### **Tempest — TryHackME(Privilege Escalation & Actions on Objective)**

#### **TASK-9: Privilege Escalation**

**9.1. After discovering the privileges of the current user, the attacker then downloaded another binary to be used for privilege escalation. What is the name and the SHA256 hash of the binary?**

***Format: binary name,SHA256 hash***

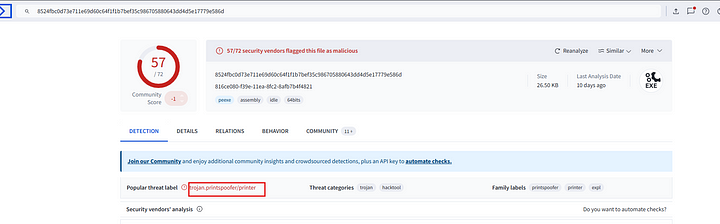
Following the trail of logs, we can see that the attacker had downloaded a file called spf.exe



**Answer:** spf.exe,8524FBC0D73E711E69D60C64F1F1B7BEF35C986705880643DD4D5E17779E586D

**9.2. Based on the SHA256 hash of the binary, what is the name of the tool used?**

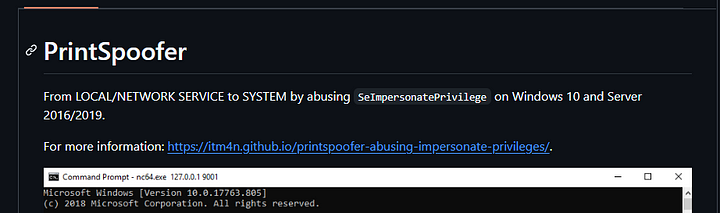
***Format: Answer in lowercase***

******

**Answer:** printspoofer

**9.3. The tool exploits a specific privilege owned by the user. What is the name of the privilege?**

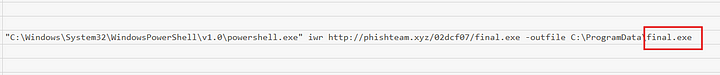
Searching the web for this malware, we find that it abuses the SeImpersonatePrivilege.



Answer: SeImpersonatePrivilege

**9.4. Then, the attacker executed the tool with another binary to establish a c2 connection. What is the name of the binary?**

Following the timeline of events, we can see another binary being downloaded.



Then they executed the previous binary using this binary.



**Answer:** final.exe

**9.5. The binary connects to a different port from the first c2 connection. What is the port used?**

Sysmon View will provide the answer to this.



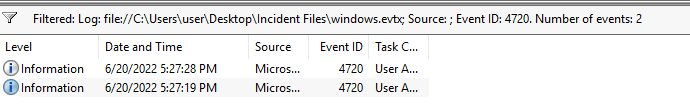
Answer: 8080

**Task-10: Actions on Objective**

**10.1. Upon achieving SYSTEM access, the attacker then created two users. What are the account names?**

**Format: Answer in alphabetical order — comma delimited**

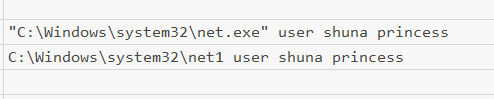
In the windows event logs, we can filter for the event ID 4720 to find out the new users created. Then in the details field we can find the usernames.



**Answer:** shion,shuna

**10.2. Prior to the successful creation of the accounts, the attacker executed commands that failed in the creation attempt. What is the missing option that made the attempt fail?**

Going back to the timeline viewer, if we follow the trail where the attacker tries to add new users.



As we can see the attacker has used the wrong syntax. The correct syntax is net user /add shuna

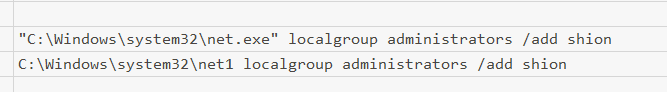
**Answer:** /add

**10.3. Based on windows event logs, the accounts were successfully created. What is the event ID that indicates the account creation activity?**

We already saw this in 10.1.

Answer: 4720

**10.4. The attacker added one of the accounts in the local administrator’s group. What is the command used by the attacker?**

****

**Answer:** net localgroup administrators /add shion

**10.5. Based on windows event logs, the account was successfully added to a sensitive group. What is the event ID that indicates the addition to a sensitive local group?**

**Answer:** 4732

**10.6. After the account creation, the attacker executed a technique to establish persistent administrative access. What is the command executed by the attacker to achieve this?**

**Format: Remove the double quotes from the log.**

****

Here the attacker created a service with the maliciuos binary which will run on startup.

Answer: C:\Windows\system32\sc.exe \\TEMPEST create TempestUpdate2 binpath= C:\ProgramData\final.exe start= auto.

This is the end of this room.