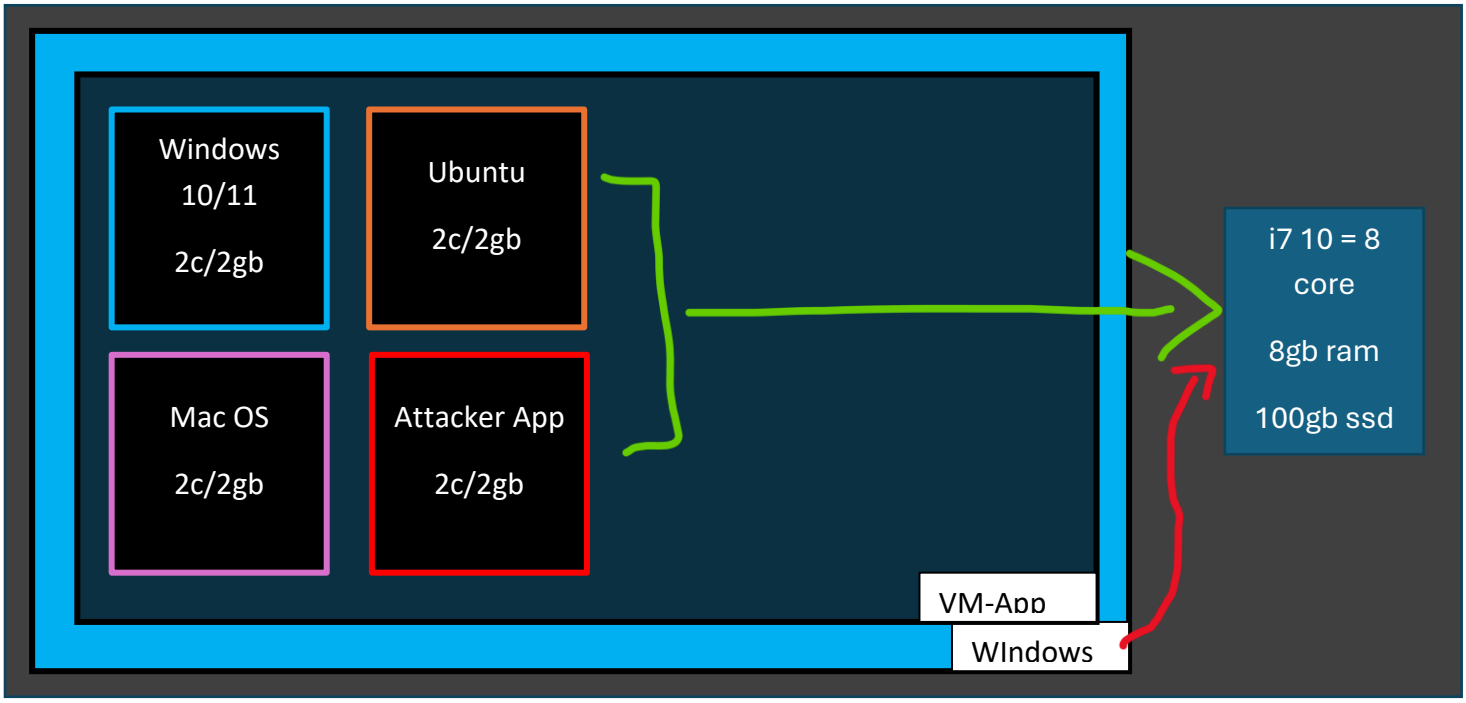
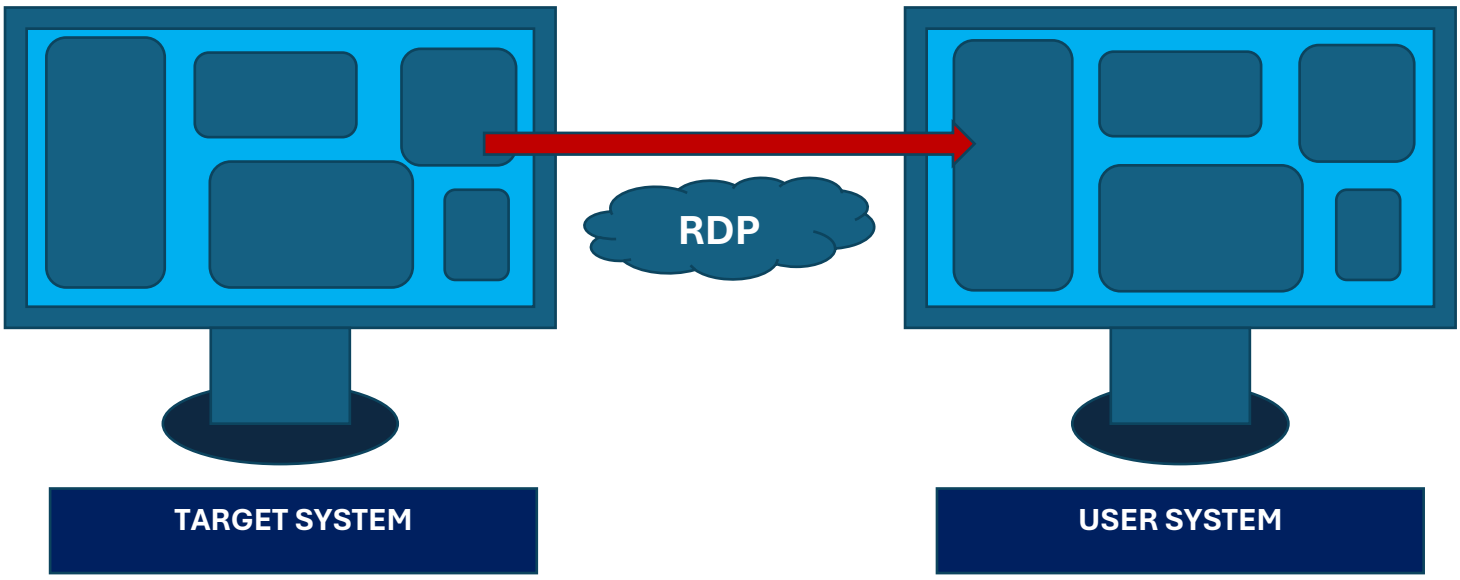
DAY 3

Virtualization: To run a virtual machine inside our host machine.



VDI (Virtual Drive Image): If an OS, say Kali Linux, is showing 80gb of hard disk space, it is not currently consuming the whole, rather just 20gb to 24gb of space. The rest of the space is 'Virtual'. It will scale automatically up to 80gb.

RDP (Remote Desktop Protocol): It is used to forecast/get the same GUI from the target desktop to our (user) desktop. It runs on port 3389 and is a TCP(Transmission Control Protocol) communication.



Microsoft AD: AD stands for Active Directory. It stores information about objects on the network and makes this information easy for administrators and users to find & use.

Static vs Dynamic IP address: Static IP address is constant whereas Dynamic IP address keeps changing.

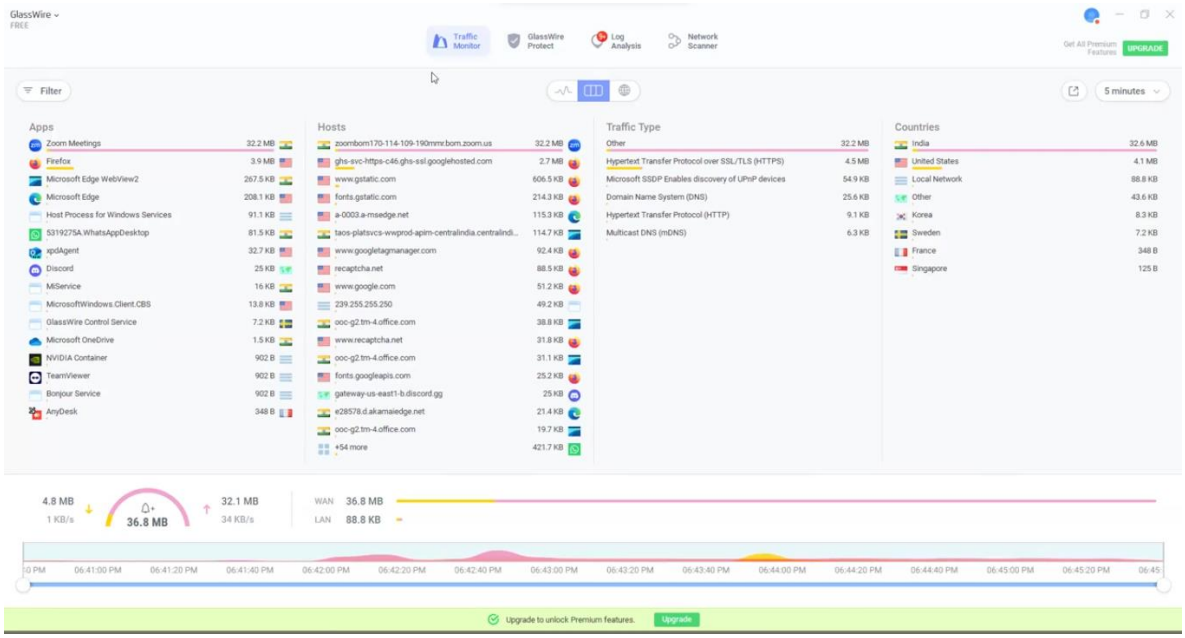
NGROK

- Used for port forwarding purpose
- Helps us to create a static domain which is dynamic, meaning when you run the command, it will generate a domain, but the domain life is only till you close the terminal as it will expire on terminal closure.

How to start, run and attack an SSH

- ls: command used to list the file content in a directory
- -lh: used to know the permissions and details of a file.
- pwd: prints current working directory
- Different types of terminals available:
    - sh: stands for 'Shell Terminal' and is the base/root of all.
    - bash: is one step advanced than shell terminal.

Glasswire Software: used to understand and protect our machine. It provides a detailed analysis view of all your network traffic, websites you visit, their country, etc. It can also be integrated with antivirus APIs like VirusTotal.



:- Glasswire Interface

To check the status of SSH: sudo systemctl status ssh

```
grey@sector21:~ $ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Tue 2024-07-23 17:14:54 IST; 1h 33min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 686 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 747 (sshd)
      Tasks: 1 (limit: 758)
        CPU: 851ms
     CGroup: /system.slice/ssh.service
             └─747 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jul 23 17:14:53 sector21 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jul 23 17:14:54 sector21 sshd[747]: Server listening on 0.0.0.0 port 22.
Jul 23 17:14:54 sector21 sshd[747]: Server listening on :: port 22.
Jul 23 17:14:54 sector21 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jul 23 18:13:37 sector21 sshd[1199]: error: kex_exchange_identification: client sent invalid protocol identifier "\033[48;5;
Jul 23 18:13:37 sector21 sshd[1199]: banner exchange: Connection from 127.0.0.1 port 38066: invalid format
Jul 23 18:46:55 sector21 sshd[1238]: Accepted password for grey from 192.168.0.101 port 25698 ssh2
Jul 23 18:46:55 sector21 sshd[1238]: pam_unix(sshd:session): session opened for user grey(uid=1000) by (uid=0)
Jul 23 18:46:55 sector21 sshd[1238]: pam_env(sshd:session): deprecated reading of user environment enabled
lines 1-21/21 (END)
```

If you see

, i.e, 0.0.0.0 in any network configuration, it means that they are ready to accept communication from any IP address to the port number mentioned after it.

To Configure SSH: install a package using command “sudo apt-get install openssh-server -y”

- sudo: command used for asking permission to the root user.
- apt-get: package manager holding all the packages.
- Name of service after ‘install’
- -y: used to agree to all conditions

Lolcat: mostly used to give a rainbow gradient colour to your terminal

- **Install lolcat:** sudo apt-get install lolcat -y

Remote Desktop Connection: Remote Desktop Connection (RDC) is a Microsoft technology that enables a local computer (client) to connect to and control a remote Windows PC (server) over a network or the Internet.