Skills Assessment - Zeek

Intrusion Detection With Zeek: Detecting Gootkit's SSL Certificate

PCAP source: https://www.malware-traffic-analysis.net/2016/07/08/index.html

Attack description and possible detection points: https://www.malware-traffic-analysis.net/2016/07/08/index.html <-- Focus on the SSL certificate parts.

`Neutrino`, a notorious exploit kit, and `Gootkit`, a potent banking trojan, collaborated in the past to perpetrate cyberattacks.

The `Neutrino` exploit kit opened the gate, and then `Gootkit` begun to communicate over the network using SSL/TLS encryption. It's within these encrypted communications that we encountered a particularly striking detail - the SSL certificates used by `Gootkit` contained the Common Name (`CN`) "`My Company Ltd.`".

Cybercriminals frequently employ self-signed or non-trusted CA issued certificates to foster encrypted communication. These certificates often feature bogus or generic details. In this case, the common name `My Company Ltd.` stands out as an anomaly we can use to identify this specific `Gootkit` infection delivered via the `Neutrino` exploit kit.

Review the previously referenced resource that discusses the network traces resulting from `Gootkit` communications, and then proceed to address the following question.

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 164ms ▾

ⓘ Terminate Pwnbox to switch location

? Go to Questions

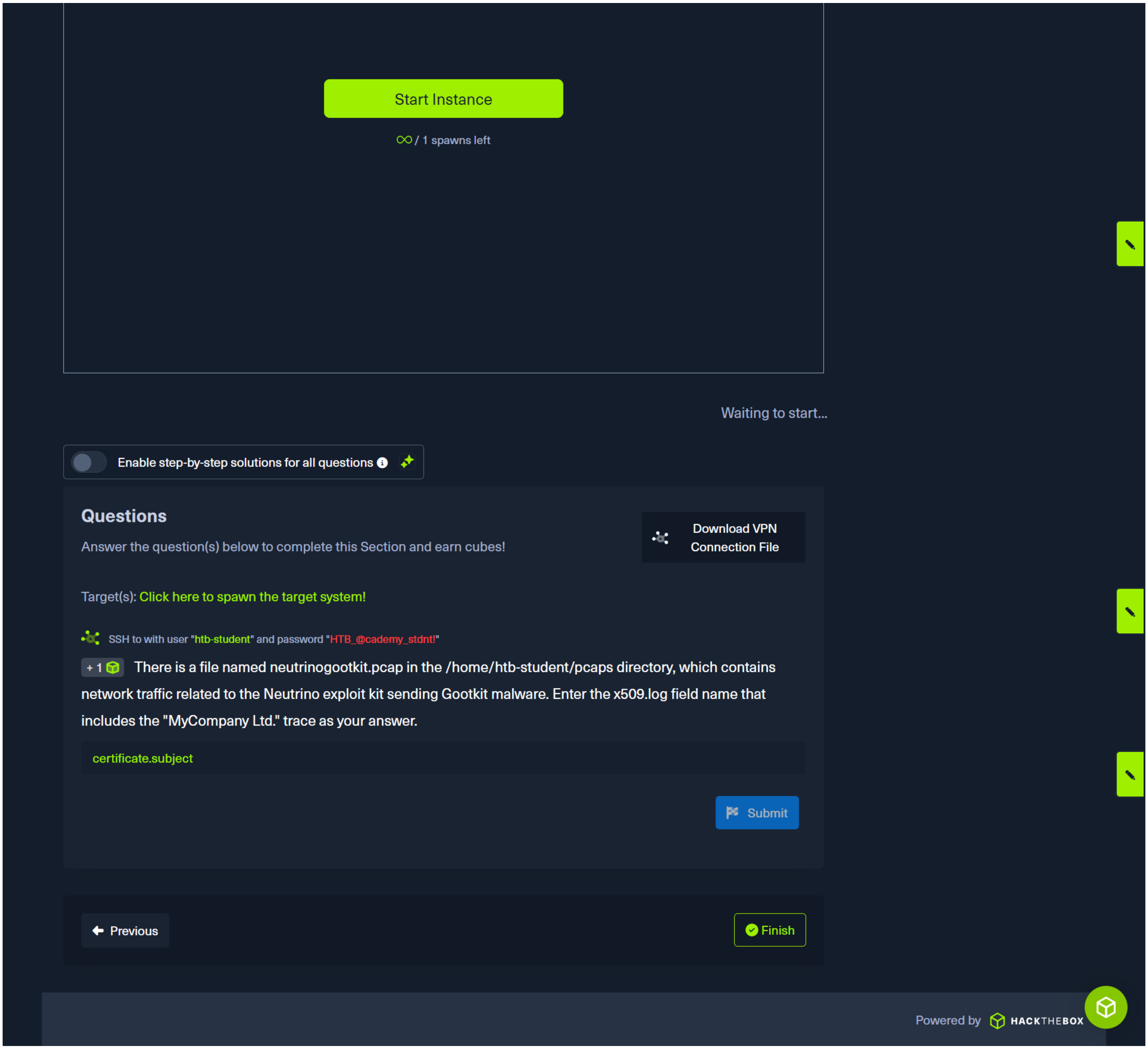
Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left



Questions

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

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

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

+ 1 There is a file named neutrinogootkit.pcap in the /home/htb-student/pcaps directory, which contains network traffic related to the Neutrino exploit kit sending Gootkit malware. Enter the x509.log field name that includes the "MyCompany Ltd." trace as your answer.

certificate.subject