Guided Lab: Traffic Analysis Workflow

One of our fellow admins noticed a weird connection from Bob's host `IP = 172.16.10.90` when analyzing the baseline captures we have been gathering. He asked us to check it out and see what we think is happening.

Attempt to utilize the concepts from the Analysis Process sections to complete an analysis of the guided-analysis.zip provided in the optional resources and live traffic from the academy network. Once done, a guided answer key is included with the PCAP in the zip to check your work.

Tasks:

Task #1

`Connect to the live host for capture.`

`Connection Instructions`: Access to the lab environment to complete the following tasks will require the use of XfreeRDP to provide GUI access to the virtual machine so we can utilize Wireshark from within the environment.

We will be connecting to the Academy lab like normal utilizing your own VM with a HTB Academy VPN key or the Pwnbox built into the module section. You can start the FreeRDP client on the Pwnbox by typing the following into your shell once the target spawns:

Code: bash

```
xfreerdp /v:<target IP> /u:htb-student /p:HTB_@cademy_stdnt!
```

You can find the `target IP`, `Username`, and `Password` needed below:

- `Click below in the Questions section to spawn the target host and obtain an IP address.`
  - `IP ==`
  - `Username == htb-student`
  - `Password == HTB_@cademy_stdnt!`

Once connected, open Wireshark and begin capturing on interface ENS224.

Analysis

Follow this workflow template and examine the suspicious traffic. The goal is to determine what is happening with the host in question.

1. what is the issue?
    1. a brief summary of the issue.
2. define our scope and the goal (what are we looking for? which time period?)
    1. Scope: what are we looking for, where?
    2. when the issue started:
    3. supporting info: Files, data sources, anything helpful.
3. define our target(s) (net / host(s) / protocol)
    1. Target hosts: Network or address of hosts.
4. capture network traffic / read from previously captured PCAP.
    1. Perform actions as needed to analyze the traffic for signs of intrusion.

Cheat Sheet
Resources
? Go to Questions

Table of Contents

Introduction
Network Traffic Analysis
Networking Primer - Layers 1-4
Networking Primer - Layers 5-7

Analysis
The Analysis Process
Analysis in Practice

Tcpdump
Tcpdump Fundamentals
Capturing With Tcpdump (Fundamentals Labs)
Tcpdump Packet Filtering
Interrogating Network Traffic With Capture and Display Filters

Wireshark
Analysis with Wireshark
Familiarity With Wireshark
Wireshark Advanced Usage
Packet Inception, Dissecting Network Traffic With Wireshark
Guided Lab: Traffic Analysis Workflow
Decrypting RDP connections

My Workstation
OFFLINE
Start Instance
∞ / 1 spawns left

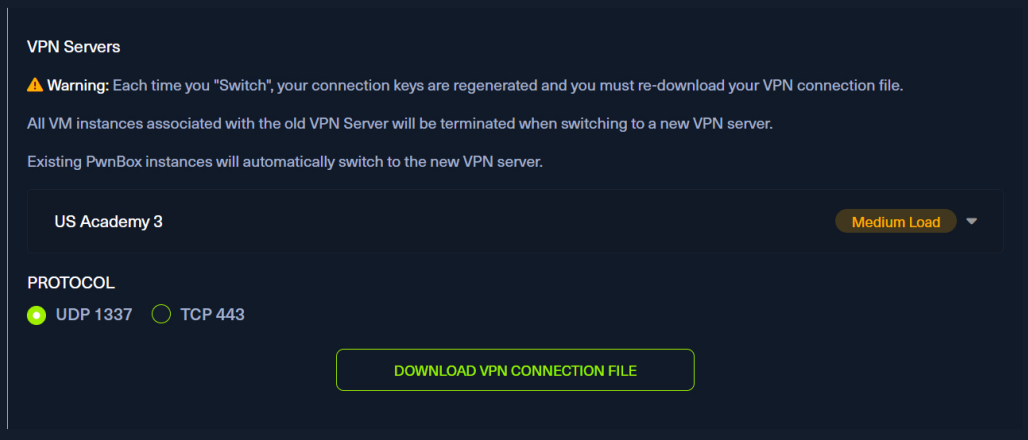
5. Identification of required network traffic components (filtering)
    1. once we have our traffic, filter out any traffic not necessary for this investigation to include; any traffic that matches our common baseline, and keep anything relevant to the scope of the investigation.
6. An understanding of captured network traffic
    1. Once we have filtered out the noise, it's time to dig for our targets. Start broad and close the circle around our scope.
7. note taking / mind mapping of the found results.
    1. Annotating everything we do, see, or find throughout the investigation is crucial. Ensure you are taking ample notes, including:
        - Timeframes we captured traffic during.
        - Suspicious hosts/ports within the network.
        - Conversations containing anything suspicious. (to include timestamps, and packet numbers, files, etc.)
8. summary of the analysis (what did we find?)
    1. Finally, summarize what has been found, explaining the relevant details so that superiors can decide to quarantine the affected hosts or perform a more critical incident response mission.
    2. Our analysis will affect decisions made, so it is essential to be as clear and concise as possible.

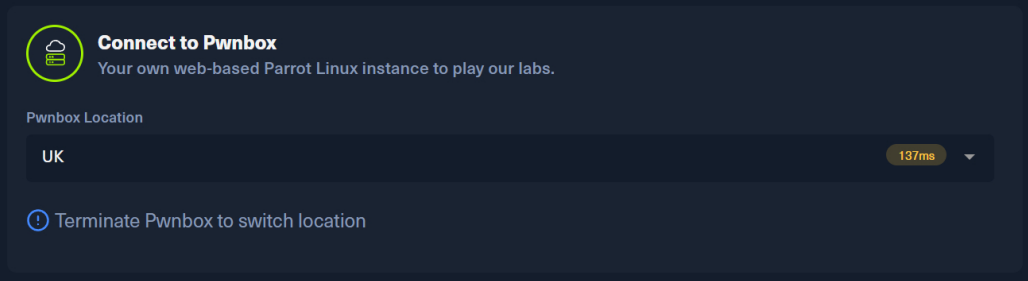
Complete an attempt on your own first to examine and follow the workflow, then look below for a guided walkthrough of the lab.

▶ **Click to show walkthrough**

Summary

After analyzing the actions taken, the IR team determined that The actor got lazy and decided to utilize a Netcat shell and directly interact with Bob's host while gathering more information. While doing so, he used RDP from Bob's host to another windows desktop in the environment to try and establish another foothold. Luckily, the IR team was able to capture some PCAP of the RDP traffic. Bob's host was quarantined, and incident response was initiated to determine what was taken and what other potential hosts were compromised. Great job spotting the intrusion.





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!

Cheat Sheet

Download VPN Connection File

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

RDP to with user "htb-student" and password "HTB_@cademy_stdnt!"

+ 1 What was the name of the new user created on mrb3n's host?

hacker

Submit Hint

+ 2 How many total packets were there in the Guided-analysis PCAP?

44

Submit Hint

+ 1 What was the suspicious port that was being used?

4444

Submit Hint

Previous Next

Mark Complete & Next