

Skills Assessment

As a Security Operations Center (SOC) analyst, you were recently provided with two PCAP (Packet Capture) files named `funky_dns.pcap` and `funky_icmp.pcap`.

Inspect the `funky_dns.pcap` and `funky_icmp.pcap` files, part of this module's resources, to identify if there are certain patterns and behaviors within these captures that deviate from what is typically observed in routine network traffic.

Then, answer the questions below.



Connect to Pwnbox

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

Pwnbox Location

UK

137ms ▾

⏸ 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!

+ 2 📦 Inspect the `funky_dns.pcap` file, part of this module's resources, and enter the related attack as your answer. Answer format: "DNS Flooding", "DNS Amplification", "DNS Tunneling"

DNS Tunneling

Resources

? Go to Questions

Table of Contents

Introduction

Intermediate Network Traffic Analysis Overview ✓

Link Layer Attacks

ARP Spoofing & Abnormality Detection ✓

ARP Scanning & Denial-of-Service ✓

802.11 Denial-of-Service ✓

Rogue Access Point & Evil-Twin Attacks ✓

Detecting Network Abnormalities

Fragmentation Attacks ✓

IP Source & Destination Spoofing Attacks ✓

IP Time-to-Live Attacks ✓

TCP Handshake Abnormalities ✓

TCP Connection Resets & Hijacking ✓

ICMP Tunneling ✓

Application Layer Attacks

HTTP/HTTPS Service Enumeration Detection ✓

Strange HTTP Headers ✓

Cross-Site Scripting (XSS) & Code Injection Detection ✓

SSL Renegotiation Attacks ✓

Peculiar DNS Traffic ✓


Strange Telnet & UDP Connections ✓

Skills Assessment

Skills Assessment ✓

My Workstation

Submit

+ 3  Inspect the funky_icmp.pcap file, part of this module's resources, and enter the related attack as your answer. Answer format: "ICMP Flooding", "ICMP Tunneling", "ICMP SMURF Attack"

ICMP Tunneling

Submit

← Previous

Finish

OFFLINE

Start Instance

∞ / 1 spawns left

Powered by  HACKTHEBOX

