Exam Report: 4.1.8 Practice Questions

Date: 5/2/2020 2:28:14 pm
Time Spent: 4:24

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 75%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

When a penetration tester starts gathering details about employees, vendors, business processes, and physical security, which phase of testing are they in?

- Covering tracks
- Reconnaissance
- Gaining access
- Scanning

Explanation

During the reconnaissance phase, you gather information about a company. In addition to technical information, you'll want to gather details about employees, vendors, business processes, and physical security.

During the scanning phase, you gather additional technical information about your target, more specifically, the systems that they have in place.

During the gaining access phase, you take control of one or more network devices and either extract data from the target or use that device to launch attacks on other targets.

During the covering tracks phase, you take the steps necessary to remove evidence of your attack.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_PROCESS_FACT_01_EH1]

Question 2: Correct

Which of the following elements of penetration testing includes the use of web surfing, social engineering, dumpster diving, and social networking?

- Information types
- Information gathering techniques
- Permission and documentation
- Maintaining access

Explanation

During the reconnaissance phase, you gather information by reading a company's website, getting to know their employees, or dumpster diving.

Before beginning work of any kind, an ethical hacker needs to obtain written documentation granting permission from the customer.

During the reconnaissance phase, you gather information about a company. In addition to technical information, you'll want to gather details about employees, vendors, business processes, and physical security.
Maintaining access is taking steps to be persistently within the target environment to gather as much data as possible.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_PROCESS_INFO_GATHER_TECH_01_EH1]

Question 3: Correct

MinJu, a penetration tester, is testing a client's security. She notices that every Wednesday, a few employees go to a nearby bar for happy hour. She goes to the bar and starts befriending one of the employees with the intention of learning the employee's personal information. Which information gathering technique is MinJu using?

- Social engineering
- Social networking
- Dumpster diving
- Web surfing

Explanation

Social engineering is an attempt to get to know a company's employees or vendors. After-work social gatherings can provide important tidbits of information about an employee and about a company, especially its weaknesses.

Despite our highly technical society, dumpster diving is still a viable hacking option. It's not the most glamorous method. But, in some instances, it may be very effective for finding employee names, account numbers, client names, and vendor information.

Web surfing can help you research company websites, social media, discussion groups, financial reports, and news articles. If you follow the breadcrumbs, you can find some pretty interesting information about an organization online.

Social networking is what you do after you've located employee names. You can extend your search to LinkedIn, Facebook, Instagram, Twitter, or People Search to learn even more information about a company, a vendor, or an employee.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_PROCESS_INFO_GATHER_TECH_02_EH1]

Question 4: Correct

A penetration tester is trying to extract employee information during the reconnaissance phase. What kinds of data is the tester collecting about the employees?

- Contact names, phone numbers, email addresses, fax numbers, and addresses
- Operating systems, applications, security policies, and network mapping
- Geographical information, entry control systems, employee routines, and vendor traffic
- Intellectual property, critical business functions, and management hierarchy

Explanation

During the reconnaissance phase, you gather information about a company. For employee information, the penetration tester collects contact names, phone numbers, email addresses, fax numbers, and addresses for any individuals associated with the target company.

For information systems, the tester collects information about the operating systems, applications, security policies, and network mapping.

For operations, the tester collects information about intellectual property, critical business functions, and management hierarchy.
For physical security, the tester collects information about geographical location and sorroundings, entry control systems, employee routines, and vendor traffic.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_PROCESS_INFO_TYPE_01_EH1]

Question 5: Correct

Which of the following is the difference between an ethical hacker and a criminal hacker?

- A criminal hacker is easily detected, but an ethical hacker isn't.
- An ethical hacker is nice, clean, and polite, but a criminal hacker isn't.
- An ethical hacker has permission to hack a system, and a criminal hacker doesn't have permission.
- A criminal hacker is all-knowing, but an ethical hacker isn't.

Explanation

The difference between an ethical hacker and a criminal hacker is that an ethical hacker always obtains permission to hack a system.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_PROCESS_PERMISSION_DOC_01_EH1]

Question 6: Correct

Whois, Nslookup, and ARIN are all examples of:

- Network footprinting tools
- Google hacking tools
- IoT hacking tools
- Internet research tools

Explanation

Website and email footprinting can provide details on information flow, operating systems, filenames, and network connections. Whois, nslookup, and ARIN are examples of footprinting tools.

Despite its name, Google hacking is legal because all of the results are pulled from public websites. By adding a few operators, you can use the Google search engine to provide filtered information about a specific topic. A few of the operators include *info:website, link:website, related:website, index of /keyword, intitle:keyword,* and *allinurl:keywords*.

Internet research tools include Google Earth, Google Maps, Webcams, Echosec, Maltego, and Wayback Machine.

IoT hacking tools include Censys, Zniffer, Shodan, Thingful, and beSTORM.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_TOOLS_FOOTPRINT_TOOLS_01_EH1]

Question 7: Incorrect

Iggy, a penetration tester, is conducting a black box penetration test. He wants to do reconnaissance by gathering information about ownership, IP addresses, domain name, locations, and server types. Which of the following tools would be most helpful?

- Whois

- beSTORM
- ~~Nslookup~~
- ARIN

Explanation

Whois is a utility used to gain information about a target network. It can gather information about ownership, IP addresses, domain name, location, server type, and the date the site was created.

ARIN is a website that will provide you with information about a network's name, range, origination dates, and server details.

Nslookup is a utility used to query DNS servers to obtain information about the host network including DNS records and host names.

beSTORM is a smart fuzzer that finds buffer overflow weaknesses as it automates and documents the process of delivering malicious input and then watches for unpredicted responses from an application.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_TOOLS_FOOTPRINT_TOOLS_02_EH1]

Question 8: Correct

What does the Google Search operator *allinurl:keywords* do?

- Shows results in pages that contain the keyword in the title.
- Shows results in pages that contain all of the listed keywords.
- Displays websites where directory browsing has been enabled.
- Displays web sites similar to the one listed.

Explanation

allinurl:keywords shows results in pages that contain all of the listed keywords.

index of /keyword displays websites where directory browsing has been enabled.

intitle:keyword shows results in pages that contain the keyword in the title.

related:website displays websites similar to the one listed.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_TOOLS_GOOGLE_HACK_01_EH1]

Question 9: Correct

What's the name of the open-source forensics tool that can be used to pull information from social media postings and find relationships between companies, people, email addresses, and other information?

- Echosec
- Wayback Machine
- Google Earth
- Maltego

Explanation

Maltego is an open-source forensics tool that can be used to pull information from social media postings and find relationships between companies, people, email addresses, and other information.

The Wayback Machine is a non-profit catalog of old site snapshots and may contain information that your target thought they had removed from the internet.

Echosec is a tool that can be used to pull information from social media postings that were made using location services. You can select a location on a map and view all posts that have occurred at that location. These results can be filtered by user, date, or keyword.

Google Earth is a satellite imagery tool that provides current and historical images of most locations. Images can date back several decades.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_TOOLS_INTERNET_RESEARCH_01_EH1]

Question 10: Incorrect

Xavier is doing reconnaissance. He is gathering information about a company and its employees by going through their social media content. Xavier is using a tool that pulls information from social media postings that were made using location services. What is the name of this tool?

- Echosec
- Wayback Machine
- ~~Maltego~~
- Google Maps

Explanation

Echosec is a tool that can be used to pull information from social media postings that were made using location services.

The Wayback Machine is a nonprofit catalog of old site snapshots and may contain information that your target thought they had removed from the internet.

Google Maps is a web mapping service that provides a street view of houses, businesses, roadways, and topologies.

Maltego is an open-source forensics tool that can be used to pull information from social media postings and find relationships between companies, people, email addresses, and other information.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_TOOLS_INTERNET_RESEARCH_02_EH1]

Question 11: Incorrect

You are in the reconnaissance phase at the XYZ company. You want to use nmap to scan for open ports and use a parameter to scan the 1,000 most common ports. Which nmap command would you use?

- **nmap -sS xyzcompany.com**
- **nmap -sV xyzcompany.com**
- **nmap -sT xyzcompany.com**
- ~~**nmap -sA xyzcompany.com**~~

Explanation

-sS TCP SYN port scan (default) scans the 1,000 most common ports.

-sV attempts to determine the version of the service running on port.

-sT TCP connects a port scan (default without root privilege).

-sA executes a TCP ACK port scan.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_TOOLS_NMAP_01_EH1]

Question 12: Correct

You have found the IP address of a host to be 172.125.68.30. You want to see what other hosts are available on the network. Which of the following nmap commands would you enter to do a ping sweep?

- **nmap -sS 172.125.68. 1-255**
- **nmap -sU 172.125.68. 1-255**
- **nmap -sn 172.125.68. 1-255**
- **nmap -sM 172.125.68. 1-255**

Explanation

The **nmap -sn** command is used to disable port scanning. The command **nmap -sn 172.125.8. 1-225** will scan a range of ip addresses without listing the ports.

The **nmap -sS** command is used for a TCP SYN port scan (default).

The **nmap -sU** command is used for UDP port scans.

The **nmap -sM** command is used for TCP Maimon port scans.

References

TestOut Ethical Hacker Pro - 4.1 Reconnaissance Overview
[e_recon_eh1.exam.xml Q_RECON_TOOLS_NMAP_02_EH1]