Introduction to Cybersecurity English 1220

Started on	Friday, 1 January 2021, 7:04 AM
State	Finished
Completed on	Friday, 1 January 2021, 7:05 AM
Time taken	1 min 41 secs
Marks	16.00/16.00
Grade	**100.00** out of 100.00

Quiz navigation

1 2 3 4 5 6 7 8

Finish review

Question 1
Correct
Mark 2.00 out of 2.00
Flag question

Which type of attack allows an attacker to use a brute force approach?

Select one:
- packet sniffing
- denial of service
- password cracking ✔
- social engineering

Refer to curriculum topic: 2.1.4
Common ways used to crack Wi-Fi passwords include social engineering, brute-force attacks, and network sniffing.

The correct answer is: password cracking

Question 2
Correct
Mark 2.00 out of 2.00
Flag question

What is the most common goal of search engine optimization (SEO) poisoning?

Select one:
- to build a botnet of zombies
- to overwhelm a network device with maliciously formed packets
- to trick someone into installing malware or divulging personal information
- to increase web traffic to malicious sites ✔

Refer to curriculum topic: 2.1.5
A malicious user could create a SEO so that a malicious website appears higher in search results. The malicious website commonly contains malware or is used to obtain information via social engineering techniques.

The correct answer is: to increase web traffic to malicious sites

Question 3
Correct
Mark 2.00 out of 2.00
Flag question

Which two characteristics describe a worm? (Choose two.)

Select one or more:
- ☐ executes when software is run on a computer
- ☑ travels to new computers without any intervention or knowledge of the user ✔
- ☐ infects computers by attaching to software code
- ☑ is self-replicating ✔
- ☐ hides in a dormant state until needed by an attacker

Refer to curriculum topic: 2.1.3
Worms are self-replicating pieces of software that consume bandwidth on a network as they propagate from system to system. They do not require a host application, unlike a virus. Viruses, on the other hand, carry executable malicious code which harms the target machine on which they reside.

The correct answers are: is self-replicating, travels to new computers without any intervention or knowledge of the user

Question 4

Question 4

Correct

Mark 2.00 out of 2.00

Flag question

What is the purpose of a rootkit?

Select one:

- to masquerade as a legitimate program
- to replicate itself independently of any other programs
- to deliver advertisements without user consent
- to gain privileged access to a device while concealing itself ✔

Refer to curriculum topic: 2.1.2
Malware can be classified as follows:

- Virus (self replicates by attaching to another program or file)
- Worm (replicates independently of another program)
- Trojan Horse (masquerades as a legitimate file or program)
- Rootkit (gains privileged access to a machine while concealing itself)
- Spyware (collects information from a target system)
- Adware (delivers advertisements with or without consent)
- Bot (waits for commands from the hacker)
- Ransomware (holds a computer system or data captive until payment is received)

The correct answer is: to gain privileged access to a device while concealing itself

Question 5

Correct

Mark 2.00 out of 2.00

Flag question

What is the primary goal of a DoS attack?

Select one:

- to obtain all addresses in the address book within the server
- to facilitate access to external networks
- to prevent the target server from being able to handle additional requests ✔
- to scan the data on the target server

Refer to curriculum topic: 2.1.5
A denial of service (DoS) attack attempts to overwhelm a system or process by sending large amounts of data or requests to the target. The goal is to keep the system so overwhelmed handling false requests that it is unable to respond to legitimate ones.

The correct answer is: to prevent the target server from being able to handle additional requests

Question 6

Correct

Mark 2.00 out of 2.00

Flag question

In what way are zombies used in security attacks?

Select one:

- They target specific individuals to gain corporate or personal information.
- They are maliciously formed code segments used to replace legitimate applications.
- They are infected machines that carry out a DDoS attack. ✔
- They probe a group of machines for open ports to learn which services are running.

Refer to curriculum topic: 2.1.5
Zombies are infected computers that make up a botnet. The zombies are used to deploy a distributed denial of service (DDoS) attack.

The correct answer is: They are infected machines that carry out a DDoS attack.

Question 7

Correct

Mark 2.00 out of 2.00

Flag question

Which example illustrates how malware might be concealed?

Select one:

- A hacker uses techniques to improve the ranking of a website so that users are redirected to a malicious site.
- A botnet of zombies carry personal information back to the hacker.
- An attack is launched against the public website of an online retailer with the objective of blocking its response to visitors.
- An email is sent to the employees of an organization with an attachment that looks like an antivirus update, but the attachment actually consists of spyware. ✔

Refer to curriculum topic: 2.1.3
An email attachment that appears as valid software but actually contains spyware shows how malware might be concealed. An attack to block access to a website is a DoS attack. A hacker uses search engine optimization (SEO) poisoning to improve the ranking of a website so that users are directed to a malicious site that hosts malware or uses social engineering methods to obtain information. A botnet of zombie computers is used to launch a DDoS

attack.

The correct answer is: An email is sent to the employees of an organization with an attachment that looks like an antivirus update, but the attachment actually consists of spyware.

Question 8
Correct
Mark 2.00 out of 2.00
Flag question

Which tool is used to provide a list of open ports on network devices?

Select one:

- Whois
- Tracert
- Nmap ✔
- Ping

Refer to curriculum topic: 2.1.4
The Nmap tool is a port scanner that is used to determine which ports are open on a particular network device. A port scanner is used before launching an attack.

The correct answer is: Nmap

Finish review

◄ Chapter 2: Terms and Concepts Practice

Jump to...

Launch Chapter 3 ►