Exam Report: 6.1.13 Practice Questions

Date: 5/2/2020 6:14:03 pm
Time Spent: 3:17

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 50%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

In which phase of the ethical hacking process do you gather information from a system to learn more about its configurations, software, and services?

- Sniffing
- Scanning
- Reconnaissance
- Enumeration

Explanation

Enumeration is the method of gathering information from a system to learn more about its configurations, software, and services.

Scanning is the method of using various tools to gather in-depth information on a network.

Reconnaissance is the method of gathering publicly available information about a target.

Sniffing is the process of collecting information as it crosses a network.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMERATION_ENUM_FACTS_01_EH1]

Question 2: Correct

Which enumeration process tries different combinations of usernames and passwords until it finds something that works?

- Brute force
- Default passwords
- Exploiting SMTP
- Zone transfers

Explanation

Brute force attacks are usually automated. A program tries different combinations of usernames and passwords until it finds something that works.

Simple Mail Transfer Protocol (SMTP) is the protocol used by most email servers and clients to send email messages.

A DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server.

All devices have default passwords. These passwords are often left in place, providing an easy access point for an attacker.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMERATION_ENUM_PROCESS_01_EH1]

Question 3: Correct

Which of the following best describes IPsec enumeration?

- Is used by most email servers and clients to send email messages.
- Uses ESP, AH, and IKE to secure communication between VPN endpoints.
- Uses SIP to enable voice and video calls over an IP network.
- Is used to manage devices such as routers, hubs, and switches.

Explanation

IPsec uses ESP (Encapsulation Security Payload), AH (Authentication Header), and IKE (Internet Key Exchange) to secure communication between virtual private network endpoints. Using enumeration tools, attackers can pull sensitive information such as the encryption and hashing algorithm, authentication type, and key distribution algorithm.

The Simple Network Management Protocol (SNMP) is used to manage devices such as routers, hubs, and switches. SNMP works with an SNMP agent and an SNMP management station. The agent is found on the device that is being managed, and the SNMP management station serves as the communication point for the agent.

VoIP uses SIP (Session Initiation Protocol) to enable voice and video calls over an IP network. SIP service generally uses UDP/TCP ports 2000, 2001, 5050, and 5061.

Simple Mail Transfer Protocol (SMTP) is the protocol used by most email servers and clients to send email messages. Scanning tools and commands can be used to verify the existence of specific email addresses and can even provide a list of all users on a distribution list.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMERATION_ENUM_PROCESS_02_EH1]

Question 4: Incorrect

Which of the following enumeration tools provides information about users on a Linux machine?

- SuperScan
- Null session
- ~~PsTools~~
- finger

Explanation

Using the **finger** command on Linux machines provides information about a user. When executed, it returns information such as the user's home directory, login time, idle times, office location, and the last time they received or read mail.

PsTools is a suite of very powerful tools that allow you to manage local and remote Windows systems. The package includes tools that can change account passwords, suspend processes, measure network performance, dump event log records, kill processes, view services, and control services.

SuperScan can be used to enumerate information from a Windows host. Information can be gathered about NetBIOS name table, services, NULL session, trusted domains, MAC addresses, logon sessions, workstation type, account policies, users, and groups.

Null Sessions are created when no credentials are used to connect to a Windows system. They are designed to allow clients access to limited types of information across a network.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMERATION_ENUM_TOOLS_01_EH1]

Question 5: Incorrect

The Simple Network Management Protocol (SNMP) is used to manage devices such as routers, hubs, and switches. SNMP works with an SNMP agent and an SNMP management station in which layer of the OSI model?

- ~~Transport Layer~~
- Application Layer
- Session Layer
- Network Layer

Explanation

The Application Layer (Layer 7) supports application and end-user processes. Examples include NFS, SNMP, Telnet, HTTP, and FTP.

The Session Layer (Layer 5) establishes, manages, and terminates connections between applications. Examples include NFS, NetBIOS names, RPC, and SQL.

The Transport Layer (Layer 4) provides transparent transfer of data between end systems or hosts. Examples include SPX, TCP, and UDP.

The Network Layer (Layer 3) prides switching and routing technologies. Examples include AppleTalk, DDP, IP, and IPX.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMERATION_ENUM_TOOLS_02_EH1]

Question 6: Incorrect

A hacker has managed to gain access to the /etc/passwd file on a Linux host. What can the hacker obtain from this file?

- ~~Usernames and passwords~~
- The root username and password
- Usernames, but no passwords
- No usernames or passwords

Explanation

The /etc/passwd file on a Linux host contains the following:

- The username and user ID used to identify each user.
- Passwords that are encrypted and saved on the computer or on the network.
- Group identification numbers (GIDs).

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMERATION_LINUX_ENUM_01_EH1]

Question 7: Incorrect

Jorge, a hacker, has gained access to a Linux system. He has located the usernames and IDs. He wants the hashed passwords for the users that he found. Which file should he look in?

- /etc/shadow
- /etc/group

~~/etc/passwd~~

/etc/services

Explanation

The hashed passwords are stored in the /etc/shadow file.

The list of groups is stored in the /etc/group file.

The list of running services is stored in the /etc/services file.

The username and ID is stored in the /etc/passwd file.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMERATION_LINUX_ENUM_02_EH1]

Question 8: Incorrect

Typically, you think of the username as being the unique identifier behind the scenes, but Windows actually relies on the security identifier (SID). Unlike the username, a SID cannot be used again. When viewing data in the Windows Security Account Manager (SAM), you have located an account ending in -501. Which of the following account types did you find?

~~The built-in administrator~~

The domain guests

The built-in guest

The domain admins

Explanation

The Guest account is a user account for people who do not have individual accounts. The SID ends with -501.

The Administrator account is a user account for the system administrator. The SID ends with -500.

The Domain Admins group is a global group whose members are authorized to administer the domain. The SID ends with -512.

The Domain Guests group is a global group that, by default, has only one member, the domain's built-in Guest account. The SID ends with -514.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMERATION_WINDOWS_ENUM_01_EH1]

Question 9: Correct

What port does a DNS zone transfer use?

TCP 139

TCP 445

TCP 23

TCP 53

Explanation

Port 53 is used for DNS zone transfers.

Port 23 is used for the Telnet protocol/software.

Port 139 is used by the NetBIOS Session Service .

Port 445 is used by SMB over TCP.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMPORTS_SERV_EMUM_PORTS_SERV_FACTS_01_EH1]

Question 10: Correct

Which of the following ports are used by null sessions on your network?

- 139 and 444
- 137 and 443
- 135 and 445
- 139 and 445

Explanation

A Null Session attack uses the Windows **net** command to map a connection using a blank username and password. These connections would take place over port 139 (NetBIOS sessions services) or 445 (runs SMB over TCP/IP without NetBIOS).

Port 135 is used by the Remote Procedure Call service in Windows for client-server communications.

Port 137 is used by the NetBIOS Name Server (NBNS). NBNS is used to associate names and IP addresses of systems and services.

Port 443 is the standard TCP port that is used for websites that use SSL.

Port 444 may use a defined protocol to communicate, depending on the application.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMPORTS_SERV_EMUM_PORTS_SERV_FACTS_02_EH1]

Question 11: Correct

LDAP is an internet protocol for accessing distributed directory services. If this port is open, it indicates that Active Directory or Exchange may be in use. What port does LDAP use?

- TCP/UDP 3268
- TCP/UDP 389
- TCP/UDP 445
- TCP/UDP 53

Explanation

TCP/UDP port 389 is used by the Lightweight Directory Access Protocol (LDAP.)

TCP/UDP port 3268 is used by the Global Catalog Service.

TCP port 53 is used for DNS zone transfers. UDP port 53 is used for UDP queries about IP-to-name and name-to-IP mappings.

TCP port 445 is used by SMB over TCP.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMPORTS_SERV_EMUM_PORTS_SERV_FACTS_03_EH1]

Question 12: Incorrect

Shawn, a malicious insider, has obtained physical access to his manager's computer and wants to listen for incoming connections. He has discovered the computer's IP address, 192.168.34.91, and he has downloaded netcat. Which of the following netcat commands would he enter on the two computers?

- **nc -l -s 2222** (manager's computer) and **nc -pv 192.168.34.91 2222** (Shawn's machine)

- ~~**nc -l -p 2222** (manager's computer) and **nc -sv 192.168.34.91 2222** (Shawn's machine)~~
- **nc -n -s 2222** (manager's computer) and **nc -lp 192.168.34.91 2222** (Shawn's machine)
- **nc -l -p 2222** (manager's computer) and **nc -nv 192.168.34.91 2222** (Shawn's machine)

Explanation

On the manager's computer, Shawn would enter **nc -l -p 2222** (the -l switch listens for an incoming connection, and the -p switch tells netcat to use specific source port). On Shawn's computer, he would enter **nc -nv 192.168.34.91 2222** (the -n switch tells netcat not to use DNS lookups, and the -v switch uses verbose output).

The -s switch tells netcat to use the source IP address.

References

TestOut Ethical Hacker Pro - 6.1 Enumeration Overview
[e_enumeration_eh1.exam.xml Q_ENUMPORTS_SERV_EMUM_WINDOW_01_EH1]