Game plan and score card

Game plan

1 Timelines

Stages / Start and End time	Start	End
2.0 Into and ice breaker	0:00	0:05
2.1 Plan	0:05	0:35
2.2 Prepare	0:35	1:35
2.3 Execute	1:35	1:45
2.4 Lessons leaned	1:45	1:50
2.5 Closing session	1:50	2:00

2 Stages

2.0 Intro and ice breaker

2.0.1 A few words about me

2.0.2 Prepare

- Check who has the prerequisites listed in the sessionize (that should have been communicated to you via email):
  - Windows
  - Visual Studio Community Edition
  - ngrok setup and able to start a server from their machine
- Check if there are people who have performed red team or purple team assessment and try to have one in each team.

2.0.3 Set the scene

- Rules of the workshop (i.e., rules of the game)
  - Stay true to ETHICAL
  - Do not do anything stupid
  - Have fun
- Key note
  - APT - Assumptions … Plan … Test

2.1 Plan

2.1.1 Ask to participant/s

- For your customer the “Big Whale” blockchain company (cryptocurrency financial services company) perform the following activities.
    - Prepare a list of tools and online resources that can be used for OSINT and Threat Intelligence
    - Perform a Threat Intelligence and draft an attack chain for a blockchain company

2.1.2 Key points

Open Threat Intelligence - MIPS	https://www.misp-project.org/
MITRE Enterprise attack matrix	https://attack.mitre.org/matrices/enterprise/
MITRE D3fend matrix	https://d3fend.mitre.org/
MITRE Mobile attack matrix	https://attack.mitre.org/matrices/mobile/

2.2 Prepare

2.2.1 Brief on the threat intelligence report

We at the “Big Whale” company have reviewed the threat intelligence report. We believe that threat actors will not be using attack chains similar to the proposed.

We want your simulation to be related to an insider threat. The attack chain is:

- Simulate attacks from internal threat actor →
- An internal threat actor that sends a Shortcut file via email. →
- The Shortcut file when opened will execute a DLL that will send the hostname of the device where it is executed to a server only.

Key notes:

- The DLL is to **only** send the hostname of the device where is executed to your server (i.e., the DLL has to do nothing else).
- I will help you with sending the Shortcut file from an internal email address that we have created for this simulation.

2.2.2 Ask to participant/s

- Create a Shortcut file that will execute your DLL.
- Create a DLL that will call your ngrok server reporting the hostname where the DLL is executed.
- Report to the “Big Whale” company CISO when your payload files are ready.

2.2.3 Key points

- A lot of online resources for malware development.
- Events such as the BSide Sofia 2024 “Malware Development 101 – From Zero to Non-Here”.

2.2.4 Hints

DLL

```
https://tekcookie.com/use-dll-files-in-powershell/
```

Start process in DLL

```
https://stackoverflow.com/questions/1255909/execute-cmd-command-from-code
```

Compile DLL

```
powershell -ep bypass> &"$env:windir\Microsoft.NET\Framework\
v4.0.30319/csc" /target:library C:\Users\admin_kali_pass\Desktop\
AMSI_exception\BSidesSofia\DLL\CSharp_CallServer\CallServer\
CallServer\Class1.cs
```

Shortcut

```
https://www.oreilly.com/library/view/windows-2000-quick/
0596000170/ch06s09.html

Properties -> Target-> C:\Windows\System32\cmd.exe /k powershell
your command
```

2.3 Execute

2.3.1 Ask to participant/s

- Upload your Shortcut file to VirusTotal. Take a screenshot of your file AV detection score and the uploaded file SHA256.
- Upload your DLL to the VirusTotal. Take a screenshot of your file AV detection score and the uploaded file SHA256.
- Brief the “Big Whale” company CISO what you have developed and show it reaches your ngrok server.
- Do you know a VirusTotal alternative that does not send files to AV providers?

2.3.2 Key points

Regarding your the payload files:

- Do they do only what you want them to do?

- Do they crash systems?
- Do they have ICOs that will be detected by security tools?

2.4 Lessons learned

2.4.1 Ask to participant/s

- Does the “Big Whale” company stated whether the DLL has to be saved to disk or not? Could this raise a difficult conversations if the CISO wanted to check whether the AV/EDR they have deployed detects saving DLLs to disk?
- What level of technical details about the attack chain should be approved?
- Does your attack chain do what the “Big Whale” company CISO wants?
- Do you know what your tools do?
- What are the benefits of using automation during a purple team?
- What are the drawbacks of using automation during a purple team?

2.4.2 Homework

- Generate a list of lessons learned that are applicable for the consulting firm.
- Generate a list of lessons learned that are applicable to the “Big Whale” company.
- Deploy free security tools to detect your payload files, these that you have created for the "Big Whale" CISO, and map their detection to a MITRE matrix.
- Execute the attack chain you have created in the Planning stage and fine tune your security tools to raise as many alerts as possible.
- Why you can choose to use a table during your purple team simulation (hint MITRE)?