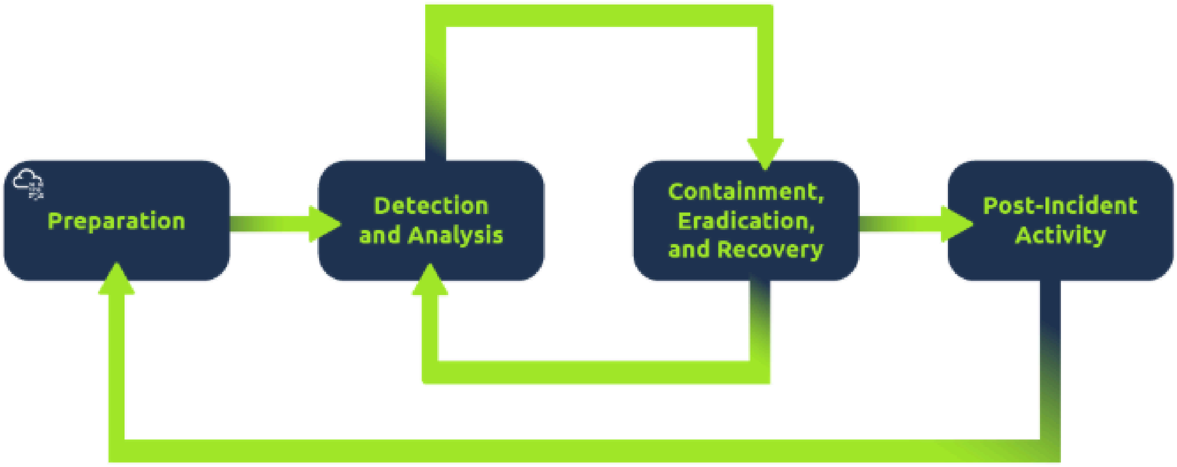
CYBERINSECURITY

firewall and intrusion prevention systems (IPS) are critical components of preventative security. Firewalls control what network traffic can go inside and what can leave the system or network. IPS blocks any network traffic that matches present rules and attack signatures.

Security operation center SOC a team of cybersec that monitors network and its system to detect malicious cyber events the main areas are ;
vulnerability, policy violation,unauthorized activity,network intrusion
threat intelligence,collects information to help company better prepare against potential adversaries, the purpose would be to achieve a threat informed defence

digital forensics and incident response DFIR
digital forensics analyzing evidence of an attack and its perpetrators and other areas such as intellectual property theft, cyber espionage and possession of unauthorized content, it focus on areas like: file system,system memory,system logs,network logs
Incident response data break or cyber attack, in some cases it can be something less critical , the phases here are : preparation,detection and analysis,containement eradication and recovery,post incident activity



Malware analysis stands for malicious software;programs,documents,and files you can save on disk or send over the network: it has many types like:
a virus that is a piece of code that attached itself to a program
trojan horse is a program that shows one desirable function but hides a malicious function underneath
ransomware is a malicious program that encrypts the user’s files
Malware analysis aimes to learn abt malicious programs using things like : static analysis works by inspecting the malicious program without running it this usually requires solid knowledge of assembly language

dynamic analysis works by running the malware in a controlled environment and monitoring its activities
SIEM security information and event management wich gathers security related information and events from various sources and presents them in one dashboard
There are many open-source databases out there, like AbuseIPDB, and Cisco Talos Intelligence, where you can perform a reputation and location check for the IP address.
security analyst are integral to constructing security measures across organisations to protect the company from attacks. Analysts explore and evaluate company networks to uncover actionable data and recommendations for engineers to develop preventative measures. This job role requires working with various stakeholders to gain an understanding of security requirements and the security landscape.

- Working with various stakeholders to analyse the cyber security throughout the company
- Compile ongoing reports about the safety of networks, documenting security issues and measures taken in response
- Develop security plans, incorporating research on new attack tools and trends, and measures needed across teams to maintain data security.

Security engineers develop and implement security solutions using threats and vulnerability data - often sourced from members of the security workforce. Security engineers work across circumventing a breadth of attacks, including web application attacks, network threats, and evolving trends and tactics. The ultimate goal is to retain and adopt security measures to mitigate the risk of attack and data loss.

Responsibilities

- Testing and screening security measures across software
- Monitor networks and reports to update systems and mitigate vulnerabilities
- Identify and implement systems needed for optimal security

Incident responders respond productively and efficiently to security breaches. Responsibilities include creating plans, policies, and protocols for organisations to enact during and following incidents. This is often a highly pressurised position with assessments and responses required in real-time, as attacks are unfolding. Incident response metrics include MTTD, MTTA, and MTTR - the meantime to detect, acknowledge, and recover (from attacks.) The aim is to achieve a swift and effective response, retain financial standing and avoid negative breach implications. Ultimately, incident responders protect the company's data, reputation, and financial standing from cyber attacks.

- Developing and adopting a thorough, actionable incident response plan

- Maintaining strong security best practices and supporting incident response measures
- Post-incident reporting and preparation for future attacks, considering learnings and adaptations to take from incidents

If you like to play detective, this might be the perfect job. If you are working as part of a law-enforcement department, you would be focused on collecting and analysing evidence to help solve crimes: charging the guilty and exonerating the innocent. On the other hand, if your work falls under defending a company's network, you will be using your forensic skills to analyse incidents, such as policy violations.

- Collect digital evidence while observing legal procedures
- Analyse digital evidence to find answers related to the case
- Document your findings and report on the case

A malware analyst's work involves analysing suspicious programs, discovering what they do and writing reports about their findings. A malware analyst is sometimes called a reverse-engineer as their core task revolves around converting compiled programs from machine language to readable code, usually in a low-level language. This work requires the malware analyst to have a strong programming background, especially in low-level languages such as assembly language and C language. The ultimate goal is to learn about all the activities that a malicious program carries out, find out how to detect it and report it.

Responsibilities

- Carry out static analysis of malicious programs, which entails reverse-engineering
- Conduct dynamic analysis of malware samples by observing their activities in a controlled environment
- Document and report all the findings

You may see **penetration testing** referred to as pentesting and ethical hacking. A penetration tester's job role is to test the security of the systems and software within a company - this is achieved through attempts to uncover flaws and vulnerabilities through systemised hacking. Penetration testers exploit these vulnerabilities to evaluate the risk in each instance. The company can then take these insights to rectify issues to prevent a real-world cyberattack.

Responsibilities

- Conduct tests on computer systems, networks, and web-based applications
- Perform security assessments, audits, and analyse policies

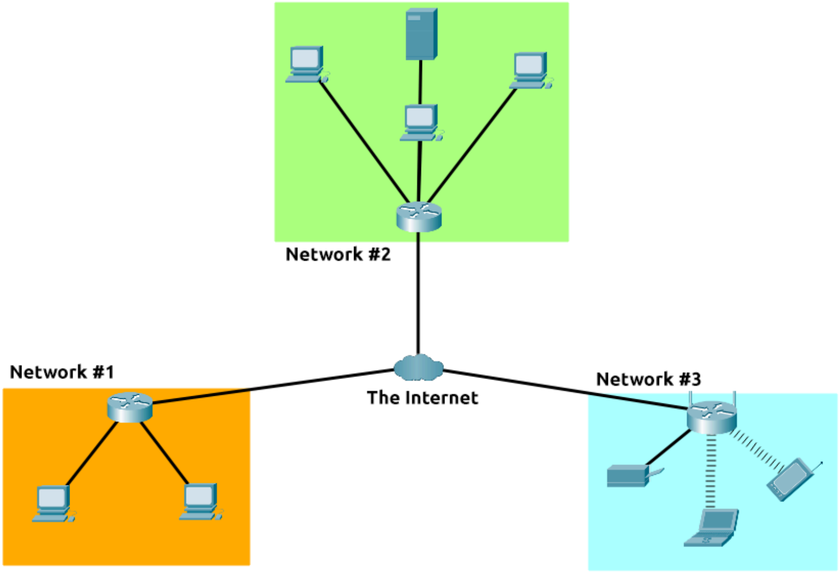
- Evaluate and report on insights, recommending actions for attack prevention

Red teamers share similarities to penetration testers, with a more targeted job role. Penetration testers look to uncover many vulnerabilities across systems to keep cyber-defence in good standing, whilst red teamers are enacted to test the company's detection and response capabilities. This job role requires imitating cyber criminals' actions, emulating malicious attacks, retaining access, and avoiding detection. Red team assessments can run for up to a month, typically by a team external to the company. They are often best suited to organisations with mature security programs in place.

Responsibilities

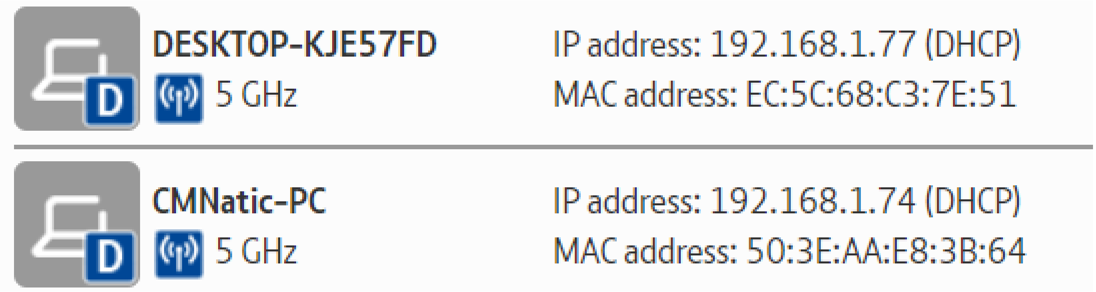
- Emulate the role of a threat actor to uncover exploitable vulnerabilities, maintain access and avoid detection
- Assess organisations' security controls, threat intelligence, and incident response procedures
- Evaluate and report on insights, with actionable data for companies to avoid real-world instances

a network is bench of connected devices, internet is a giant network with many many small networks connected between each other, the first iteration of the internet was within ARPANET project in the 1960s a project that was founded by the US defence departemeny and was the first documented network in action and up until 1989 that internet as we know was created by tim berners lee WWW,



you see how humans have two ways of identification a name and fingerprint, even if they change their name they can’t change their fingerprint and will always be associated to it? well the same for machines in a network, they have two means of identification with one being permeable: an IP address and a MAC (media access control) address(think of it as a serial number)

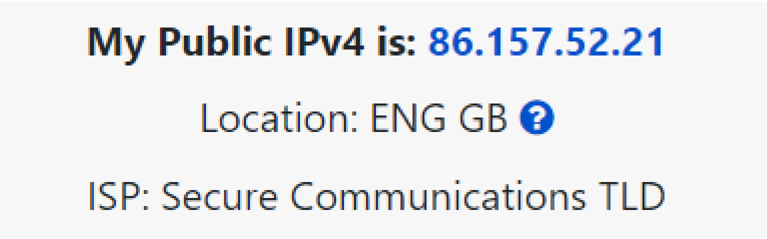
IP ADDRESS internet protocol: can be used as a way of identifying a host on a network for a period of time, it is divided into a four octets the value of each octet will summarise to be the IP address of the device within the network we can calculate it through IP addressing and subnetting, it is important to note that an IP address changes from one device to another but can not actively and simultaneously be more than one within the same network.since devices within a network can be public or private same thing goes for IP addresses,a public address is used to identify the device on the Internet, whereas a private address is used to identify a device amongst other devices.



DESKTOP-KJE57FD IP address: 192.168.1.77 (DHCP)
5 GHz MAC address: EC:5C:68:C3:7E:51

CMNatic-PC IP address: 192.168.1.74 (DHCP)
5 GHz MAC address: 50:3E:AA:E8:3B:64

These two devices will be able to use their private IP addresses to communicate with each other. However, any data sent to the Internet from either of these devices will be identified by the same public IP address. Public IP addresses are given by your **I**nternet **S**ervice **P**rovider (or **ISP**) at a monthly fee (your bill!)



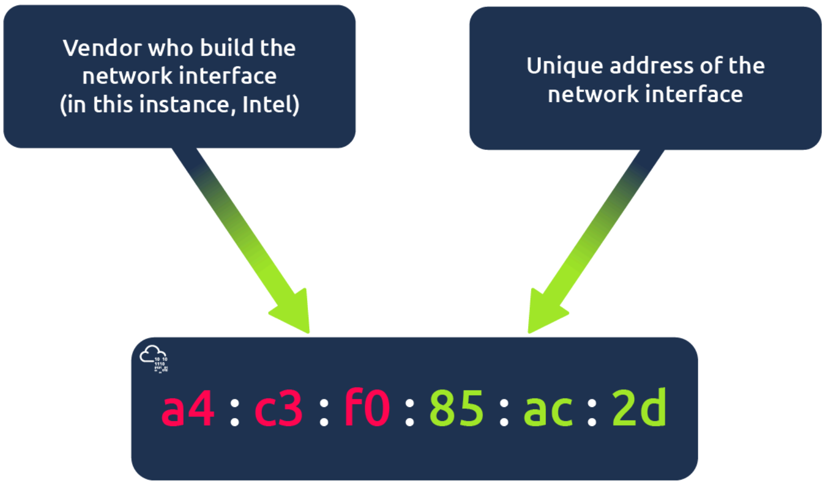
My Public IPv4 is: 86.157.52.21

Location: ENG GB

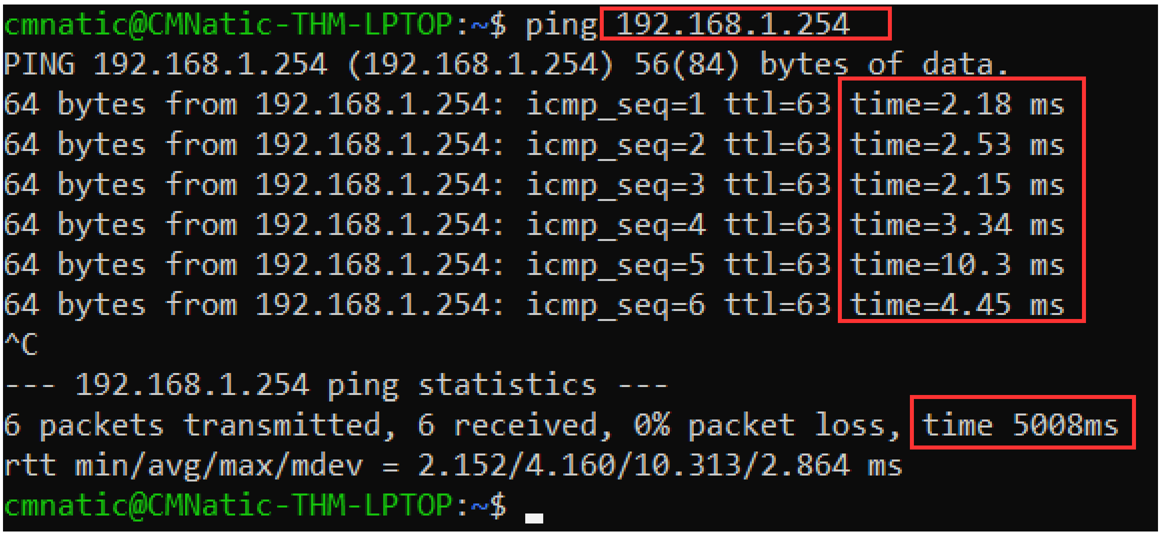
ISP: Secure Communications TLD

Mac addresson on a network every device would have a physical network interface, which is a microchip board on the device’s motherboard, this interface is assigned a unique address at the factory will building and called the mac address(media access control) it is represented in twelve hexadecimal character split into two and separated by colon *a4:c3:f0:85:ac:2d* in here the first six numbers represent the company that made the network interface and the other six are a unique number the process to fake amac address is called spoofing it occurs when a networked device pretends to identify as another using its mac address: take the following scenario :A firewall is configured to allow any communication going to and from the MAC address of the administrator. If a device were to pretend or "spoof" this MAC address, the firewall would now think that it is receiving communication from the administrator when it isn't.

Places such as cafes, coffee shops, and hotels alike often use MAC address control when using their "Guest "or "Public" Wi-Fi. This configuration could offer better services, i.e. a faster connection for a price if you are willing to pay the fee per device. The **interactive lab attached to this task** has been made to replicate this scenario!


Vendor who build the network interface (in this instance, Intel)
Unique address of the network interface
a4 : c3 : f0 : 85 : ac : 2d

PING uses ICMP internet control message protocol packet to determine the performance of a connection between devices, the ping measures the time taken by an ICMP packet travelling between devices, this measuring is done using ICMP echo packet and then IMCP's echo reply from the target device,it also can be performed against devices on a network, it comes installed on OS like linux or windows



```
cmnatic@CMNatic-THM-LPTOP:~$ ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=63 time=2.18 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=63 time=2.53 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=63 time=2.15 ms
64 bytes from 192.168.1.254: icmp_seq=4 ttl=63 time=3.34 ms
64 bytes from 192.168.1.254: icmp_seq=5 ttl=63 time=10.3 ms
64 bytes from 192.168.1.254: icmp_seq=6 ttl=63 time=4.45 ms
^C
--- 192.168.1.254 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 2.152/4.160/10.313/2.864 ms
cmnatic@CMNatic-THM-LPTOP:~$
```

```
user@thm:~$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=8.70 ms
```

```
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=7.33 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=9.67 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=8.31 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 8.132/9.428/10.957/1.057 ms
Flag: THM{I_PINGED_THE_SERVER}
```