Skills Assessment

Hunting For Stuxbot (Round 2)

Recently uncovered details shed light on the operational strategy of Stuxbot's newest iteration.

1. The newest iterations of Stuxbot are exploiting the `C:\Users\Public` directory as a conduit for deploying supplementary utilities.
2. The newest iterations of Stuxbot are utilizing registry run keys as a mechanism to ensure their sustained presence within the infected system.
3. The newest iterations of Stuxbot are utilizing PowerShell Remoting for lateral movement within the network and to gain access to domain controllers.

The Available Data

The cybersecurity strategy implemented is predicated on the utilization of the Elastic stack as a SIEM solution. Through the "Discover" functionality we can see logs from multiple sources. These sources include:

- `Windows audit logs` (categorized under the index pattern windows*)
- `System Monitor (Sysmon) logs` (also falling under the index pattern windows*, more about Sysmon here)
- `PowerShell logs` (indexed under windows* as well, more about PowerShell logs here)
- `Zeek logs`, a network security monitoring tool (classified under the index pattern zeek*)

The Tasks

Navigate to the bottom of this section and click on `Click here to spawn the target system!`

Now, navigate to `http://[Target IP]:5601`, click on the side navigation toggle, and click on "Discover". Then, click on the calendar icon, specify "last 15 years", and click on "Apply".

`Hunt 1`: Create a KQL query to hunt for "Lateral Tool Transfer" to `C:\Users\Public`. Enter the content of the `user.name` field in the document that is related to a transferred tool that starts with "r" as your answer.

`Hunt 2`: Create a KQL query to hunt for "Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder". Enter the content of the `registry.value` field in the document that is related to the first registry-based persistence action as your answer.

`Hunt 3`: Create a KQL query to hunt for "PowerShell Remoting for Lateral Movement". Enter the content of the `winlog.user.name` field in the document that is related to PowerShell remoting-based lateral movement towards DC1.

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

VPN Servers

Warning: Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 159ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

+ 2 Enter your answer for Hunt 1.

svc-sql1

Submit

+ 3 Enter your answer for Hunt 2.

LgvHsviAUVTsIN

Submit Hint

+ 3 Enter your answer for Hunt 3.

svc-sql1

Submit Hint

Previous

Finish