**Eviction**

A hand holding a pencil

AI-generated content may be incorrect.

Sunny is a SOC analyst at E-corp, which manufactures rare earth metals for government and non-government clients. She receives a classified intelligence report that informs her that an APT group (APT28) might be trying to attack organizations similar to E-corp. To act on this intelligence, she must use the MITRE ATT&CK Navigator to identify the TTPs used by the APT group, to ensure it has not already intruded into the network, and to stop it if it has.

Please visit [this link](https://static-labs.tryhackme.cloud/sites/eviction/) to check out the MITRE ATT&CK Navigator layer for the APT group and answer the questions below.

**Q1. What is a technique used by the APT to both perform recon and gain initial access?**

APT28 commonly uses Spearphishing Attachments for both reconnaissance and initial access. They craft deceptive emails containing malicious attachments and send them to targeted employees, gaining access once the attachment is opened.

A screenshot of a computer

AI-generated content may be incorrect.

*Spearphishing link*

**Q2. Top of Form**

**Bottom of Form**

**Sunny identified that the APT might have moved forward from the recon phase. Which accounts might the APT compromise while developing resources?**

*A screenshot of a computer

AI-generated content may be incorrect.*

*Email accounts*

**Q3. Top of Form**

**Bottom of Form**

**E-corp has found that the APT might have gained initial access using social engineering to make the user execute code for the threat actor. Sunny wants to identify if the APT was also successful in execution. What two techniques of user execution should Sunny look out for? (Answer format: <technique 1> and <technique 2>)**

Under the Execution, we have the two techniques that Sunny is looking for.

*A screenshot of a computer

AI-generated content may be incorrect.*

*Malicious file and malicious link*

**Q4. Top of Form**

**Bottom of Form**

**If the above technique was successful, which scripting interpreters should Sunny search for to identify successful execution? (Answer format: <technique 1> and <technique 2>)**

We have the two scripting interpreters to identify successful execution.

*A screenshot of a computer

AI-generated content may be incorrect.*

*Powershell and Windows Command shell*

**Q5. Top of Form**

**Bottom of Form**

**While looking at the scripting interpreters identified in Q4, Sunny found some obfuscated scripts that changed the registry. Assuming these changes are for maintaining persistence, which registry keys should Sunny observe to track these changes?**

Under Persistence, the relevant registry keys that can be used to track changes are displayed.

*A screenshot of a computer

AI-generated content may be incorrect.*

*Registry run keys*

**Q6. Top of Form**

**Bottom of Form**

**Sunny identified that the APT executes system binaries to evade defences. Which system binary's execution should Sunny scrutinize for proxy execution?**

We're now in Defense Evasion. Sunny should closely examine rundll32.exe for proxy execution. Attackers use this binary to run malicious code and bypass security measures.

A screenshot of a computer

AI-generated content may be incorrect.

*Rundll32*

**Q7. Top of Form**

**Bottom of Form**

**Sunny identified tcpdump on one of the compromised hosts. Assuming this was placed there by the threat actor, which technique might the APT be using here for discovery?**

tcpdump suggests that network sniffing is being employed. This is a technique attackers use to capture network traffic and extract valuable information about the internal network.

*A screenshot of a computer

AI-generated content may be incorrect.*

*Network sniffing*

**Q8. Top of Form**

**Bottom of Form**

**It looks like the APT achieved lateral movement by exploiting remote services. Which remote services should Sunny observe to identify APT activity traces?**

*A screenshot of a computer

AI-generated content may be incorrect.*

*SMB/Windows Admin shares*

**Q9. Top of Form**

**Bottom of Form**

**It looked like the primary goal of the APT was to steal intellectual property from E-corp's information repositories. Which information repository can be the likely target of the APT?Top of Form**

*A screenshot of a computer

AI-generated content may be incorrect.*

*Sharepoint*

**Q10. Bottom of Form**

**Although the APT had collected the data, it could not connect to the C2 for data exfiltration. To thwart any attempts to do that, what types of proxy might the APT use? (Answer format: <technique 1> and <technique 2>)**

**A screenshot of a computer

AI-generated content may be incorrect.**

*external proxy and multi-hop proxy*

**Q11. Top of Form**

**Bottom of Form**

**Congratulations! You have helped Sunny successfully thwart the APT's nefarious designs by stopping it from achieving its goal of stealing the IP of E-corp.**

*No answer needed*