Exam Report: 2.2.3 Practice Questions

Date: 4/4/29 3:49:08 pm
Time Spent: 1:42

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 40%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

The Stuxnet worm was discovered in 2010 and was used to gain sensitive information on Iran's industrial infrastructure. This worm was probably active for about five years before being discovered. During this time, the attacker had access to the target. Which type of attack was Stuxnet?

- Logic bomb
- APT
- ~~Trojan horse~~
- Virus

Explanation

An APT (advanced persistent threat) is a stealthy attack that gains access to a network or computer system and remains hidden for an extended period of time.

A logic bomb is designed to be triggered by a certain event, such as running a specific program, visiting a certain website, or the arrival of a specific date or time.

A Trojan horse provides the hacker with covert remote access to the victim's system. These programs are embedded and hidden inside legitimate programs.

A virus is a self-replicating program that often attaches and hides itself in a legitimate program. A virus is designed to replicate itself throughout the computer and modify existing programs, often to cause damage to the computer system.

References

TestOut Ethical Hacker Pro - 2.2 Threat Actors
[e_threat_actors_eh1.exam.xml Q_ACTOR_TYPES_ADV_PERSIST_THREAT_01_EH1]

Question 2: Correct

Which type of threat actor only uses skills and knowledge for defensive purposes?

- Hacktivist
- White hat
- Gray hat
- Script kiddie

Explanation

A white hat is a skilled hacker who uses their skills and knowledge for defensive purposes only. Many organizations and companies now employ these security analysts, who understand the hacker's mindset.

The gray hat hacker falls in the middle of the white hat and black hat hackers. The gray hat may cross the

line of what is ethical, but usually has good intentions and isn't being malicious like a black hat hacker.

A hacktivist often targets government agencies, corporations, or any entity they are protesting.

A script kiddie only uses tools and scripts that have been developed by others. This person has no desire to understand how these tools work and is extremely unskilled.

References

TestOut Ethical Hacker Pro - 2.2 Threat Actors
[e_threat_actors_eh1.exam.xml Q_ACTOR_TYPES_FACTS_01_EH1]

Question 3: Correct

Which statement best describes a suicide hacker?

- This hacker's main purpose is to protest an event and draw attention to their views and opinions.
- This hacker is motivated by religious or political beliefs and wants to create severe disruption or widespread fear.
- This hacker is only concerned with taking down their target for a cause. They have no concerns about being caught.
- This hacker may cross the line of what is ethical, but usually has good intentions and isn't being malicious.

Explanation

A suicide hacker is only concerned with taking down their target for a cause. This hacker has no concerns about being caught or going to jail.

A gray hat hacker falls in the middle of the white hat and black hat hackers. The gray hat may cross the line of what is ethical, but usually has good intentions and isn't being malicious like a black hat hacker.

A cyber terrorist is motivated by religious or political beliefs and wants to create severe disruption or widespread fear.

A hacktivist will often target government agencies, corporations, or any entity they are protesting. Their main purpose is to protest an event and draw attention to their views and opinions.

References

TestOut Ethical Hacker Pro - 2.2 Threat Actors
[e_threat_actors_eh1.exam.xml Q_ACTOR_TYPES_FACTS_02_EH1]

Question 4: Incorrect

Miguel has been practicing his hacking skills. He has discovered a vulnerability on a system that he did not have permission to attack. Once Miguel discovered the vulnerability, he anonymously alerted the owner and instructed him how to secure the system. What type of hacker is Miguel in this scenario?

- Script kiddie
- State-sponsored
- Gray hat
- ~~White hat~~

Explanation

A gray hat hacker falls in the middle of the white hat and black hat hackers. The gray hat may cross ethical lines, but usually has good intentions and isn't being malicious like a black hat hacker.

A white hat is a skilled hacker who uses their skills and knowledge for defensive purposes only. Many organizations and companies employ these security analysts, who understand the hacker's mindset.

A state-sponsored hacker works for a government and attempts to gain top-secret information by hacking other governments.

A script kiddie only uses tools and scripts that have been developed by others. This person has no desire to understand how these tools work and is extremely unskilled.

References

TestOut Ethical Hacker Pro - 2.2 Threat Actors
[e_threat_actors_eh1.exam.xml Q_ACTOR_TYPES_FACTS_03_EH1]

Question 5: Incorrect

The process of analyzing an organization's security and determining its security holes is known as:

- ~~Penetration testing~~
- Enumeration
- Threat modeling
- Ethical hacking

Explanation

Threat modeling is the process of analyzing an organization's security and determining its security holes. Once a threat model is put together, the organization can begin securing its systems and data.

Penetration testing is the practice of finding vulnerabilities and risks with the purpose of securing the computer or network system.

Ethical hacking is an all-embracing term that includes all hacking methods.

Extracting information such as usernames, computer names, network resources, shares, and services is called enumeration.

References

TestOut Ethical Hacker Pro - 2.2 Threat Actors
[e_threat_actors_eh1.exam.xml Q_ACTOR_TYPES_THREAT_MODEL_01_EH1]