win32_StartupCommand | Select-Object Name, command, Location, User | Format-List

Name : OneDriveSetup
Command : C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup
Location : HKU\$-1-5-19\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User : NT AUTHORITY\LOCAL SERVICE

Name : OneDriveSetup
Command : C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup
Location : HKU\$-1-5-20\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User : NT AUTHORITY\NETWORK SERVICE

Name : Twitch
Command : Twitch.lnk
Location : Startup
User : LAPTOP-UE4331SF\HARSHIT

Name : HPSEU_Host_Launcher
Command : C:\System.sav\util\HpsseuHostLauncher.exe
Location : HKU\$-1-5-21-3258786884-371703526-3764206948-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User : LAPTOP-UE4331SF\HARSHIT

Name : OneDrive
Command : "C:\Users\HARSHIT\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
Location : HKU\$-1-5-21-3258786884-371703526-3764206948-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User : LAPTOP-UE4331SF\HARSHIT

Name : Steam
Command : "C:\Program Files (x86)\Steam\steam.exe" -silent
Location : HKU\$-1-5-21-3258786884-371703526-3764206948-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User : LAPTOP-UE4331SF\HARSHIT

Name : Samsung DeX
Command : C:\Program Files (x86)\Samsung\Samsung DeX\SamsungDeX.exe --autorun
Location : HKU\$-1-5-21-3258786884-371703526-3764206948-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User : LAPTOP-UE4331SF\HARSHIT

Name : CCXProcess
Command : "C:\Program Files (x86)\Adobe\Adobe Creative Cloud Experience\CCXProcess.exe"
Location : HKU\$-1-5-21-3258786884-371703526-3764206948-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User : LAPTOP-UE4331SF\HARSHIT

Name : com.squirrel.Teams.Teams
Command : C:\Users\HARSHIT\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe" --process-start-args "--system-initiated"
Location : HKU\$-1-5-21-3258786884-371703526-3764206948-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
User : LAPTOP-UE4331SF\HARSHIT

Name : Amazon Music Helper

```

REGISTRY EDITOR

The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under 'Computer\HKEY_CURRENT_USER\Console'. The right pane shows a table with columns 'Name', 'Type', and 'Data' for each entry. The table includes the following entries:

Name	Type	Data
(Default)	REG_SZ	(value not set)
ColorTable00	REG_DWORD	0x00000000 (0)
ColorTable01	REG_DWORD	0x00800000 (8388608)
ColorTable02	REG_DWORD	0x00000800 (32768)
ColorTable03	REG_DWORD	0x00808000 (8421376)
ColorTable04	REG_DWORD	0x00000080 (128)
ColorTable05	REG_DWORD	0x00800080 (8388736)
ColorTable06	REG_DWORD	0x00000800 (32896)
ColorTable07	REG_DWORD	0x00c0c0c0 (12632256)
ColorTable08	REG_DWORD	0x00808080 (8421504)
ColorTable09	REG_DWORD	0x00ff0000 (16711680)
ColorTable10	REG_DWORD	0x0000ff00 (65280)
ColorTable11	REG_DWORD	0x00ffff00 (16776960)
ColorTable12	REG_DWORD	0x000000ff (255)
ColorTable13	REG_DWORD	0x00ff00ff (16711935)
ColorTable14	REG_DWORD	0x0000ffff (65535)
ColorTable15	REG_DWORD	0x00ffffff (16777215)
CtrlKeyShortcuts...	REG_DWORD	0x00000000 (0)
CurrentPage	REG_DWORD	0x00000003 (3)
CursorColor	REG_DWORD	0xffffffff (4294967295)
CursorSize	REG_DWORD	0x00000019 (25)
CursorType	REG_DWORD	0x00000000 (0)
DefaultBackground...	REG_DWORD	0xffffffff (4294967295)
DefaultForeground...	REG_DWORD	0xffffffff (4294967295)
EnableColorSele...	REG_DWORD	0x00000000 (0)
ExtendedEditKey...	REG_DWORD	0x00000001 (1)

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SecurityHealth    REG_EXPAND_SZ    %windir%\system32\SecurityHealthSystray.exe
RtkAudUService    REG_SZ    "C:\WINDOWS\System32\RtkAudUService64.exe" -background
XboxStat    REG_SZ    "C:\Program Files\Microsoft Xbox 360 Accessories\XboxStat.exe" silentrun
AdobeGCInvoker-1.0    REG_SZ    "C:\Program Files (x86)\Common Files\Adobe\AdobeGCCClient\AGCInvokerUtility.exe"
PentabletService    REG_SZ    C:\Program Files\Pentablet\PentabletService.exe

PS C:\WINDOWS\system32>
```

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> reg query HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HPSEU_Host_Launcher    REG_SZ    C:\System.sav\util\HpseuHostLauncher.exe
OneDrive    REG_SZ    "C:\Users\HARSHIT\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
Steam    REG_SZ    "C:\Program Files (x86)\Steam\steam.exe" -silent
Samsung DeX    REG_SZ    C:\Program Files (x86)\Samsung\Samsung DeX\SamsungDeX.exe --autorun
CCXProcess    REG_SZ    "C:\Program Files (x86)\Adobe\Adobe Creative Cloud Experience\CCXProcess.exe"
com.squirrel.Teams.Teams    REG_SZ    C:\Users\HARSHIT\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe" --process-start-args "--system-initiated"
Amazon Music Helper    REG_SZ    "C:\Users\HARSHIT\AppData\Local\Amazon Music\Amazon Music Helper.exe"
Amazon Music    REG_SZ    C:\Users\HARSHIT\AppData\Local\Amazon Music\Amazon Music.exe
Discord    REG_SZ    C:\Users\HARSHIT\AppData\Local\Discord\Update.exe --processStart Discord.exe
Figma Agent    REG_SZ    "C:\Users\HARSHIT\AppData\Local\FigmaAgent\figma_agent.exe"
MySQL Notifier    REG_SZ    C:\Program Files (x86)\MySQL\MySQL Notifier 1.1\MySQLNotifier.exe
Docker Desktop    REG_SZ    C:\Program Files\Docker\Dockers\Dockers.exe -Autostart
com.squirrel.slack.slack    REG_SZ    "C:\Users\HARSHIT\AppData\Local\slack\slack.exe" --process-start-args --startup
GoogleChromeAutoLaunch_DE895F7B1BEBBF27A662AB411E57C477E    REG_SZ    "C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe" --no-startup-win
dow /prefetch:5

PS C:\WINDOWS\system32>
```

NETWORK [TCP and UDP]

```
Command Prompt
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HARSHIT>netstat -ano

Active Connections

Proto  Local Address          Foreign Address        State      PID
TCP    0.0.0.0:135            0.0.0.0:0             LISTENING  1332
TCP    0.0.0.0:445            0.0.0.0:0             LISTENING  4
TCP    0.0.0.0:902            0.0.0.0:0             LISTENING  5444
TCP    0.0.0.0:912            0.0.0.0:0             LISTENING  5444
TCP    0.0.0.0:2869           0.0.0.0:0             LISTENING  4
TCP    0.0.0.0:3306           0.0.0.0:0             LISTENING  6956
TCP    0.0.0.0:5040           0.0.0.0:0             LISTENING  2728
TCP    0.0.0.0:5357           0.0.0.0:0             LISTENING  4
TCP    0.0.0.0:5432           0.0.0.0:0             LISTENING  7284
TCP    0.0.0.0:27036          0.0.0.0:0             LISTENING  5840
TCP    0.0.0.0:33060          0.0.0.0:0             LISTENING  6956
TCP    0.0.0.0:49664          0.0.0.0:0             LISTENING  1084
TCP    0.0.0.0:49665          0.0.0.0:0             LISTENING  664
TCP    0.0.0.0:49666          0.0.0.0:0             LISTENING  1864
TCP    0.0.0.0:49667          0.0.0.0:0             LISTENING  3124
TCP    0.0.0.0:49668          0.0.0.0:0             LISTENING  3520
TCP    0.0.0.0:49669          0.0.0.0:0             LISTENING  4852
TCP    0.0.0.0:49676          0.0.0.0:0             LISTENING  1056
TCP    127.0.0.1:5939          0.0.0.0:0             LISTENING  5476
TCP    127.0.0.1:27017         0.0.0.0:0             LISTENING  5112
TCP    127.0.0.1:27060         0.0.0.0:0             LISTENING  5840
TCP    127.0.0.1:49672         127.0.0.1:49673        ESTABLISHED 6956
TCP    127.0.0.1:49673         127.0.0.1:49672        ESTABLISHED 6956
TCP    127.0.0.1:49674         127.0.0.1:49675        ESTABLISHED 6956
TCP    127.0.0.1:49675         127.0.0.1:49674        ESTABLISHED 6956
TCP    127.0.0.1:50911          0.0.0.0:0             LISTENING  5316
TCP    127.0.0.1:50912          0.0.0.0:0             LISTENING  5304
TCP    127.0.0.1:60797          127.0.0.1:65001        ESTABLISHED 5080
TCP    127.0.0.1:60863          0.0.0.0:0             LISTENING  26040
TCP    127.0.0.1:60863          127.0.0.1:60885        ESTABLISHED 26040
TCP    127.0.0.1:60885          127.0.0.1:60863        ESTABLISHED 1744
TCP    127.0.0.1:65001          0.0.0.0:0             LISTENING  5080
TCP    127.0.0.1:65001          127.0.0.1:60797        ESTABLISHED 5080
TCP    192.168.1.6:139           0.0.0.0:0             LISTENING  4
TCP    192.168.1.6:51801          52.113.206.43:443      ESTABLISHED 24404
TCP    192.168.1.6:52123          117.18.237.29:80        CLOSE_WAIT  21052
TCP    192.168.1.6:52125          23.201.220.24:443       CLOSE_WAIT  21052
TCP    192.168.1.6:54645          103.10.124.164:27025      ESTABLISHED 5840
TCP    192.168.1.6:58051          20.198.162.76:443       ESTABLISHED 21956
TCP    192.168.1.6:58058          20.198.162.76:443       ESTABLISHED 1208
TCP    192.168.1.6:58353          23.215.196.10:443        CLOSE_WAIT  13604
```

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Get-NetTCPConnection -LocalAddress 192.168.1.6 | Sort-Object LocalPort
LocalAddress          LocalPort RemoteAddress           RemotePort State      AppliedSetting OwningProcess
-----          -----          -----           -----      -----      -----      -----
192.168.1.6            139     0.0.0.0                  0 Listen
192.168.1.6          51801    52.113.206.43        443 Established Internet 24404
192.168.1.6          52123    117.18.237.29        80 CloseWait Internet 21052
192.168.1.6          52125    23.201.220.24       443 CloseWait Internet 21052
192.168.1.6          54645    103.10.124.164      27025 Established Internet 5840
192.168.1.6          58051    20.198.162.76       443 Established Internet 21956
192.168.1.6          58058    20.198.162.76       443 Established Internet 1208
192.168.1.6          58353    23.215.196.10       443 CloseWait Internet 13604
192.168.1.6          58416    18.66.78.126        443 CloseWait Internet 28008
192.168.1.6          58417    117.18.237.29        80 CloseWait Internet 28008
192.168.1.6          58418    54.200.189.169      443 CloseWait Internet 28008
192.168.1.6          58600    20.198.162.78       443 Established Internet 20844
192.168.1.6          58876    52.114.44.84        443 Established Internet 20452
192.168.1.6          59431    54.239.36.69        443 Established Internet 14136
192.168.1.6          59478    199.232.253.229      443 Established Internet 14136
192.168.1.6          59499    18.66.85.28        443 Established Internet 14136
192.168.1.6          59500    142.250.194.197      443 Established Internet 14136
192.168.1.6          59501    52.114.133.48       443 Established Internet 24404
192.168.1.6          59502    52.114.133.48       443 Established Internet 24404
192.168.1.6          59503    52.113.194.132      443 Established Internet 24404
192.168.1.6          59504    13.107.3.254        443 Established Internet 11284
192.168.1.6          59505    204.79.197.200       443 Established Internet 11284
192.168.1.6          59506    117.18.232.200      443 Established Internet 11284
192.168.1.6          59507    13.107.128.254      443 Established Internet 11284
192.168.1.6          59508    52.109.56.48        443 Established Internet 11244
192.168.1.6          59509    204.79.197.222      443 Established Internet 11284
192.168.1.6          59511    23.15.34.108        80 Established Internet 2900
192.168.1.6          59512    23.15.34.108        80 Established Internet 2900
192.168.1.6          59513    23.15.34.108        80 Established Internet 2900
192.168.1.6          59539    52.218.136.1        443 CloseWait Internet 12784
192.168.1.6          60786    20.198.162.76       443 Established Internet 5736

PS C:\WINDOWS\system32>
```

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> net view \\127.0.0.1
There are no entries in the list.

PS C:\WINDOWS\system32>
```

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Get-SMBShare
Name  ScopeName Path          Description
----  -----   -----          -----
ADMIN$ *          C:\WINDOWS Remote Admin
C$    *          C:\          Default share
D$    *          D:\          Default share
IPC$  *          Remote IPC

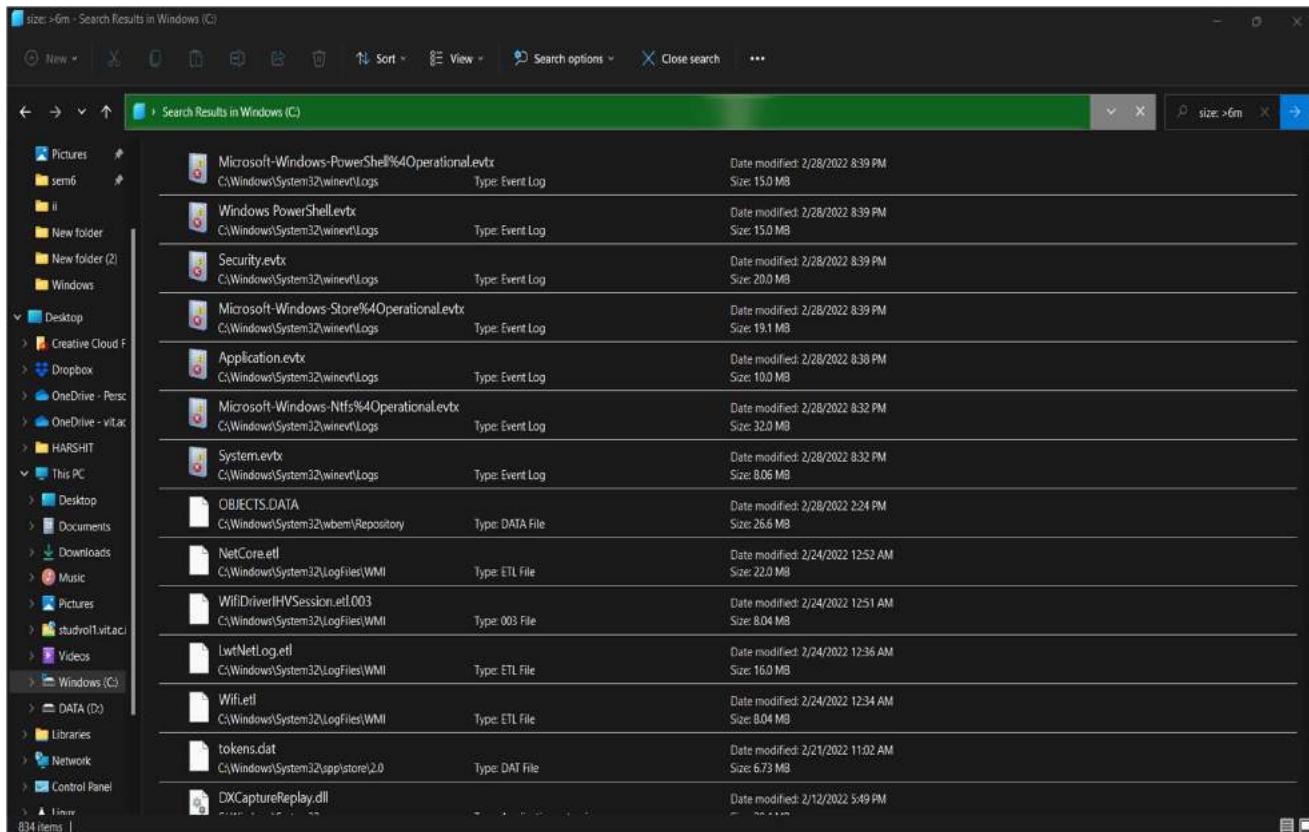
PS C:\WINDOWS\system32>
```

FILES and FILE SHARING:

```
PS C:\WINDOWS\system32> forfiles /D -10 /S /M *.exe /C "cmd /c echo @path"
"C:\WINDOWS\system32\agentactivationruntimestarter.exe"
"C:\WINDOWS\system32\AggregatorHost.exe"
"C:\WINDOWS\system32\aitstatic.exe"
"C:\WINDOWS\system32\alg.exe"
"C:\WINDOWS\system32\WebHostRegistrationVerifier.exe"
"C:\WINDOWS\system32\appidcertstorecheck.exe"
"C:\WINDOWS\system32\appidpolicyconverter.exe"
"C:\WINDOWS\system32\appidtel.exe"
"C:\WINDOWS\system32\ApplicationFrameHost.exe"
"C:\WINDOWS\system32\ApplyTrustOffline.exe"
"C:\WINDOWS\system32\ApproveChildRequest.exe"
"C:\WINDOWS\system32\appverif.exe"
"C:\WINDOWS\system32\ARP.EXE"
"C:\WINDOWS\system32\at.exe"
"C:\WINDOWS\system32\AtBroker.exe"
"C:\WINDOWS\system32\attrib.exe"
"C:\WINDOWS\system32\audiogd.exe"
"C:\WINDOWS\system32\auditpol.exe"
"C:\WINDOWS\system32\AuthHost.exe"
"C:\WINDOWS\system32\autochk.exe"
"C:\WINDOWS\system32\AxInstUI.exe"
"C:\WINDOWS\system32\backgroundTaskHost.exe"
"C:\WINDOWS\system32\BackgroundTransferHost.exe"
"C:\WINDOWS\system32\bash.exe"
"C:\WINDOWS\system32\bcdboot.exe"
"C:\WINDOWS\system32\bcdeedit.exe"
"C:\WINDOWS\system32\BdeUISrv.exe"
"C:\WINDOWS\system32\bdeunlock.exe"
"C:\WINDOWS\system32\BioIso.exe"
"C:\WINDOWS\system32\BitLockerDeviceEncryption.exe"
"C:\WINDOWS\system32\BitLockerWizardElev.exe"
"C:\WINDOWS\system32\bitsadmin.exe"
"C:\WINDOWS\system32\bootim.exe"
"C:\WINDOWS\system32\bootsect.exe"
"C:\WINDOWS\system32\bridgeunattend.exe"
"C:\WINDOWS\system32\browserexport.exe"
"C:\WINDOWS\system32\browser_broker.exe"
"C:\WINDOWS\system32\bthudtask.exe"
"C:\WINDOWS\system32\ByteCodeGenerator.exe"
"C:\WINDOWS\system32\cacls.exe"
"C:\WINDOWS\system32\calc.exe"
"C:\WINDOWS\system32\CameraSettingsUIHost.exe"
"C:\WINDOWS\system32\CastSrv.exe"
"C:\WINDOWS\system32\CertEnrollCtrl.exe"
"C:\WINDOWS\system32\certreq.exe"
"C:\WINDOWS\system32\certutil.exe"
"C:\WINDOWS\system32\changeapk.exe"
```

```
PS C:\WINDOWS\system32> forfiles /D -10 /S /M *.exe /C "cmd /c echo @ext @fname @fdate"
"exe" "agentactivationruntimestarter" 6/5/2021
"exe" "AggregatorHost" 11/4/2021
"exe" "aitstatic" 6/5/2021
"exe" "alg" 6/5/2021
"exe" "AppHostRegistrationVerifier" 6/5/2021
"exe" "appidcertstorecheck" 6/5/2021
"exe" "appidpolicyconverter" 6/5/2021
"exe" "appidtel" 11/4/2021
"exe" "ApplicationFrameHost" 6/5/2021
"exe" "ApplyTrustOffline" 2/11/2022
"exe" "ApproveChildRequest" 11/4/2021
"exe" "appverif" 12/2/2020
"EXE" "ARP" 6/5/2021
"exe" "at" 6/5/2021
"exe" "AtBroker" 6/5/2021
"exe" "attrib" 6/5/2021
"exe" "audiogd" 2/4/2022
"exe" "auditpol" 6/5/2021
"exe" "AuthHost" 6/5/2021
"exe" "autochk" 6/5/2021
"exe" "AxInstUI" 6/5/2021
"exe" "backgroundTaskHost" 6/5/2021
"exe" "BackgroundTransferHost" 6/5/2021
"exe" "bash" 12/12/2021
"exe" "bcdboot" 11/4/2021
"exe" "bcdedit" 12/17/2021
"exe" "BdeUISrv" 11/4/2021
"exe" "bdeunlock" 6/5/2021
"exe" "BioIso" 2/4/2022
"exe" "BitLockerDeviceEncryption" 6/5/2021
"exe" "BitLockerWizardElev" 6/5/2021
"exe" "bitsadmin" 6/5/2021
"exe" "bootim" 6/5/2021
"exe" "bootsect" 6/5/2021
"exe" "bridgeunattend" 6/5/2021
"exe" "browserexport" 6/5/2021
"exe" "browser_broker" 6/5/2021
"exe" "bthudtask" 6/5/2021
"exe" "ByteCodeGenerator" 11/4/2021
"exe" "cacls" 6/5/2021
"exe" "calc" 6/5/2021
"exe" "CameraSettingsUIHost" 6/5/2021
"exe" "CastSrv" 6/5/2021
"exe" "CertEnrollCtrl" 6/5/2021
"exe" "certreq" 1/13/2022
"exe" "certutil" 1/13/2022
"exe" "changepek" 6/5/2021
```

```
PS C:\WINDOWS\system32> forfiles /p c:/s /D -10  
"0409"  
"07409496-a423-4a3e-b620-2cfb01a9318d_HyperV-ComputeNetwork.dll"  
"0ae3b998-9a38-4b72-a4c4-06849441518d_Servicing-Stack.dll"  
"1028"  
"1029"  
"1031"  
"1033"  
"1036"  
"1040"  
"1041"  
"1042"  
"1045"  
"1046"  
"1049"  
"1055"  
"2052"  
"3082"  
"69fe178f-26e7-43a9-aa7d-2b616b672dde_eventLogservice.dll"  
"6bea57fb-8dfb-4177-9ae8-42e8b3529933_RuntimeDeviceInstall.dll"  
"@AdvancedKeySettingsNotification.png"  
"@AppHelpToast.png"  
"@AudioToastIcon.png"  
"@BackgroundAccessToastIcon.png"  
"@bitlockertoastimage.png"  
"@edptoastimage.png"  
"@EnrollmentToastIcon.png"  
"@language_notification_icon.png"  
"@optionalfeatures.png"  
"@StorageSenseToastIcon.png"  
"@VpnToastIcon.png"  
"@Windows-hello-V4.1.gif"  
"@WindowsHelloFaceToastIcon.png"  
"@WindowsUpdateToastIcon.contrast-black.png"  
"@WindowsUpdateToastIcon.contrast-white.png"  
"@WindowsUpdateToastIcon.png"  
"@WirelessDisplayToast.png"  
"@WLOGO_48x48.png"  
"aadauthhelper.dll"  
"aadcloudap.dll"  
"aadjcsp.dll"  
"aadtb.dll"  
"aadwamExtension.dll"  
"AarSvc.dll"  
"AboutSettingsHandlers.dll"  
"AboveLockAppHost.dll"  
"accessibilitycp1.dll"  
"accountaccessor.dll"
```



FIREWALL SETTINGS:

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> netsh firewall show config
Domain profile configuration:
-----
Operational mode          = Enable
Exception mode            = Enable
Multicast/broadcast response mode = Enable
Notification mode         = Enable

IMPORTANT: "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .

PS C:\WINDOWS\system32>
```

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> netsh advfirewall show currentprofile
Public Profile Settings:
-----
State                      ON
Firewall Policy             BlockInbound,AllowOutbound
LocalFirewallRules          N/A (GPO-store only)
LocalConSecRules             N/A (GPO-store only)
InboundUserNotification     Enable
RemoteManagement             Disable
UnicastResponseToMulticast  Enable

Logging:
LogAllowedConnections       Disable
LogDroppedConnections       Disable
FileName                   %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                4096
ok.
```

SESSIONS

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

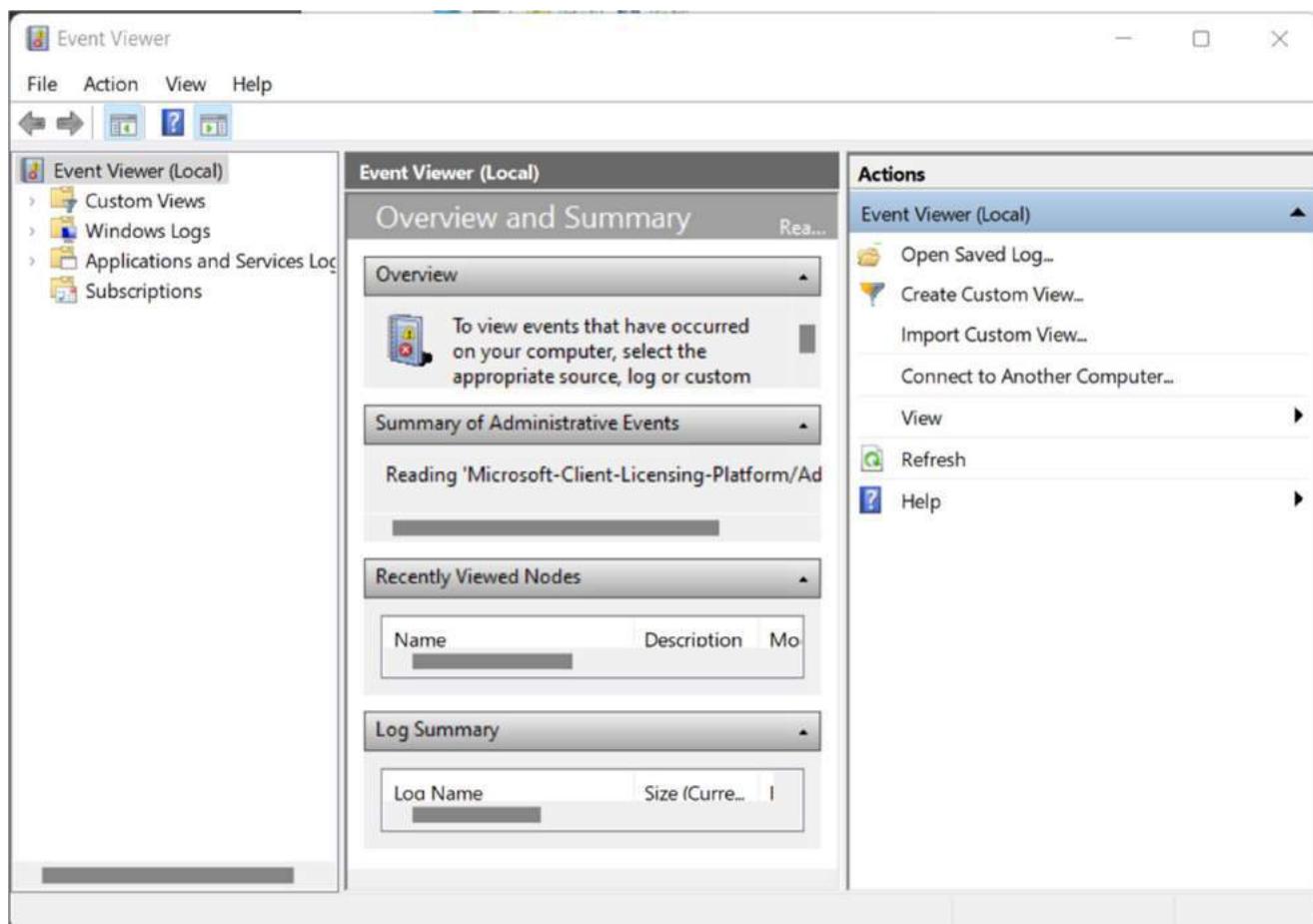
C:\WINDOWS\system32>net use
New connections will be remembered.

There are no entries in the list.

C:\WINDOWS\system32>net sessions
There are no entries in the list.

C:\WINDOWS\system32>
```

LOG ENTRIES



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Get-EventLog -List

Max(K) Retain OverflowAction
----- -----
20,480 0 OverwriteAsNeeded
20,480 0 OverwriteAsNeeded
512 7 OverwriteOlder
4,096 0 OverwriteAsNeeded
512 7 OverwriteOlder
512 7 OverwriteOlder
20,480 0 OverwriteAsNeeded
128 0 OverwriteAsNeeded
20,480 0 OverwriteAsNeeded
20,480 0 OverwriteAsNeeded
512 7 OverwriteOlder
15,360 0 OverwriteAsNeeded

Entries Log
----- --
16,461 Application
0 HardwareEvents
93 HP Analytics
88 HP Diagnostics
0 IntelAudioServiceLog
0 Internet Explorer
0 Key Management Service
5 OAlerts
33,720 Security
14,750 System
0 Visual Studio
14,720 Windows PowerShell

PS C:\WINDOWS\system32>
```

DEMONSTRATION OF MAN IN THE MIDDLE ATTACK
USING PENETRATION TESTING TOOLS

INFORMATION SECURITY MANAGEMENT (CSE3502)
J COMPONENT [F2/ L5+L6]

HARSHIT SRIVASTAVA
19BCE0382

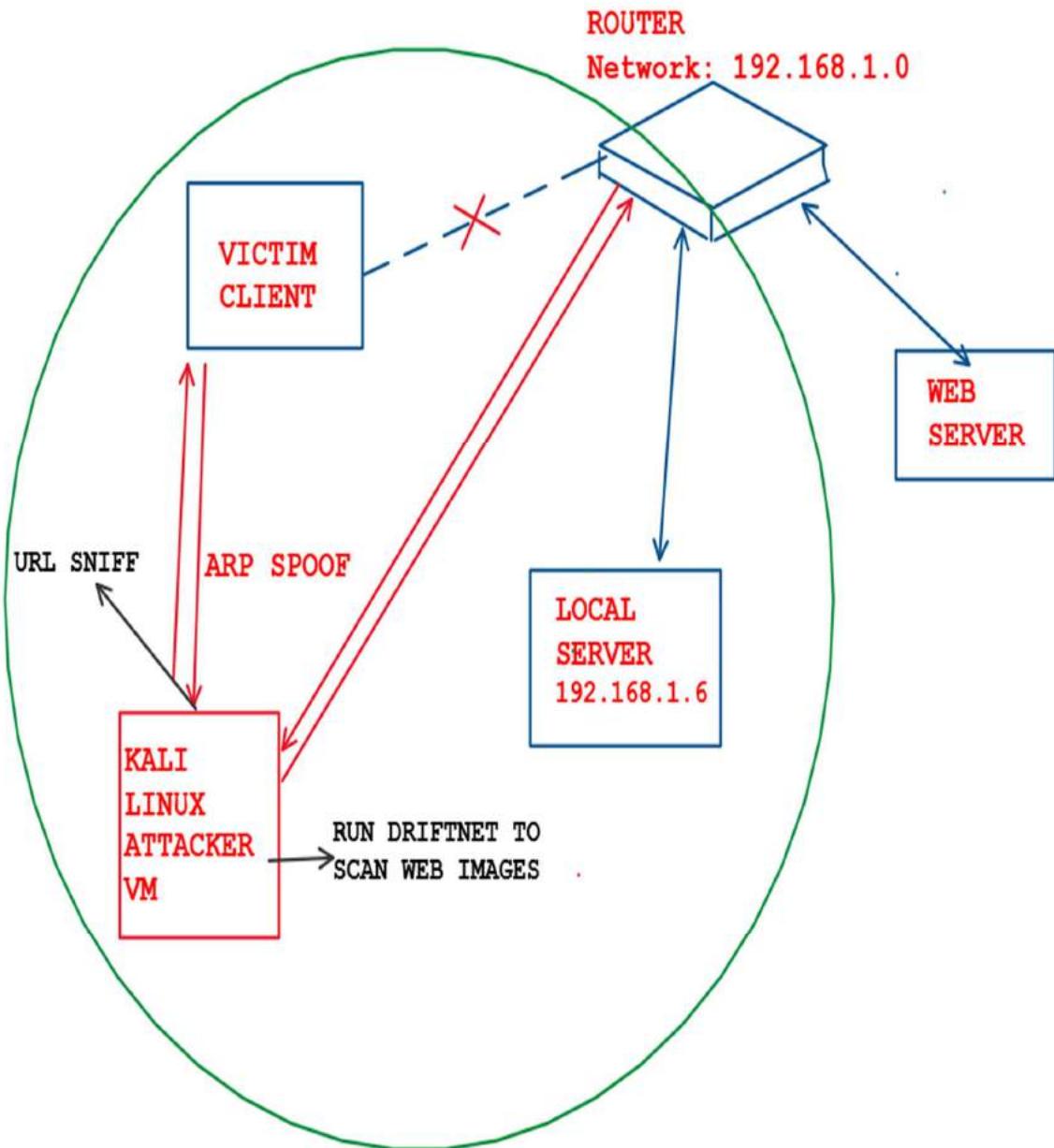
WINTER SEMESTER 2021-22

PROFESSOR: SIVA SHANMUGAM G

ARCHITECTURE DIAGRAM AND WORKING MODEL



Architecture Diagram:



Working Model:

A **Man in the Middle attack** occurs when a hacker inserts itself between the communications of a client and a server.

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol. MITM attacks can rely on ARP spoofing to intercept and modify traffic between victims.

Methodology:

Firstly, here we are using a Kali Linux machine as an attacker which is connected to the same network as that of Client which is our target/victim. In our Linux machine we would enable packet forwarding such that it acts like a router. So, while a client sends a request it would actually reach to the attacker machine and the request will be forwarded from there to the Router/ Internet Server.

In this scenario we will be using ARP spoofing. Here the packets in the LAN that are intended for the router by the client will be captured by our attack machine. This way we will be able to sniff all the packets and monitor the flow from victim/client to the router.

Similarly, it will be necessary for us to intercept packets from routers to the victim to be redirected via the attacker in case of a response. We will again use ARP spoofing for the same. With this, we have created a tunnel for all the

communications between the victim client and the router such that all incoming and outgoing data packets are routed via our attacker machine.

At this stage, our requirement is to sniff images from these packets which means reading the data packets. So, in order to see the images of websites that our victim visits we will use a tool known as driftnet. Driftnet is a program which listens to network traffic and picks out images from TCP streams it observes. Fun to run on a host which sees lots of web traffic. It is necessary to note that in case our attack machine is not forwarding the packets, the internet connection of the client will freeze thus the attack will be rendered useless.

Finally, in this process, we will use another tool known as urlsnarf, which is used to get information about the websites that our victim visits, it's a command line tool that sniffs HTTP requests in Common Log Format. It outputs all requested URLs sniffed from HTTP traffic in CLF (Common Log Format, used by almost all web servers), suitable for offline post-processing using web log analysis tool (analog, wwwstat, etc.).
