VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

PAKETŲ ANALIZĖ

Saugumo patikros ir etiško įsilaužimo technologijų laboratorinis darbas nr. 2

Darbą atliko: Simonas Riška

Darbą tikrino: lekt. [redacted]

VILNIUS 2025

Examined file : 1.pcap MD5 Hash : 47451679a42fc2a5a637886e97fd7283 SHA-1 Hash : 4623636b88b6293888a3ebcb75cffb767bd11094	Time taken to complete: 5 minutes.
Question 1. What is/are the source(s) (IP address) of the suspicious traffic?	
Answer 1. 192.0.2.245, 192.0.2.196, 192.0.2.207, 192.0.2.6, 192.0.2.25, 192.0.2.120, 192.0.2.83, 192.0.2.154, 192.0.2.253, 192.0.2.236	
Question 2. What is the destination (IP address) of the suspicious traffic?	
Answer 2. 192.0.2.2	
Question 3. What is the transport layer protocol used?	
Answer 3. TCP	
Question 4. What is/are the source port(s)?	
Answer 4. 35356, 44463, 23784, 51136, 57003, 20920, 36927, 52048, 62151, 46528	
Question 5. What is/are the destination port(s)?	
Answer 5. 64354, 58034, 25895, 62694, 48897, 46680, 35104, 43120, 17166, 19043	
Question 6. What conclusions can you come up to regarding the type of the 'attack' illustrated by this pcap?	
Answer 6. This pcap file appears to be a TCP SYN flood attack, because all packets are TCP with the SYN flag set and no ACK replies are shown, which indicates incomplete TCP handshakes and each source IP attempts to initiate a connection to different destination ports on the same destination IP (192.0.2.2). Diversity in source IP addresses suggests either a spoofed source IP attack (source addresses are fake) or a distributed attack from multiple hosts. Goal of such attack is to overwhelm the target system by forcing it to allocate resources for each half-open connection, eventually exhausting its capacity.	

Examined file : 2.pcap MD5 Hash : 19633e3a2a3d4c315994fddc3ce7090f SHA-1 Hash : f9d5be156ca124b46450910d2b7b1e79f2f6825c	Time taken to complete: 10 min
Question 1. What is the source(s) (MAC address) of the suspicious traffic?	
Answer 1. 00:11:22:33:44:55 (CIMSYS_33:44:55)	
Question 2. What is/are the destination (MAC address[es]) of where the suspicious traffic is mostly directed towards?	
Answer 2. ff:ff:ff:ff:ff:ff, 00:0c:83:13:e8 (Intel_83:13:e8)	
Question 3. What is the link layer protocol used?	
Answer 3. ARP (Address Resolution Protocol)	
Question 4. What is the purpose of this protocol?	
Answer 4. To map an IP address to a MAC address (resolve local network device MAC addresses)	
Question 5. What conclusions can you come up to regarding the type of the attack illustrated by this pcap? How can this attack be used for launching other kinds of attack?	
Answer 5. This is an ARP scan or ARP reconnaissance – t he attacker sends multiple ARP requests to identify active hosts on the local network. This is a reconnaissance technique that can be used before launching MITM attacks (like ARP spoofing) or scanning for exploitable systems.	

Examined file : 3.pcap MD5 Hash : 0944977919541d4ee176450b7ce36f9d SHA-1 Hash : 7349e1fea8e6ed6b4dce3f89898b1c6492f3a610	Time taken to complete:
Question 1. What is the source (IP address) of the suspicious traffic?	
Answer 1. 10.0.23.109	
Question 2. What is the destination (IP address) of the suspicious traffic?	
Answer 2. 80.237.98.132	
Question 3. What is the transport layer protocol used?	
Answer 3. TCP	
Question 4. This may be considered as not a direct attack but as a preparation step before an attack. Name the technique used and its purpose.	
Answer 4. The technique is TCP SYN scanning. Its purpose is to identify open TCP ports on the target system (80.237.98.132). The attacker sends a flood of SYN packets to different destination ports. The absence of SYN-ACK responses and repeated retransmissions suggest the scan is stealthy or blocked, and might be used to map live ports/services before a deeper intrusion attempt.	

Examined file : 4.pcap MD5 Hash : 10828ee58a4000050ef7d9ed0fd9bcee SHA-1 Hash : 26d41564189600941a63d5553bd1d7c560f7f228	Time taken to complete:
Question 1. What is the source (IP address) of the suspicious traffic?	
Answer 1. 10.0.32.25	
Question 2. What is the destination (IP address) of the suspicious traffic?	
Answer 2. 80.237.98.132	
Question 3. What is the transport layer protocol used?	
Answer 3. UDP	
Question 4. What is the lowest requested destination port? What is the highest?	
Answer 4. Lowest destination port: 1684, highest destination port: 59951	
Question 5. Again this may not be considered as a direct attack, but as a preparation step before an attack. Name the technique used and its purpose.	
Answer 5. The technique is UDP port scanning. Its purpose is to discover open UDP ports on the target system. Since UDP is connectionless, the attacker sends small UDP packets to many ports and interprets any ICMP Port Unreachable replies (if available) or lack of response to detect if a port is open. This is often used by attackers to recon service availability.	