Exam Report: 5.2.3 Practice Questions

Date: 5/2/2020 5:53:08 pm
Time Spent: 3:17

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 20%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

Information transmitted by the remote host can be captured to expose the application type, application version, and even operating system type and version. Which of the following is a technique hackers use to obtain information about the services running on a target system?

- ○ Firewalking
- ○ Wardialing
- ○ Wardriving
- ➡ ● Banner grabbing

Explanation

Banner grabbing is a technique hackers use to obtain information about the services running on a target system. Capturing information transmitted by the remote host includes the application type, application version, and even operating system type and version.

Firewalking is using traceroute techniques to discover which services can pass through a firewall or a router.

Wardriving is scanning for wireless access points within the organization.

Wardialing is trying to access phone lines that will answer a calling modem.

References

TestOut Ethical Hacker Pro - 5.2 Banner Grabbing
[e_banner_eh1.exam.xml Q_BANNER_GRAB_BANNER_GRAB_FACT_01_EH1]

Question 2: Incorrect

Joe wants to use a stealthy Linux tool that analyzes network traffic and returns information about operating systems. Which of the following banner grabbing tools is he most likely to use?

- ➡ ○ P0f
- ○ Netcraft
- ○ Telnet
- ● ~~Shodan~~

Explanation

P0f is a Linux tool that analyzes network traffic and returns information on operating systems. Because it passively views traffic, it is a stealthy method for gathering information.

Telnet operates on port 23. These banners can include some interesting information about the target system, such as software type, software version, services, patches, and the latest modification date.

Netcraft is an online tool used to obtain server and web server information.
Shodan is a search engine for finding specific devices and device types that exist online. The most popular searches are for things like webcams, routers, switches, and servers. Shodan works by scanning the entire internet and analyzing the banners returned by devices.

References

TestOut Ethical Hacker Pro - 5.2 Banner Grabbing
[e_banner_eh1.exam.xml Q_BANNER_GRAB_BANNER_GRAB_TOOL_01_EH1]

Question 3: Incorrect

Nmap can be used for banner grabbing. Nmap connects to an open TCP port and returns anything sent in a five-second period. Which of the following is the proper nmap command?

○ **nmap -sN --script=banner *ip_address***

● ~~**nmap -sX --script=banner *ip_address***~~

○ **nmap -sT --script=banner *ip_address***

➡ ○ **nmap -sV --script=banner *ip_address***

Explanation

Nmap attempts to determine the version of the service running on a port using **nmap -sV -script=banner ip_address**.

When a packet is sent with no flags set and the port is open, there will be no response. You can check this lack of response with; **nmap -sN *ip_address.***

An Xmas tree scan gets its name because all of the flags are turned on, and the packet is lit up like a Christmas tree. To do an Xmas tree scan, use **nmap -sX -v *ip_address.***

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

References

TestOut Ethical Hacker Pro - 5.2 Banner Grabbing
[e_banner_eh1.exam.xml Q_BANNER_GRAB_BANNER_GRAB_TOOL_02_EH1]

Question 4: Incorrect

Which of the following is an online tool that is used to obtain server and web server information?

○ Telnet

● ~~nmap~~

➡ ○ Netcraft

○ P0f

Explanation

Netcraft is an online tool that is used to obtain server and web server information.

P0f is a Linux tool that analyzes network traffic and returns information about operating systems. Because it passively views traffic, it is a stealthy method for gathering information.

Telnet is a command line tool that can be used for banner grabbing and operates on port 23. These banners can include some interesting information about the target system including software type, software version, services, patches, and the latest modification date.

Nmap is a command line tool that can be used for banner grabbing. Nmap connects to an open TCP port and returns anything set in a five-second period.

References

TestOut Ethical Hacker Pro - 5.2 Banner Grabbing
[e_banner_eh1.exam.xml Q_BANNER_GRAB_BANNER_GRAB_TOOL_03_EH1]

Question 5: Incorrect

Which of the following best describes telnet?

- ○ An online tool that is used to obtain server and web server information.
- ○ A Linux tool that analyzes network traffic and returns information about operating systems.
- ➡ ○ The tool of choice for banner grabbing that operates on port 23.
- ● ~~A tool that connects to an open TCP port and returns anything sent in a five-second period.~~

Explanation

Telnet is a tool that can be used for banner grabbing. It operates on port 23. If you type telnet*ip_address*, you'll send TCP packets to the destination port 23. However, by tacking a port number onto the end of the same command, you can check for other openings. If the port is open, you'll receive a banner response. These banners can include some interesting information about the target system, such as software type, software version, services, patches, and the last modification date.

Netcraft is an online tool that is used to obtain server and web server information.

P0F is a Linux tool that analyzes network traffic and returns information on operating systems. Because it passively views traffic, it is a stealthy method for gathering information.

Nmap can be used for banner grabbing. Nmap connects to an open TCP port and returns anything sent in a five-second period. The command syntax is **nmap -sV --script=banner ip_address**.

References

TestOut Ethical Hacker Pro - 5.2 Banner Grabbing
[e_banner_eh1.exam.xml Q_BANNER_GRAB_BANNER_GRAB_TOOL_04_EH1]