Started on	State	Completed on
Friday, 10 May 2024, 10:31 AM	Finished	Friday, 10 May 2024, 10:37 AM

Time taken	Grade
5 mins 28 secs	9.40 out of 10.00 (94%)

Question 1

Complete

Mark 1.00 out of 1.00

q2-8a

Why would an attacker want to perform lateral movement after gaining initial access to a victim's computer or network?

- [ ] a. To better evade UEBA detection as it is common for a user to access multiple computers concurrently
- [x] b. To gain access to other sensitive data that may otherwise not be available to the attacker due to access control restriction
- [x] c. To create an indirect attack path to the victim's crown jewel as part of a distributed denial of service attack
- [ ] d. To assist in hardware and software inventory check as part of attack surface management
- [x] e. To perform a targeted attack as part of a spearphishing campaign
- [x] f. As an attempt to identify other network routes that may be able to bypass existing network defences such as strict firewall rules
- [ ] g. To oscillate and achieve simple harmonic motion, so as to cause physical damage to the network switches

Question 2

Complete

Mark 1.00 out of 1.00

q2-7a

Which of the following statement about the contents of security awareness training is/are correct?

- [ ] a. It should be delivered to only the C-suites as they are often targeted
- [x] b. It should be delivered to all employees
- [ ] c. It should remain the same for consistency, fairness and ease of measuring progress.
- [x] d. It should be constantly updated to include new attack techniques and relevant considerations

Question 3

Complete

Mark 1.00 out of 1.00

q2-3

Which of the following can safely remove the data stored within an SSD?

- [x] a. Perform an ATA-Secure wipe on the SSD, assuming the feature is supported
- [ ] b. Write the drive with "1" repeatedly for 7 times
- [ ] c. Encrypt the disk with numeric key and save it in a secure cloud repository
- [ ] d. Write a single pass of "0" for the entire drive
- [x] e. Encrypt the disk with a long random key and forget the key, then format the disk.

Question 4

Complete

Mark 1.00 out of 1.00

q2-7b

Which of the following statement about policy and procedure is/are correct?

- [x] a. Policy must be enforced by a proper authority while procedure outlines what needs to be done
- [x] b. Policy should not contain too much prescriptive technical information while procedure needs to provide enough details to facilitate execution
- [ ] c. Policy must include the mission while procedure must include the vision
- [ ] d. Policy must be prescriptive and definitive while procedure can be deliberately vague

Question 5

Complete

Mark 1.00 out of 1.00

q2-5

Which of the following statement(s) about Windows Registry and Windows Group Policy in a Windows Active Directory setting is/are true?

- [x] a. Group Policy is a Windows server feature that allows administrators to making changes to the working environment of user accounts and their associated computer. A Registry stores the program and system settings for a computer.
- [ ] b. Group Policy is a living document that needs to be maintained by the CISO while a registry is the document used to register vendors when they visit classified compound
- [ ] c. Group Policy is used to make configuration changes to one computer only while a Registry is used to implement changes for a group of computers
- [x] d. Group Policy can be used to implement changes in the Registry to harden a computer. Registry keys can be created to implement specific software logic changes as they act as configuration settings for the software
- [ ] e. Group Policy defines the rules for zero trust network setup while Registry defines the rules for lateral movement

Question 6

Complete

Mark 1.00 out of 1.00

q2-2

Why are IoT devices more prone to cyber attacks, compared to other devices like a server or a network router?

- [ ] a. Manufacturer prioritises security over functionality, and ensures hardware and software are secured by design, despite the increase in manufacturing cost.
- [x] b. Manufacturer often prioritises efficiency and functionality over security, resulting in security settings not turned on by default.
- [x] c. Users often leave their IoT devices in their default security configuration due to ignorance, complacency or laziness.
- [ ] d. Users often leave their IoT devices in their default security configuration as they are more secure

Question 7

Complete

Mark 1.00 out of 1.00

q2-1

Explain what the "Water Holing" attack is.

a. An attack strategy, in which the attacker guesses or observes which security product the group often uses and infects the up stream supply chain.

b. A physical attack against digital assets through the use of conductive material like water to short circuit and damage microprocessors

c. An attack strategy, in which the attacker guesses or observes which websites the group often uses and infects one or more of them with malware.

d. A cyber attack targeting Africa continent companies and entities

e. A security exploit that compromises a database server and corrupts its data

f. A software feature that relieves a visitor's thirst

g. An attack strategy, in which the attacker guesses or observes which email exchange server a company uses and perform a torrential waterfall-like bruteforce attack against them

h. A passive attack using nmap to identify vulnerabilities and using nmap scripts to further exfiltrate data

Question 8

Complete

Mark 1.00 out of 1.00

q2-4

How can "broken authentication" be prevented?

- [ ] a. Save all cookies and close the browser
- [x] b. Delete all cookies and perform a proper account log out, before closing the browser
- [ ] c. Click "Remember this computer" to save the session credentials within the browser cache
- [ ] d. Post the last used browser's URL in social media with the session ID embedded in the URL so that others can see the same funny meme that you saw.
- [x] e. When using a chrome browser, use it in "incognito" mode to ensure no credentials are saved, and perform proper log out before closing the browser.

Question 9

Complete

Mark 0.40 out of 1.00

q2-8b

Why do hackers use tools that are often pre-installed on specific operating systems (also known as "live off the land") to conduct their hands-on-keyboard attack?

- [ ] a. As a form of distraction and diversion while zero day malware is deployed somewhere else
- [x] b. To reduce maintenance overhead as the blue team would patch and update the system
- [ ] c. Living off the land can help save electricity bill
- [ ] d. Increases the attack complexity to confuse the blue team, so as to demonstrate the technical superiority of the red team
- [ ] e. For increased efficiency as the blue team would often deploy Robotic Process Automation software technology that can help the attack move laterally with ease
- [x] f. Evade detection as such attack can be "mistakenly" interpreted as system administration activities
- [ ] g. Using a custom malware will increase the risk of attack attribution as the blue team could potentially reverse engineer the malware

Question 10

Complete

Mark 1.00 out of 1.00

q2-6

Explain what pass-the-hash attack is?

- [ ] a. It is a hacking technique that allows an attacker to authenticate to a remote server or service by using the stolen multi-factor authentication token
- [ ] b. It is a hacking technique that allows an attacker to authenticate to a remote server or service by using a user's password, instead of the underlying NTLM or LanMan hash
- [x] c. It is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying NTLM or LanMan hash of a user's password, instead of requiring the associated plaintext password
- [ ] d. It is a hacking technique that allows an attacker to authenticate to a remote server or service by using the PKI private certificate instead of the user's hash

Finish review

Jump to...

On the lands that we study, we walk, and we live, we acknowledge and respect the traditional custodians and cultural knowledge holders of these lands.

University of Wollongong

Copyright © 2023 University of Wollongong
CRICOS Provider No: 00102E | TEQSA Provider ID: PRV12062 | ABN: 61 060 567 686
Copyright & disclaimer | Privacy & cookie usage | Web Accessibility Statement