Exam Report: 7.1.4 Practice Questions

Date: 5/2/2020 6:29:53 pm
Time Spent: 0:46

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 38%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

An ethical hacker is running an assessment test on your networks and systems. The assessment test includes the following items:

- Inspecting physical security
- Checking open ports on network devices and router configurations
- Scanning for Trojans, spyware, viruses, and malware
- Evaluating remote management processes
- Determining flaws and patches on the internal network systems, devices, and servers

Which of the following assessment tests is being performed?

- Active assessment
- ~~Passive assessment~~
- Internal assessment
- External assessment

Explanation

An internal assessment is an evaluation of a network that is created by testing and analyzing processes and systems inside the network. This assessment may include:

- Inspecting physical security
- Checking open ports on network devices and router configurations
- Scanning for Trojans, spyware, viruses, and malware
- Evaluating remote management processes
- Determining flaws and patches on the internal network systems, devices, and servers

An active assessment is an evaluation of a network that is created by actively testing the network for weaknesses. Specifically created packets are sent to target nodes to determine the OS of the domain, the host, services, and vulnerabilities in the network.

A passive assessment is an evaluation of a network that is created by looking for weaknesses through observation and no direct interaction with the network. Using sniffer traces from a remote system, the operating system of the remote host can be determined, as well as a list of the current users of the network

An external assessment is an evaluation of a network that is created by testing external systems and testing from outside the network. This assessment may include:

- Determining if maps exist for network and external service devices
- Checking for vulnerabilities in web applications
- Examining the rule set for external network router configurations and firewalls
- Detecting open ports on the external network and services
- Identifying DNS zones

References

TestOut Ethical Hacker Pro - 7.1 Vulnerability Assessment
[e_vuln_assessment_eh1.exam.xml Q_VULN_ASSESSMENT_ASSESS_TYPES_01_EH1]

Question 2: Correct

In a world where so much private information is stored and transferred digitally, it is essential to proactively discover weaknesses. An ethical hacker's assessment sheds light on the flaws that can open doors for malicious attackers. Which of the following types of assessments does an ethical hacker complete to expose these weeknesses?

- Host-based assessment
- Passive assessment
- External assessment
- Vulnerability assessment

Explanation

A vulnerability assessment refers to identifying weaknesses in an organization infrastructure, including its operating system, web applications, and web server.

A host-based assessment focuses on all types of user risks, including threats from malicious users, ignorant users, vendors, and administrators.

A passive assessment uses sniffer traces from a remote system. The operating system of the remote host can be determined, as well as a list of the current users of the network.

An external assessment is external because it works from the outside, using public networks through the internet.

References

TestOut Ethical Hacker Pro - 7.1 Vulnerability Assessment
[e_vuln_assessment_eh1.exam.xml Q_VULN_ASSESSMENT_ASSESS_TYPES_02_EH1]

Question 3: Incorrect

Which of the following assessment types focus on all types of user risks, including threats from malicious users, ignorant users, vendors, and administrators?

- External assessment
- Passive assessment
- ~~Wireless network assessment~~
- Host-based assessment

Explanation

A host-based assessment focuses on all types of user risks, including threats from malicious users, ignorant users, vendors, and administrators. Host-based assessment can also test the vulnerability of databases, firewalls, files, and web servers, and flag configuration errors.

In a wireless network assessment, a hacker can access sensitive information even from outside a building by sniffing network packets that are transmitted wirelessly through radio waves.

An external assessment looks for ways to access the network infrastructure through open firewall ports, routers, web servers, web pages, and public DNS servers.

A passive assessment uses sniffer traces from a remote system to determine a remote host's operating system and/or discover a network's current users.

References

TestOut Ethical Hacker Pro - 7.1 Vulnerability Assessment
[e_vuln_assessment_eh1.exam.xml Q_VULN_ASSESSMENT_ASSESS_TYPES_03_EH1]

Question 4: Incorrect

On your network, you have a Windows 10 system with the IP address 10.10.10.195. You have installed XAMPP along with some web pages, php, and forms. You want to put it on the public-facing internet, but you are not sure if it has any vulnerabilities. On your Kali Linux system, you have downloaded the nmap-vulners script from GitHub. Which of the following is the correct nmap command to run?

- ~~**nmap -sC nmap-vulners -sV 10.10.10.195**~~
- **nmap --script vulners -sV 10.10.10.195**
- **nmap --script nmap-vulners -sV 10.10.10.195**
- **nmap -sC vulners -sV 10.10.10195**

Explanation

The command you will enter is **nmap --script nmap-vulners -sV 10.10.10.195**. The --script switch performs a script scan using the comma-separated list of filenames, script categories, and directories.

The -sC switch performs a script scan using the default set of scripts.

References

TestOut Ethical Hacker Pro - 7.1 Vulnerability Assessment
[e_vuln_assessment_eh1.exam.xml Q_VULN_ASSESSMENT_VULN_ASSESS_SCAN_01_EH1]

Question 5: Correct

This type of assessment evaluates deployment and communication between the server and client. It is imperative to develop tight security through user authorization and validation. Open-source and commercial tools are both recommended for this assessment. Which of the following types of vulnerability research is being done?

- Buffer overflows
- Application flaws
- Open services
- Default settings

Explanation

Flaws, while validating and authorizing the user, present the greatest threat to security in transactional applications. This type of assessment evaluates deployment and communication between the server and client. It is imperative to develop tight security through user authorization and validation. Open-source and commercial tools are both recommended for this assessment.

A buffer is a temporary data storage area with limited space. Overflows occur when users attempt to store more data than the program was written for.

Ports and services must be checked regularly to prevent unsecure, open, or unnecessary ports, which can lead to attacks on connected nodes or devices, loss of private information, or even denial of service.

It is important to check default settings, especially for default SSIDs and admin passwords.

References

TestOut Ethical Hacker Pro - 7.1 Vulnerability Assessment
[e_vuln_assessment_eh1.exam.xml Q_VULN_ASSESSMENT_VULN_RESEARCH_01_EH1]

Question 6: Correct

Jaxon, a pentester, is discovering vulnerabilities and design flaws on the Internet that will open an operating system and applications to attack or misuse. Which of the following tasks is he accomplishing?

- Vulnerability management
- Vulnerability scanning

- Vulnerability research
- Vulnerability assessment

Explanation

Vulnerability research is the process of discovering vulnerabilities and design flaws that will open an operating system and its applications to attack or misuse. Time is on the attacker's side. It is crucial for an ethical hacker to put in the effort and time to research an organization from the outside in and to scan and gather information at every level.

Vulnerability assessment refers to identifying weaknesses in the organization infrastructure, including the operating system, web applications, and web servers.

Vulnerability scanning attempts to find points that can be exploited on a computer or network.

An ethical hacker uses the vulnerability management life cycle to protect their organization.

References

TestOut Ethical Hacker Pro - 7.1 Vulnerability Assessment
[e_vuln_assessment_eh1.exam.xml Q_VULN_ASSESSMENT_VULN_RESEARCH_02_EH1]

Question 7: Incorrect

Which of the following best describes active scanning?

- A scanner transmits to a network node to determine exposed ports and can also independently repair security flaws.
- A scanner is limited to the moment in time that it is running and may not catch vulnerabilities that only occur at other times.
- A scanner allows the ethical hacker to scrutinize completed applications when the source code is unknown.
- ~~A scanner tries to find vulnerabilities without directly interacting with the target network.~~

Explanation

An active scanner transmits to the nodes within a network to determine exposed ports and can also independently repair security flaws.

A passive scanner tries to find vulnerabilities without directly interacting with the target network.

A point in time scan is limited to the moment in time that it is running and may not catch vulnerabilities that only occur at other times.

Application-level scans allow the ethical hacker to scrutinize completed applications when the source code is unknown.

References

TestOut Ethical Hacker Pro - 7.1 Vulnerability Assessment
[e_vuln_assessment_eh1.exam.xml Q_VULN_ASSESSMENT_VULN_SCAN_TYPES_01_EH1]

Question 8: Incorrect

Which of the following assessment types can monitor and alert on attacks but cannot stop them?

- External
- Passive
- ~~Vulnerability~~
- Host-based

Explanation

Passive assessment uses sniffer traces from a remote system to determine a remote host's operating system and/or a network's current users. Wireshark is a common tool for this information gathering. It establishes the information retrieved from the sniffer traces obtained from the packets.
Vulnerability assessment refers to identifying weaknesses in the organization infrastructure, including the operating system, web applications, and web servers.

Host-based assessment focuses on all types of user risks, including threats from malicious users, ignorant users, vendors, and administrators.

External assessment is external because it is working from the outside using public networks.

References

TestOut Ethical Hacker Pro - 7.1 Vulnerability Assessment
[e_vuln_assessment_eh1.exam.xml Q_VULN_ASSESSMENT_VULN_SCAN_TYPES_02_EH1]