Good job!
You have successfully identified the correct answers.

You answered 12 out of 12 questions correctly.

Show Menu

1 The Danger

1.3.2 Lost Competitive Advantage

1.3.3 Politics and National Security

1.3.4 Lab – Visualizing the Black Hats

1.4 The Danger Summary

1.4.1 What Did I Learn in this Module?

1.4.2 Module 1: The Danger Quiz

2 Fighters in the War Against Cybercrime

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

The Danger Summary

1.4.1

What Did I Learn in this Module?

War Stories

Threat actors can hijack banking sessions and other personal information by using “evil twin” hotspots. Threat actors can target companies, as in the example where opening a pdf on the company computer can install ransomware. Entire nations can be targeted. This occurred in the Stuxnet malware attack.

Threat Actors

Threat actors include, but are not limited to, amateurs, hacktivists, organized crime groups, state sponsored, and terrorist groups. The amateur may have little to no skill and often use information found on the internet to launch attacks. Hacktivists are hackers who protest against a variety of political and social ideas. Much of the hacking activity is motivated by financial gain. Nation states are interested in using cyberspace for industrial espionage. Theft of intellectual property can give a country a significant advantage in international trade. As the Internet of Things (IoT) expands, webcams, routers, and other devices in our homes are also under attack.

Threat Impact

It is estimated that businesses will lose over $5 trillion annually by 2024 due to cyberattacks. Personally identifiable information (PII), protected health information (PHI), and personal security information (PSI) are forms of

9 The Transport Layer
10 Network Services
Show Menu
1 The Danger
1.3.2 Lost Competitive Advantage
1.3.3 Politics and National Security
1.3.4 Lab – Visualizing the Black Hats
1.4 The Danger Summary
1.4.1 What Did I Learn in this Module?
1.4.2 Module 1: The Danger Quiz
2 Fighters in the War Against Cybercrime

protected information that are often stolen. A company
is information
tomers lose
ir data.
cking.

Good job!
You have successfully identified the correct answers.
You answered 12 out of 12 questions correctly.

1.4.2

Module 1: The Danger Quiz

1. An attacker sends a piece of malware as an email attachment to employees in a company. What is one probable purpose of the attack?

Topic 1.1.0 – Curriculum Reference: Module 2.1
This item is based on information contained in the presentation.
This is a malware attack. The purpose of a typical malware attack is to disrupt computer operations, gather sensitive information, or gain access to a private computer system. Cracking a password

4 Linux Overview
5 Network Protocols
6 Ethernet and Internet Protocol (IP)
7 Connectivity Verification
8 Address Resolution Protocol
9 The Transport Layer

noticeable. A reconnaissance attack would be used to probe open ports on a border firewall. Similarly, denying external access to a web server is a DoS attack launched from outside the company.

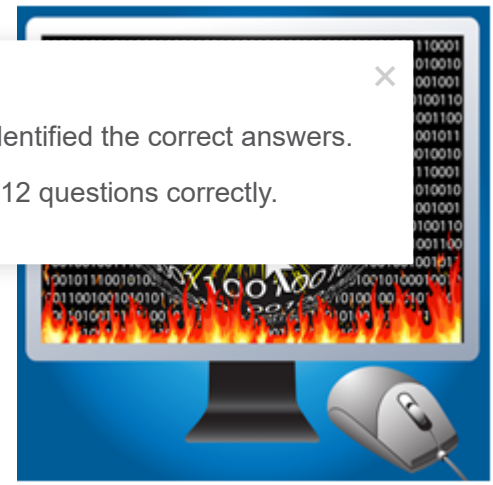
- cracking the administrator password for a critical server
- probing open ports on the firewall on the border network
- searching and obtaining trade secrets
- denying external access to a web server that is open to the public

9 The Transport Layer
10 Network Services
Show Menu
1 The Danger
1.3.2 Lost Competitive Advantage
1.3.3 Politics and National Security
1.3.4 Lab - Visualizing the Black Hats
1.4 The Danger Summary
1.4.1 What Did I Learn in this Module?
1.4.2 Module 1: The Danger Quiz
2 Fighters in the War Against Cybercrime
3 The Windows Operating System
4 Linux Overview
5 Network Protocols
6 Ethernet and Internet Protocol (IP)
7 Connectivity Verification
8 Address Resolution Protocol
9 The Transport Layer

Good job!
You have successfully identified the correct answers.

You answered 12 out of 12 questions correctly.

2.



What is cyberwarfare?

Topic 1.3.0 - Curriculum Reference: Module 5.1
This item is based on information contained in the presentation. Cyberwarfare is a subset of information warfare (IW). Its objective is to disrupt (availability), corrupt (integrity) or exploit (confidentiality or privacy). It can be directed against military forces, critical infrastructures, or other national interests, such as economic targets. It involves several teams that work together. Botnet might be one of several tools to be used for launching the attack.

- It is an attack designed to disrupt, corrupt, or exploit national interests.
- It is an attack only on military targets.
- It is an attack that only involves robots and bots.
- It is an attack on a major corporation.

9 The Transport Layer
10 Network Services
Show Menu
1 The Danger
1.3.2 Lost Competitive Advantage
1.3.3 Politics and National Security
1.3.4 Lab - Visualizing the Black Hats
1.4 The Danger Summary
1.4.1 What Did I Learn in this Module?
1.4.2 Module 1: The Danger Quiz
2 Fighters in the War Against Cybercrime
3 The Windows Operating System
4 Linux Overview
5 Network Protocols
6 Ethernet and Internet Protocol (IP)
7 Connectivity Verification
8 Address Resolution Protocol
9 The Transport Layer

Good job!
You have successfully identified the correct answers.

You answered 12 out of 12 questions correctly.

3. What type of malware has the primary objective of

ose of a
opagate
type of
malicious software that needs a user to spread. A trojan horse is not self-replicating and disguises itself as a legitimate application when it is not. A botnet is a series of zombie computers working together to wage a network attack.

- Trojan horse
- virus
- worm
- botnet

4. What is a potential risk when using a free and open wireless hotspot in a public location?

Topic 1.1.0 - Many free and open wireless hotspots operate with no authentication or weak authentication mechanisms. Attackers could easily capture the network traffic in and out of such a hotspot and steal user information. In addition, attackers might set up a "rogue" wireless hotspot to attract unsuspecting users to it and then collect information from those users.

- The Internet connection can become too slow when many users access the wireless hotspot.
- Purchase of products from vendors might be required in exchange for the Internet access.
- Too many users trying to connect to the Internet may cause a network traffic jam.
- Network traffic might be hijacked and information stolen.

9 The Transport Layer
10 Network Services
Show Menu
1 The Danger
1.3.2 Lost Competitive Advantage
1.3.3 Politics and National Security
1.3.4 Lab - Visualizing the Black Hats
1.4 The Danger Summary
1.4.1 What Did I Learn in this Module?
1.4.2 Module 1: The Danger Quiz
2 Fighters in the War Against Cybercrime
3 The Windows Operating System
4 Linux Overview
5 Network Protocols
6 Ethernet and Internet Protocol (IP)
7 Connectivity Verification
8 Address Resolution Protocol
9 The Transport Layer

Good job!
You have successfully identified the correct answers.

You answered 12 out of 12 questions correctly.

5. At the request of investors, a company is ... a particular ...ternal source. ...e the person ...

Topic 1.2.0 - Some people may use the common word of "hacker" to describe a threat actor. A threat actor is an entity that is involved with an incident that impacts or has the potential to impact an organization in such a way that it is considered a security risk or threat.

- tunneler
- threat actor
- fragmenter
- skeleton

6. What name is given to an amateur hacker?

Topic 1.2.0 - Script kiddies is a term used to describe inexperienced hackers.

- red hat
- black hat
- blue team
- script kiddie

7. What commonly motivates cybercriminals to attack networks as compared to hacktivists or state-sponsored hackers?

Topic 1.1.0 - Cybercriminals are commonly motivated by money. Hackers are known to hack for status. Cyberterrorists are motivated to commit cybercrimes for religious or political reasons.

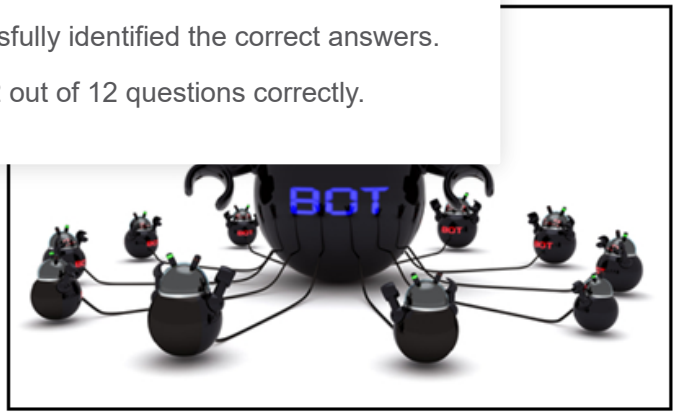
- political reasons
- financial gain
- status among peers

9 The Transport Layer
10 Network Services
Show Menu
1 The Danger
1.3.2 Lost Competitive Advantage
1.3.3 Politics and National Security
1.3.4 Lab – Visualizing the Black Hats
1.4 The Danger Summary
1.4.1 What Did I Learn in this Module?
1.4.2 Module 1: The Danger Quiz
2 Fighters in the War Against Cybercrime
3 The Windows Operating System
4 Linux Overview
5 Network Protocols
6 Ethernet and Internet Protocol (IP)
7 Connectivity Verification
8 Address Resolution Protocol
9 The Transport Layer

Good job!
You have successfully identified the correct answers.

You answered 12 out of 12 questions correctly.

fame seeking



What is a botnet?

Topic 1.2.0 – One method of executing a DDoS attack involves using a botnet. A botnet builds or purchases a botnet of zombie hosts, which is a group of infected devices. The zombies continue to create more zombies which carry out the DDoS attack.

- a group of web servers that provide load balancing and fault tolerance
- an online video game intended for multiple players
- a network that allows users to bring their own technology
- a network of infected computers that are controlled as a group

9. What is a rogue wireless hotspot?

Topic 1.1.0 – A rogue wireless hotspot is a wireless access point running in a business or an organization without the official permission from the business or organization.

- It is a hotspot that does not implement strong user authentication mechanisms.
- It is a hotspot that appears to be from a legitimate business but was actually set up by

9 The Transport Layer
10 Network Services
Show Menu
1 The Danger
1.3.2 Lost Competitive Advantage
1.3.3 Politics and National Security
1.3.4 Lab – Visualizing the Black Hats
1.4 The Danger Summary
1.4.1 What Did I Learn in this Module?
1.4.2 Module 1: The Danger Quiz
2 Fighters in the War Against Cybercrime
3 The Windows Operating System
4 Linux Overview
5 Network Protocols
6 Ethernet and Internet Protocol (IP)
7 Connectivity Verification
8 Address Resolution Protocol
9 The Transport Layer

Good job!
You have successfully identified the correct answers.

You answered 12 out of 12 questions correctly.

someone without the permission from the

outdated

t network

10. What is the best definition of personally identifiable information (PII)?

Topic 1.3.0 – Personally identifiable information (PII) is data that could be used to distinguish the identity of an individual, such as mother's maiden name, social security number, and/or date of birth.

- Data that is collected from servers and websites for anonymous browsing.
- Data that is collected by businesses to track the digital behavior of consumers.
- Data that is collected by businesses to distinguish identities of individuals.
- Data that is collected from servers and web browsers using cookies in order to track a consumer.

11. What was used as a cyberwarfare weapon to attack a uranium enrichment facility in Iran?

Topic 1.1.0 – The Stuxnet malware program is an excellent example of a sophisticated cyberwarfare weapon. In 2010, it was used to attack programmable logic controllers that operated uranium enrichment centrifuges in Iran.

- DDoS
- PSYOPS
- Stuxnet
- SQL injection

9 The Transport Layer

10 Network Services

Show Menu

1 The Danger

1.3.2 Lost Competitive Advantage

1.3.3 Politics and National Security

1.3.4 Lab – Visualizing the Black Hats

1.4 The Danger Summary

1.4.1 What Did I Learn in this Module?

1.4.2 Module 1: The Danger Quiz

2 Fighters in the War Against Cybercrime

3 The Windows Operating System

4 Linux Overview

5 Network Protocols

6 Ethernet and Internet Protocol (IP)

7 Connectivity Verification

8 Address Resolution Protocol

9 The Transport Layer

Good job!
You have successfully identified the correct answers.

You answered 12 out of 12 questions correctly.

12. A company pays a significant sum of money to … email and … ack was used …

… volves the nackers preventing user access to the infected and controlled system until the user pays a specified amount.

- spyware
- Trojan horse
- ransomware
- DoS

Check

Show Me

Reset

1.3 Threat Impact

2.0 Introduction