PCAP

Log analysis challenge

1/09/2019
European Cyber Security Challenge 2019
Bucharest, Romania

Version	Name	Comments	Date
0.1	Csaba Virág		26/08/2019
0.2	Adrian Belmonte		10/09/2019

1. Initial Write-Up

Description:

As member of a computer network administration team, you received a network traffic file recording a client-server communication. Your task is to analyse it and see if there are any sensitive information involved in it.

2. Challenge specifications

- Category: Network/traffic/log analysis
- Difficulty : Easy
- Expected time to solve: 30 min

3. Technical specifications

Description:

Challenge Technical Specification, data to set up and access to the environment.

1. Log file is provided in pcap format
2. Participant shall have software to open and analyse it (eg Wireshark)

4. Questions and answers

Question:

How to filter for packets coming from 192.168.10.10/25 and sent to Aruba devices in WireShark?

Answer:

ip.src == 192.168.10.108/25 && eth.dst[0:3] == 9C:1C:12

Question:

Display filters and capture filters can be interchanged because they use the same syntax:

Answer:

False

Question:

Which display filter is used to display all DHCP traffic?

Answer:

1. Dhcp

2. Tcp.port == 68

3. Bootp

Question:

How do you quickly spot large gaps in time between packets in a trace file containing 10,000 packets?

Answer:

1. Set the Time column to Seconds Since Epoch and scroll through the trace file

2. Open and examine the Notes section of Wireshark's Expert infos window

3. Set the Time column to Seconds Since Previously Displayed Packet and sort the Time column

Question:

Which of these filters can be used as either a capture or display filter?

Answer:

1. Dns

2. Udp

3. Dhcp

Question:

Which display filter operator is the equivalent of AND?

Answer:

1., $$

2. &&

3. ||

Question:

Both of the the display filters below will provide the same output. ip.dst==10.100.0.1 or ip.dst==10.100.0.1 ip.dst==10.100.0.1 || ip.dst==10.100.0.1

Answer:

1. True

2. False

Question:

What is the sensible information involved in the pcap file?

Answer:

Username: rocky

Password: Melory66!

Question:

What kind of filter displays the DNS queries sent to look up the https://www.enisa.europe.eu address in Wireshark?

Answer:

dns contains "enisa.europe.eu"

Question:

What kind of display filter produces the HTTPS traffic originating from 10.192.73.117?

Answer:

tls && ip.src == 10.192.73.117

5. Attack Scenario

Description:

In the field of computer network administration, pcap (packet capture) consists of an application programming interface (API) for capturing network traffic. A client-server authentication recorded and the communication is saved to .pcap format.

6. Installation instructions

Description:

Distribute the attached pcap file with the task description.

7. Tools needed

Description:

Tools needed for the solution of the challenge:

- Wireshark

8. Artefacts Provided

Description:

List of artifacts provided with checksums.

Example:

Name	**Format**	**Comment**	**Checksum (SHA256)**
Challenge1.pcap	pcap		9b50a0a22e71da983a70262a1ecba62a6720ad22c943ba590d055645ac423c20
2019 Technical Challenges Challenge 1.docx	Word Document		d97c577a1fa392a7011ce0b067426c1d538bc9065f1c6c61038caf5f362978ec

9. Walkthrough (writeup)

1. Participants open the attached pcap file with Wireshark

2. After analyzing it there are two HTTP requests, a post and a get

3. In the post there is a username and a password (rocky/Melory66!)