This advent will be about firewalls, defensive strategies (honey pots), and incident analysis, using the Diamond Model.

**What is the Diamond Model?**

A security analysis framework that seasoned professionals use to unravel the mysteries of adversary operations and identify the elements used in an intrusion. It’s comprised of four core facets, interconnected to form a well-orchestrated blueprint of the attacker’s plans.

Identify the following:

1. Adversary
2. Victim
3. Infrastructure (hardware/software used)
4. Capability (skills, tools, techniques employed)

**Capability**

**Example**: phishing, exploiting vulnerabilities, social engineering, malware attacks, insider threat, DoS.

What is threat Hunting?

* Proactive & iterative process
* Search for signs of malicious activities or security weaknesses within organisation’s network or systems.
* Detect adversaries early in their attack lifecycle by conducting regular threat hunts.

What is Vulnerability Management?

* Identify, assess, prioritise, mitigate, and monitor vulnerabilities in an organisations systems and applications.
* Regular scans help identify weaknesses that adversaries could exploit.
* Integration with threat intelligence feeds, and periodic penetration testing further strengthen the organisation’s security posture.

This activity will use Uncomplicated Firewall (UFW) as its firewall of choice.

Check the status of the firewall.

Enable UFW.



**What are Honeypots?**

* A defensive piece of infrastructure.
* A mirage of vulnerabilities tempting attackers away from the true systems.
* Come in multiple types: software applications, servers, or entire networks.

**Question 1. Which security model is being used to analyse the breach and defence strategies?**

**Answer**: Diamond Model

**Question 2. Which defence capability is used to actively search for signs of malicious activities?**

**Answer**: Threat Hunting

**Question 3. What are our main two infrastructure focuses?**

**Answer**: Firewalls and Honeypots

**Question 4. Which firewall command is used to block traffic?**

**Answer**: Deny

**Question 5. There is a flag in one of the stories. Can you find it?**

A screen shot of a computer

Description automatically generatedThese are the rules that were set.

A screen shot of a computer

Description automatically generatedAfter a quick nmap scan I found the following ports open.

Now I just need to allow port 8090 to be open then I am good to go.

Now I changed the firewall to allow everything.

With a quick ‘control + F’ I found the flag.

A close up of words

Description automatically generated

**Answer**: THM{P0T$\_W@11S\_4\_S@N7@}

**More of the same work**: <https://tryhackme.com/room/networkdevicehardening>