Security Solutions BY P3NGU1N

Intrusion Detection System (IDS)

🎯 How many of the following are tools in the IDS type?

1. Snort
2. Volatility
3. OllyDbg
4. Suricata
5. Zeek/Bro
6. REMnux

ANSWER: 3

🎯 **Question:** According to the Snort IDS log, what is the IP address from which the response came?

```
[**] [1:254:4] DNS SPOOF query response with TTL of 1 min. and no authority [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
03/14-14:13:32.988223 4.2.2.3:53 -> 192.168.52.10:1044
UDP TTL:54 TOS:0x0 ID:16027 IpLen:20 DgmLen:82
Len: 54
```

ANSWER: 4.2.2.3

🎯 Check the Snort IDS log, according to the OSI model, which layer 7 network protocol does it belong to?

ANSWER: DNS

🎯 **Question:**

What is the HTTP request method according to the given Zeek IDS HTTP log?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\zeek-http.log.zip

ANSWER: GET

🎯 **Question:**

What is the FTP command used for file transfer according to the given Zeek IDS FTP log?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\zeek-ftp.log.zip

ANSWER: RETR

Intrusion Prevention System (IPS)

🎯 **Question:**

According to the given Suricata IPS log, has the command been run successfully?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\suricata1.log.zip

ANSWER: y

🎯 What is the name of the SSL vulnerability that is attempted to be exploited in the given Suricata IPS log?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\suricata2.log.zip

ANSWER: poodle

🎯 What is the name of the scanning tool that triggers the creation of the given Suricata IPS log?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\suricata3.log.zip

ANSWER: Nmap

Firewall

🎯 **Question:**

What is the action taken according to the given firewall log?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\firewall.log.zip

ANSWER: deny

🎯 What is the source IP address according to the given firewall log?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\firewall.log.zip

ANSWER: 192.168.68.12

🎯 What is the destination port number according to the given firewall log?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\firewall.log.zip

ANSWER: 143

🎯 According to the given Windows Defender Firewall log, what is the IP address that sends the TCP segment whose source port is 5421?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\pfirewall.log.zip

ANSWER: 192.168.1.9

🎯 According to the given Windows Defender Firewall log, which network protocol do the logs associated with the "8.8.8.8" IP address belong to?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\pfirewall.log.zip

ANSWER: ICMP

Endpoint Detection and Response (EDR)

🎯 **Question:**

What is the name of the powershell script that is tried to be downloaded according to the given Crowdstrike EDR log?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\edr1.log.zip

ANSWER: Invoke-Mimikatz

🎯 According to the given Crowdstrike EDR log, what is the name of the MITRE technique used by the attacker?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\edr1.log.zip

ANSWER: OS Credential Dumping

🎯 According to the given Crowdstrike EDR log, what is the name and extension of the file that the attacker is trying to download onto the system?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\edr2.log.zip

ANSWER: Get-System.ps1

🎯 What is the severity of the alert based on the given Crowdstrike EDR log?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\edr2.log.zip

ANSWER: high

Antivirus Software (AV)

🎯 **Question:**

According to the given Windows Defender log, what is the type of malware named “executable.8180.exe”?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\win-defender.log.zip

ANSWER: Trojan

🎯 According to the given Windows Defender log, what is the name of the file belonging to the "Backdoor" type malware?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\win-defender.log.zip

ANSWER: program1

Sandbox Solutions

🎯 According to the sandbox analysis result in the URL given below, for which domain address was the DNS request made?

URL:

https://app.any.run/tasks/2d2ca664-521c-48bf-9748-722cbf34bcea/

SHA256 Hash:

4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784

ANSWER: www.xmlformats.com

🎯 What is the name and extension of the file that performs the malicious activity on the system according to the sandbox analysis result in the URL given below?

URL:

https://app.any.run/tasks/73db6760-6ca1-42fc-bd8d-dd6425d7acea

SHA256 Hash:

dcbd77ad65145ab5aa64b8c08608991a6cc23daabf02cf0695f2261da3ec5b7d

ANSWER: DotSetupSDK.dll

Web Application Firewall (WAF)

🎯 **Question:**

According to the given AWS WAF log, a request for SQL_Injection attack was blocked. What is the IP Address that sent this request?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\aws-waf.log.zip

ANSWER: 185.220.101.35

🎯 According to the given Cloudflare WAF log, an HTTP request was sent to the IP address 185.220.102.244 . Which HTTP method does this HTTP request use?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\cloudflare-waf.log.zip

ANSWER: GET

Load Balancer

🎯 **Question:**

What is the User-Agent in the HTTP request in the given AWS load balancer log?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\aws-loadbalancer.log.zip

ANSWER: curl/7.46.0

Proxy Server

🎯 **Question:**

According to the given Squid Web Proxy Server log, to which port of the "letsdefend.io" address was the request sent?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\squid-proxy.log.zip

ANSWER: 443

🎯 According to the given Squid Web Proxy Server log, how many different web addresses are there to send HTTP GET method requests?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\squid-proxy.log.zip

ANSWER: 5

Email Security Solutions

🎯 **Question:**

According to the email security solution log, what is the email address of the recipient of the email?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\email.log.zip

ANSWER: jonas@letsdefend.io

🎯 What is the type of threat according to the email security solution log provided?

File Location:

C:\Users\LetsDefend\Desktop\QuestionFiles\email.log.zip

ANSWER: malware

QUIZ:

🎯 **What is a security product that detects attacks by monitoring the network or a host but does not have the ability to take action?**

ANSWER: IDS

🎯 **Which of the following is a security product that is generally installed on the outward-facing interfaces of organizations and prevents or allows packet passage by managing network packet passes?**

ANSWER: Firewall

🎯 **What is a security product that tries to detect threats by monitoring activities on the system installed on endpoint devices?**

ANSWER: EDR

🎯 **Which of the following is not an endpoint device?**

ANSWER: Router

🎯 **What is a security product that scans the system and detects malicious software with a signature-based or behavioral analysis method?**

ANSWER: **AntiVirus**

🎯 **What is a security solution that enables analysis of malware behavior by running malware in an isolated environment?**

ANSWER: **Sandbox**

🎯 **Which of the following is not a benefit of Asset Management software?**

ANSWER: **Decreases the operating performance of assets.**

🎯 **What is a security tool that detects and blocks security threats by passing requests to the web application?**

ANSWER: WAF

🎯 **What is the tool used to distribute the traffic to the servers evenly?**

ANSWER: **Load Balancer**

🎯 **Which of the following is not one of the benefits of a proxy server?**

ANSWER: **It does not provide any options to manage network traffic**

🎯 **Which of the following is the most effective security solution against phishing attacks?**

ANSWER: **Email Security Gateway**

🎯 **What is the security product that prevents the leakage of sensitive and critical information outside the organization?**

ANSWER: DLP