# **Introduction to Cyber Security**

## **Exam preparation – Sample Questions**

### **What is an EDR system?**

1. Endpoint driver recovery
2. Enterprise detection and recovery
3. Endpoint detection and response
4. Enumerating devices recursively

### **Which of the terms can be excluded from the list?**

1. SSH
2. FTP
3. TCP
4. MySQL

### **In Cyber Security TTP stands for:**

1. Thrombotic thrombocytopenic purpura
2. Training, tools and protocols
3. Tactics techniques and procedures
4. Tools, techniques and procedures

### **Which tools is used to perform directory (active) scanning?**

1. LogStash
2. Kibana
3. SQLMap
4. Feroxbuster

### **On which step from the Lockheed Martin kill chain, exploitation is performed?**

1. 7
2. 1
3. 4
4. 3

### **Which of the following is considered an IP range?**

1. 10.1.1.1
2. 192.168.1.2
3. 10.2.2.0/24
4. 20.2.2.4

### **Virtual private network is an infrastructure that allows machines to:**

1. download, upload and transfer files from one location to another via Internet
2. connect to each other in a secure way
3. monitor and manage devices from a remote location
4. all of the above is true

### **How can you prevent exploiting publicly available vulnerabilities?**

1. By removing Windows and installing Linux
2. By conducting more pentests
3. By updating the software
4. By restricting the internet access

### **Imagine during pentest you found a web application for listing newsletters. By supplying the following payload (‘category=Products'+OR+1=1--’) you were able to retrieve all of the newsletters from the database. What is the vulnerability?**

1. OS Command Injection
2. Misconfiguration
3. SQL injection
4. Directory listing

### **What is Firewall?**

1. Anti-virus software
2. Penetration testing software
3. Protection against ransomware
4. Security software / hardware to filter traffic

### **Which of the following statements is not correct?**

1. Vulnerabilities can only occur within a software
2. Regular patching prevents vulnerabilities from being exploited
3. Zero-day vulnerabilities can remain undiscovered for a long time
4. An exploit cannot be done without discovered vulnerability

### **What is a DoS / DDoS attack?**

1. Attack aiming to inject a trojan horse within a specific network
2. Attack aiming to encrypt data of resources within a specific network
3. Attack aiming to overstress a network, workloads or applications and disrupt the  
    working process
4. Attack aiming to perform TCP reverse shell on a particular workload

### **Brute-Forcing is an attack of:**

1. OS Command Injection Attack
2. A type of social engineering
3. Trying multiple combination in order to "guess" a valid credentials
4. Decrypting the stored hash value of credentials

### **Which of the following statements is true?**

1. Red Teamer is a defensive oriented position
2. Pentesting is focused on web and mobile applications only
3. The Security Analyst is responsible for implementing security solutions
4. Incident Responders look after the security posture of a company

### **Which of the following is considered as a secure and up to date HASH algorithm?**

1. LM
2. SHA-1
3. MD5
4. SHA-256

### **What service is assigning local IP addresses?**

1. SSH
2. HTTP
3. DHCP
4. FTP

### **Access Control Vulnerabilities are types of vulnerabilities that allows the attacker to:**

1. Perform SQL injection attacks
2. Compromise Firewalls and access the network
3. Bypass the security of an application, accessing internal assets and functions
4. Bypass the IPS and sniff network traffic

### **What is ELK stack? A software framework that combines and aggregates many logs**

1. A software framework that combines different networking protocols
2. A software framework for penetration testing
3. A software framework for network monitoring

### **The first step in order to identify incidents is:**

1. Utilizing TTPs to discover an active attack, breaches or other type of incidents
2. Utilizing network administration tools in order to close all inbound traffic
3. Check for any encrypted data on workloads within the network
4. Making sure that more penetration tests are conducted on internal resources

### **JWT token is used for:**

1. Authentication in web apps
2. Authorization in web apps
3. Authentication in Windows OS
4. Authorization in Linux OS