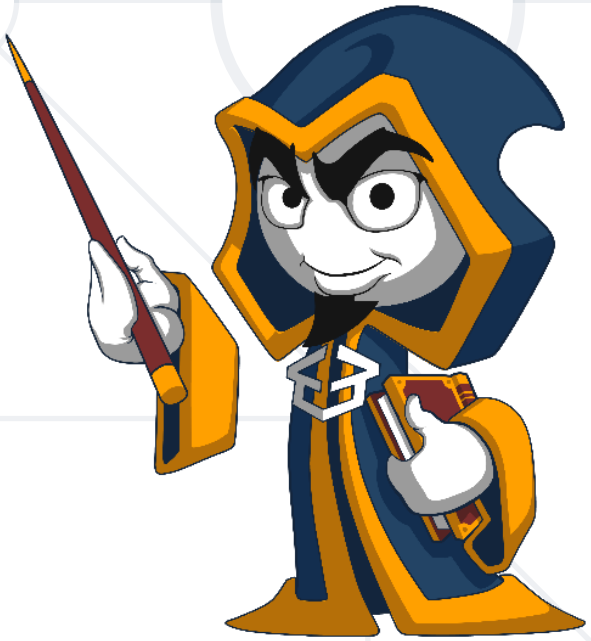
Exam Preparation

SoftUni Team

Technical Trainers

Software University

SoftUni



Software University

https://softuni.bg

Have a Questions?

Software University

sli.do

#Cyber_Security

Question 1

Software University

What is an EDR system?

a) Endpoint driver recovery

b) Enterprise detection and recovery

c) Endpoint detection and response

d) Enumerating devices recursively

Question 2

Software University

Which of the terms can be excluded from the list?

a) SSH

b) FTP

c) TCP

d) MySQL

Question 3

In Cyber Security TTP stands for:

a) Thrombotic thrombocytopenic purpura

b) Training, tools and protocols

c) Tactics techniques and procedures

d) Tools, techniques and procedures

Question 4

Software University

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

a) LogStash

b) Kibana

c) SQLMap

d) Feroxbuster

Question 5

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

a) 7

b) 1

c) 4

d) 3

Question 6

Software University

Which of the following is considered an IP range?

a) 10.1.1.1

b) 192.168.1.2

c) 10.2.2.0/24

d) 20.2.2.4

Question 7

Virtual private network is an infrastructure that allows machines to:

a) download, upload and transfer files from one location to another via Internet

b) connect to each other in a secure way

c) monitor and manage devices from a remote location

d) all of the above is true

Question 8

How can you prevent exploiting publicly available vulnerabilities?

a) By removing Windows and installing Linux

b) By conducting more pentests

c) By updating the software

d) By restricting the internet access

Question 9

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?

a) OS Command Injection

b) Misconfiguration

c) SQL injection

d) Directory listing

Question 10

What is Firewall?

a) Anti-virus software

b) Penetration testing software

c) Protection against ransomware

d) Security software / hardware to filter traffic

Question 11

Software University

Which of the following statements is NOT correct?

a) Vulnerabilities can only occur within a software

b) Regular patching prevents vulnerabilities from being exploited

c) Zero-day vulnerabilities can remain undiscovered for a long time

d) An exploit cannot be done without discovered vulnerability

Question 12

Software University

What is a DoS / DDoS attack?

a) Attack aiming to inject a trojan horse within a specific network

b) Attack aiming to encrypt data of resources within a specific network

c) Attack aiming to overstress a network, workloads or applications and disrupt the working process

d) Attack aiming to perform TCP reverse shell on a particular workload

Question 13

Brute-Forcing is an attack of:

a) OS Command Injection Attack

b) A type of social engineering

c) Trying multiple combination in order to "guess" a valid credentials

d) Decrypting the stored hash value of credentials

Question 14

Software University

Which of the following statements is true?

a) Red Teamer is a defensive oriented position

b) Pentesting is focused on web and mobile applications only

c) The Security Analyst is responsible for implementing security solutions

d) Incident Responders look after the security posture of a company

Question 15

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

a) LM

b) SHA-1

c) MD5

d) SHA-256

Question 16

Software University

What service is assigning local IP addresses?

a) SSH

b) HTTP

c) DHCP

d) FTP

Question 17

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

a) Perform SQL injection attacks

b) Compromise Firewalls and access the network

c) Bypass the security of an application, accessing internal assets and functions

d) Bypass the IPS and sniff network traffic

Question 18

Software University

What is ELK stack?

a) A software framework that combines and aggregates many logs

b) A software framework that combines different networking protocols

c) A software framework for penetration testing

d) A software framework for network monitoring

Question 19

The first step in order to identify incidents is:

a) Utilizing TTPs to discover an active attack, breaches or other type of incidents

b) Utilizing network administration tools in order to close all inbound traffic

c) Check for any encrypted data on workloads within the network

d) Making sure that more penetration tests are conducted on internal resources

Question 20

Software University

JWT token is used for:

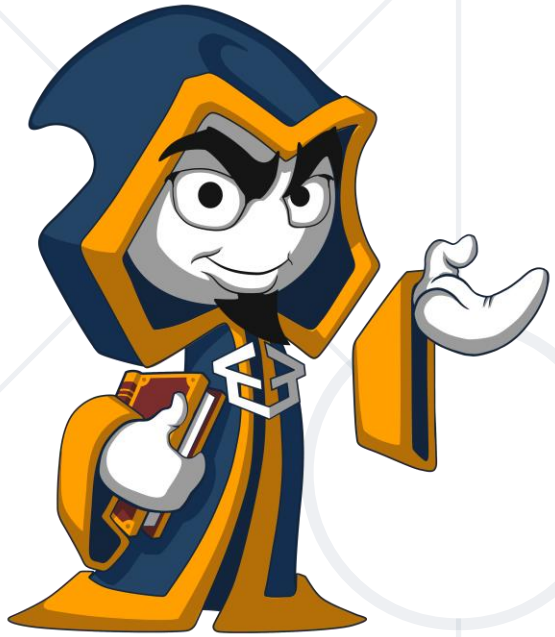
a) Authentication in web apps

b) Authorization in web apps

c) Authentication in Windows OS

d) Authorization in Linux OS

Questions?



SoftUni

Software University

SoftUni Creative

SoftUni Digital

SoftUni Foundation

SoftUni Kids

СофтУни БУДИТЕЛ

Finance Academy

SoftUni Diamond Partners

Software University

SmartIT

Coca-Cola HBC Bulgaria

SUPER HOSTING .BG

createX

Postbank

Решения за твоето утре

DRAFT KINGS

THE CROWN IS YOURS

VIVACOM

AMBITIONED

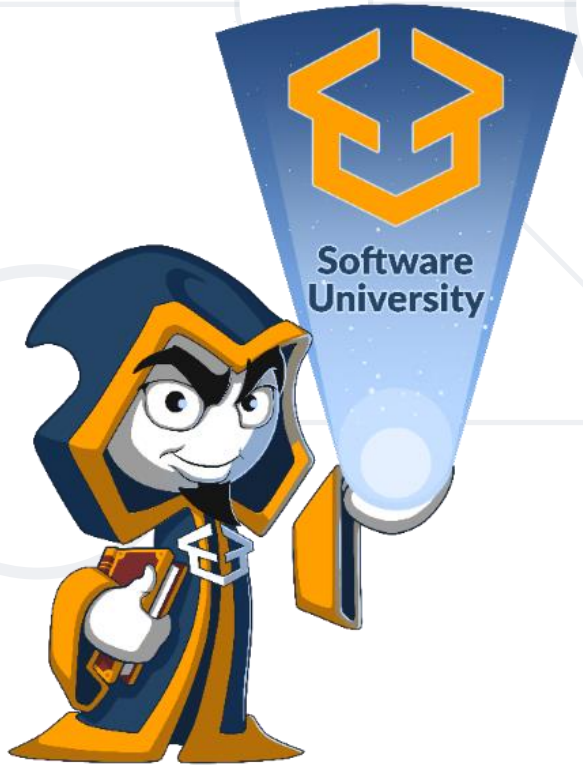
INDEAVR

Serving the high achievers

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity



License

- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – https://about.softuni.bg/
- © Software University – https://softuni.bg