Skills Assessment

This module's skills assessment involves identifying malicious activity using Splunk and Zeek logs.

In many instances, the solution can be discovered by simply viewing the events in each index, as the number of events is limited. However, please take the time to refine your Splunk searches to achieve a better understanding.

Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, access the Splunk interface at https://[Target IP]:8000 and launch the Search & Reporting Splunk application to answer the questions below.

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 — 139ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Resources

Go to Questions

Table of Contents

Skills Assessment

My Workstation

OFFLINE

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!

+ 1 Use the "empire" index and the "bro:http:json" sourcetype. Identify beaconing activity by modifying the Splunk search of the "Detecting Beaconing Malware" section and enter the value of the "TimeInterval" field as your answer.

4.680851063829787

Submit

+ 1 Use the "printnightmare" index and the "bro:dce_rpc:json" sourcetype to create a Splunk search that will detect possible exploitation of the PrintNightmare vulnerability. Enter the IP included in the "id.orig_h" field as your answer.

192.168.1.149

Submit

+ 1 Use the "bloodhound_all_no_kerberos_sign" index and the "bro:dce_rpc:json" sourcetype to create a Splunk search that will detect possible BloodHound activity (https://www.lares.com/blog/active-directory-ad-attacks-enumeration-at-the-network-layer/). Enter the IP included in the "id.orig_h" field as your answer.

192.168.109.105

Submit

Previous

Finish