Google IT Support Certificate: Course 5: IT Security - Defense Against the Digital Dark Arts

Week 5: Defense in Depth

Quiz: Defense in Depth

Question 1:

What is a class of vulnerabilities that are unknown before they are exploited?

Zero-day

Attack Surfaces

ACLs

Attack Vectors

Question 2:

What are Bastion hosts?

VLANs

Servers that are specifically hardened and minimized to reduce what's permitted to run on them.

Users that have the ability to change firewall rules and configurations.

A VPN subnet

Question 3:

When looking at aggregated logs, you see a large percentage of Windows hosts connecting to an Internet Protocol (IP) address outside the network in a foreign country. Why might this be worth investigating more closely?

It can indicate a malware infection

It can indicate that ACLs are not configured correctly

It can indicate what software is on the binary whitelist

It can indicate log normalization

Question 4:

What are the two main issues with antivirus software? Select all that apply.

They depend on the IT support professional to discover new malware and write new signatures.

They depend on antivirus signatures distributed by the antivirus software vendor.

They depend on the antivirus vendor discovering new malware and writing new signatures for newly discovered threats.

There are no issues with antivirus software.

Question 5:

What can provide resilience against data theft and prevent an attacker from stealing confidential information from a hard drive that was stolen?

Full disk encryption (FDE)

OS upgrades

Software patch management

Key escrow

Question 6:

A hacker exploited a bug in the software and triggered unintended behavior, which led to the system being compromised by running vulnerable software. Which of these helps to fix these types of vulnerabilities?

Log analysis

Implicit deny

Application policies

Software patch management

Question 7:

Besides software, what other things will also need patches? Select all that apply.

Infrastructure firmware

Operating systems

NFC tags

Hardware

Question 8:

Why is it risky if you want to make an exception to the application policy to allow file sharing software?

The software can shrink attack vectors

The software could disable full disk encryption (FDE)

The software can normalize log data

The software could be infected with malware

Question 9:

What is the defining characteristic of a defense-in-depth strategy for IT security?

Strong passwords

Confidentiality

Encryption

Multiple overlapping layers of defense

Question 10:

Which of the following are potential attack vectors? Select all that apply

Email attachments

Passwords

Network interfaces

Network protocols

Question 11:

Which of these host-based firewall rules helps to permit network access from a Virtual Private Network (VPN) subnet?

Group Policy Objects (GPOs)

Active Directory

Secure Shell (SSH)

Access Control Lists (ACLs)

Question 12:

Securely storing a recovery or backup encryption key is referred to as _______.

Key backup

Key encryption

Key obfuscation

Key escrow

Question 13:

Which of these plays an important role in keeping attack traffic off your systems and helping to protect users? Select all that apply.

Antivirus software

Multiple Attack Vectors

Full disk encryption (FDE)

Antimalware measures

Question 14:

What can provide resilience against data theft, and prevent an attacker from stealing confidential information from a hard drive that was stolen?

Key escrow

Full disk encryption (FDE)

OS upgrades

Software patch management.

Question 15:

What does applying software patches protect against? Select all that apply.

MITM attacks

Newly found vulnerabilities

Undiscovered vulnerabilities

Data tampering

Question 16:

Besides software, what other things will also need patches? Select all that apply.

Hardware

Infrastructure firmware

NFC tags

Operating systems

Question 17:

What are the two primary purposes of application software policies? Select all that apply.

To use a database of signatures to identify malware

To take log data and convert it into different formats

To define boundaries of what applications are permitted

To help educate users on how to use software more securely

Question 18:

While antivirus software operates using a ______, binary whitelisting software uses a whitelist instead.

Secure list

Blacklist

Whitelist

Greylist

Question 19:

Ideally, an attack surface is ___

open and defended.

as large as possible.

frequently updated.

as small as possible.

Question 20:

While antivirus software operates using a ______, binary whitelisting software uses a whitelist instead.

Secure list

Blacklist

Whitelist

Greylist

Question 21:

If a full disk encryption (FDE) password is forgotten, what can be incorporated to securely store the encryption key to unlock the disk?

Application hardening

Application policies

Key escrow

Secure boot

Question 22:

What model does antivirus software operate off of?

Secure list

Whitelist

Greylist

Blacklist

Question 23:

A network security analyst received an alert about a potential malware threat on a user’s computer. What can the analyst review to get detailed information about this compromise? Select all that apply.

Security Information and Event Management (SIEM) system

Full disk encryption (FDE)

Logs

Binary whitelisting software

Question 24:

A core authentication server is exposed to the internet and connected to sensitive services. What are some measures you can take to secure the server and prevent it from getting compromised by a hacker? Select all that apply.

Access Control Lists (ACLs)

Secure firewall

Designate as a bastion host

Patch management

Question 25:

How can software management tools like Microsoft SCCM help an IT professional manage a fleet of systems? Select all that apply

Analyze installed software across multiple computers

Detect and prevent malware on managed devices

Force update installation after a specified deadline

Confirm update installation