Exam Report: 8.3.7 Practice Questions

Date: 5/4/2020 9:23:08 pm
Time Spent: 0:23

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 40%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following is malware that works by stealth to capture information and then sends it to a hacker to gain remote access?

● ~~ERD Commander~~

○ Crackers

○ Writable services

➡ ○ Spyware

Explanation

Spyware is malware that works by stealth to capture information and sends it to a hacker to gain remote access. It can be keystroke logging, activity tracking, screen captures, or file operations. Spyware can be unintentionally installed by a user through normal web activity and is often undetectable.

Crackers are software programs that crack code and passwords to gain unauthorized access to a system. There are many methods and tools available for this approach to maintaining access, like dictionary, brute force, and rainbow attacks.

Writable Services have weak permissions that allow anyone to alter the execution of the service.

ERD Commander is software designed to correct problems that can occur when rebooting after you install new software on a Windows NT system. It allows users access to the command prompt to perform basic system maintenance tasks during the boot process.

References

TestOut Ethical Hacker Pro - 8.3 Maintain Access
[e_maintain_access_eh1.exam.xml Q_MAINTAIN_ACCESS_EXPLOIT_SYS_FACTS_01_EH1]

Question 2: Incorrect

Which of the following do hackers install in systems to allow them to have continued admittance, gather sensitive information, or establish access to resources and operations within the system?

○ cPassword

○ Kerberos

● ~~Crackers~~

➡ ○ Backdoors

Explanation

Backdoors allow continued admittance, gather sensitive information for exploitation, or establish access to resources and operations within the system. Hackers can leave the backdoor open by installing

rootkits, Trojan horses, and RATs, or remote access Trojans.
Kerberos is a protocol that allows authentication over a non-secure network using tickets or service principal names.

cPassword is the attribute that stores passwords in a Group Policy preference item.

Crackers are software programs that crack code and passwords to gain unauthorized access to a system.

References

TestOut Ethical Hacker Pro - 8.3 Maintain Access
[e_maintain_access_eh1.exam.xml Q_MAINTAIN_ACCESS_EXPLOIT_SYS_FACTS_02_EH1]

▼ **Question 3:** Incorrect

Hackers can maintain access to a system in several ways. Which of the following best describes the unsecure file and folder method?

➡ ○ This can lead to DLL hijacking and malicious file installations on a non-admin targeted user.

○ Services with weak permissions allow anyone to alter the execution of the service.

○ The hacker will have rights to do whatever the admin account can do.

● ~~There is no problem if the path is written within quotation marks and has no spaces.~~

Explanation

Older versions of Windows allow administrators to access the files and folders of any non-admin user. This can lead to DLL hijacking and malicious file installations on a non-admin targeted user.

Another way to exploit a service is to search for admin level accounts that have services that are writable. Services with weak permissions allow anyone to alter the execution of the service. This may include creating a new admin user account that gives the hacker rights to do whatever the admin account can do.

When an executable such as an app, service, or process is started, the system looks for a path for the file that runs it. There is no problem if the path is written within quotation marks and has no spaces. However, if the path name doesn't have quotation marks around it and there are spaces in the path name, there is an opportunity for a hacker to add a path that routes to a malicious file.

References

TestOut Ethical Hacker Pro - 8.3 Maintain Access
[e_maintain_access_eh1.exam.xml Q_MAINTAIN_ACCESS_EXPLOIT_SYS_FACTS_03_EH1]

▼ **Question 4:** Correct

Which of the following system exploitation methods happens by adding a malicious file to a file path that is missing quotation marks and has spaces in it?

➡ ● Path interception

○ Unsecure file and folder permissions

○ Spyware

○ Writable services

Explanation

In path interception, a hacker uses the way services normally operate to cause an unintended program to run. When a service is started, it looks for a path to the file that runs the service. There is no problem if the path is written within quotation marks and has no spaces. But if it doesn't have quotation marks around it and it has spaces in the code, there is an opportunity for a hacker to add a malicious file name to the path and reroute it to the malicious file. If the service runs with admin or system rights, the hacker can gain escalated privileges as soon as the system restarts.

Older versions of Windows allow administrators to access any non-admin user's files and folders, which can lead to DLL hijacking and malicious file installations on a non-admin targeted user.

Writable services are services with weak permissions that allow anyone to alter the execution of the service.

Spyware is malware that stealthily captures information and sends it to a hacker.

References

TestOut Ethical Hacker Pro - 8.3 Maintain Access
[e_maintain_access_eh1.exam.xml Q_MAINTAIN_ACCESS_EXPLOIT_SYS_FACTS_04_EH1]

Question 5: Correct

A hacker finds a system that has a poorly design and unpatched program installed. He wants to create a backdoor for himself. Which of the following tools could he use to establish a backdoor?

○ CCleaner

➡ ● Metasploit

○ Timestomp

○ AuditPol

Explanation

Metasploit is a computer security project that can be used to detect vulnerabilities in a system. Like most useful tools, it can also be used to create a backdoor and exploit the vulnerabilities.

Timestomp is a tool for modifying or deleting a timestamp on a file in order to hide when it was created, accessed, or modified.

CCleaner is a cleaning tool that can remove files and clear internet browsing history. It also frees up hard disk space. It clears the temporary files, history, and cookies from each of the six major search engines.

AuditPol is a utility you can use to retrieve, set, back up, and restore logging policies on Windows.

References

TestOut Ethical Hacker Pro - 8.3 Maintain Access
[e_maintain_access_eh1.exam.xml Q_MAINTAIN_ACCESS_EXPLOIT_SYS_FACTS_05_EH1]