Challenge #6
Analyze network traffic

Anchoring and overview

Modul:	681	Angriffe auf ICT-Infrastrukturen detektieren und abwehren
Handlungsziele:	HZ 1	Definiert unter Berücksichtigung der Bedrohungslage die relevanten Indikatoren, Signaturen und Muster zur Erkennung von Angriffen auf die ICT-Infrastruktur der Organisation.
	HZ 2	Wählt geeignete Überwachungs- und Schutzlösungen zur netzwerkbasierten Erkennung und Abwehr von Angriffen aus und nimmt diese in Betrieb.
	679	Informationen über Bedrohungen beschaffen und aufbereiten
	HZ 4	Analysiert Informationen über Bedrohungen und dokumentiert die Erkenntnisse auf der taktischen und operativen Ebene der CTI.
Leistungskriterien PO:	[LK-B-4]	CSS sind fähig, technische Lösungen zur Erkennung von Angriffen zu erläutern und deren Funktion zu gewährleisten.
	LK-B-5	CSS sind fähig, Protokollierungen von unterschiedlichen Systemen und in unterschiedlichen Formaten auszuwerten und zu interpretieren.

Formulation of task (candidate view)

Analyze network traffic

Resources

[1] Packet Capture File to be analyzed
`c6-traffic.pcap` - MD5-Checksum: xxx

Introduction

Trogawa Inc. is a successful and expanding company providing various SaaS services for video and movie editing for major Hollywood brands and Influencers alike.

A network administrator recently detected and recorded suspicious HTTP traffic from an external IP 154.49.2.126. He now asks you to analyze the recorded traffic.

Download the PCAP file from the resource section and check its integrity by calculating and comparing the MD5 checksum.

Goal and tasks

Analyze the given network traffic and answer to the following questions in a written report:

1. Analyze the connection establishments between the client and the server **within the first 20 packets** of the PCAP file. List all successful TCP handshakes with the corresponding packet numbers and the control flags in the TCP header and specify the total number of handshakes.
2. What type of request does the client sends repeatedly after a connection has been established? Indicate the TCP control flags and briefly explain their intention as well as the server-side impact.
3. What kind of attack is being carried out here? Categorize and characterize the attack as accurately as possible.
4. Analyze the information about the user agent that the client claims to use. Specify the operation system and the browser, both including its version.
5. Which security goal is being defeated according to the “CIA Triad”?
6. Which threat actor goal is being achieved according to the “DAD Triad”?

Submission

Submit a written report as PDF document with your answers. Make sure that your answers can be clearly assigned to the question numbers in the goal and task section.

Specifications for correction

Evaluation criteria

Question #1

C01: Total 5 handshakes correctly counted and mentioned in the report = 1pt.

C02: Correct sequence of handshake SYN > SYN / ACK > SYN mentioned = 1pt.

C03: Packet numbers of all 5 handshakes listed correctly = 2pt.

Question #2

C04: PSH / ACK request identified = 1pt.

C05: Intention of ACK correctly explained = 1pt.

C06: Intention of PSH correctly explained = 1pt.

C07: Server-side impact described = 1pt.

Question #3

C08: Answer contains the classification as a DoS attack = 1pt.

C09: Answer contains the classification as a protocol based / level attack = 1pt.

C10: Answer contains the characteristic of flooding = 1pt.

Question #4

C11: Correct operating system including version reported = 1pt.

C12: Correct Agent (Browser) including version reported = 1pt.

Question #5

C13: “Availability” identified as security goal (according to the CIA triad) = 1 pt.

Question #6

C14: “Denial” identified as actor goal (according to DAD triad) = 1 pt.

Correction instructions

- This challenge gives a maximum of **15 points**.
- Given scores on the criteria may not be further subdivided.

Sample solutions

Q	Answer
#1	The following **5 handshakes** can be identified in the first 20 packets of the PCAP file: **#1**: Client SYN **#2**: Server SYN / ACK **#3**: Client ACK **#5**: Client SYN **#8**: Server SYN / ACK **#9**: Client ACK **#6**: Client SYN **#12**: Server SYN /ACK **#13**: Client ACK **#11**: Client SYN **#17**: Server SYN / ACK **#18**: Client ACK **#15**: Client SYN **#22**: Server SYN / ACK **#23**: Client ACK
	Background: The easiest way to identify the sequences is to follow the TCP stream in Wireshark.
#2	**Request type**: The client repeatedly sends **(PSH, ACK)** requests. **Intention** • The ACK informs the server that he has received data (which in fact is not really true). • The PSH flag instructs the server to immediately forward data to application level (without buffering and not waiting for additional data). **Impact** The server will waste its system resources trying to define where the packets belong. This results in productivity loss and can succeed in server unavailability.
	Background: Since connections were established in a correct manner, PUSH / ACK messages are considered as standard traffic flow (and the server does not reply with RST). However, a huge flood of these messages alone indicates abuse
#3	Elements of a correct answer are • **Denial of Service (DoS)** attack • **Protocol based attack** (and not volume based or application layer attack, see below) • **PSH / ACK flood** (or PSH flood only) • Slowloris **Incorrect answers** in the given context are: • DDoS attack, since all requests origin on one single source IP (not a distributed attack) • Volume based attacks such as UDP floods, ICMP floods • Application layer attacks such as HTTP (GET- or POST) floods, webserver or OS attacks, since (almost) no meaningful data is exchanged • Other protocol attacks such as SYN Flood, Ping of Death, since the client does not skip or delay the final ACK in the handshake
	Background: Slowloris can take down a server with a single host and without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by creating connections to the target server, but sending only a partial request. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This can end in overflowing the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.

Q	Answer
#4	HTTP header: User-Agent: Mozilla/4.0 (compatible; **MSIE 7.0**; **Windows NT 5.1**; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.503l3; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12) Interpretation • MSIE 7.0 > **Internet Explorer 7.0** • Windows NT 5.1 > **Windows XP**
	Background: The HTTP header fields can be read with Wireshark either by following a TCP stream or directly int TCP payload of a packet. By the way, the "MSOffice 12" part of the user-agent string indicates that the requests originated from an application that is part of the Microsoft Office suite (where Office 12 is the internal name for Office 2007). However, the HTTP header User Agent can be spoofed by the attacker. A quick search on the web will lead to slowloris scripts that use this header.
#5	**Availability** (A) according to the CIA Triad
#6	**Denial** (D) according to the DAD Triad