Exam Report: 8.2.9 Practice Questions

Date: 5/4/2020 8:42:18 pm
Time Spent: 2:51

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 44%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Roger, a security analyst, wants to tighten up privileges to make sure each user has only the privileges they need to do their work. Which of the following additional countermeasure could he take to help protect privelige?

- Create plain text storage for passwords.
- Instigate multi-factor authentication and authorization.
- Allow unrestricted interactive logon privileges.
- ~~Restrict the interactive logon privileges.~~

Explanation

Instigating multi-factor authentication and authorization is important for preventing escalation because it adds more layers to protect unauthorized access.

Restrict the interactive logon privileges to have higher security during the logon process.

Always use encryptions for sensitive information. Never store passwords in plain text.

Perform updates often on operating systems and applications as they regularly fix bugs and add protection.

References

TestOut Ethical Hacker Pro - 8.2 Privilege Escalation
[e_priv_escalation_eh1.exam.xml Q_PRIV_ESCALATION_COUNTERMEASURE_01_EH1]

Question 2: Incorrect

Which of the following is used to remove files and clear the internet browsing history?

- ~~User Account Control~~
- Steganography
- cPassword
- CCleaner

Explanation

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.

User Account Control's goal is to prevent unauthorized changes from happening on your system. It does this by running all processes on the system as a limited user by default. UAC was introduced back in Windows Vista, and it's been used in all versions of Windows ever since then.

cPasswords is the name of the attribute that stores passwords in a Group Policy preference item in Windows.

Steganography is the method of embedding data into legitimate files like graphics, banner ads, or plain text messages to hide it and then extracting the data once it reaches its destination, hiding messages or files in plain sight.

References

TestOut Ethical Hacker Pro - 8.2 Privilege Escalation
[e_priv_escalation_eh1.exam.xml Q_PRIV_ESCALATION_COUNTERMEASURE_02_EH1]

Question 3: Incorrect

Which of the following is a protocol that allows authentication over a non-secure network by using tickets or service principal names (SPNs)?

- DLL hijacking
- Kerberoasting
- Unattended installation
- ~~Credentials in LSASS~~

Explanation

Kerberoasting is a protocol that allows authentication over a non-secure network by using tickets or service principal names (SPNs).

DLL hijacking is when malicious DLL (dynamic link library) is inserted in a directory, and a service or application follows that malicious path instead of the correct path.

In Microsoft Windows, the local security authority subsystem service (LSASS) is a file in the directory that performs the security protocol of the system. It's an essential part of the security process as it verifies user logins, creates access tokens, and handles the password changes.

Installing a program throughout a network without having to sit at every computer and having to stay involved with the process during the installation is often necessary, but it does have risks. If the administrator fails to go back and clean up after the installation, a file called Unattended is left on the individual workstations. The Unattended file is an XML file and has configuration settings used during the installation that can contain the configuration of individual accounts to include admin accounts, making for easy privilege escalation on each computer.

References

TestOut Ethical Hacker Pro - 8.2 Privilege Escalation
[e_priv_escalation_eh1.exam.xml Q_PRIV_ESCALATION_TECHNIQUES_01_EH1]

Question 4: Correct

Which of the following best describes the Security Account Manager (SAM)?

- The attribute that stores passwords in a Group Policy preference item in Windows.
- A file in the directory that performs the system's security protocol.
- A database that stores user passwords in Windows as an LM hash or a NTLM hash.
- A protocol that allows authentication over an unsecure network through tickets or service principal names.

Explanation

Security Account Manager (SAM) is a database that stores user passwords in Windows as an LM hash or a NTLM hash. This database is used to authenticate local users and remote users. It doesn't store the domain system user credentials like the LSASS database does; rather, it stores the system's administrator recovery account information and passwords. While the SAM file can't be copied to another location, it is possible to dump the hashed passwords to on off-site location, which can then be decrypted through a brute force method.

LSASS or the local security authority subsystem service is a file in the directory that performs the system's security protocol. It's an essential part of the security process as it verifies user logins, creates access tokens, and handles the password changes.

cPasswords is the name of the attribute that stores passwords in a Group Policy preference item in Windows.

Kerberos is a protocol that allows authentication over an unsecure network by using tickets or service principal names (SPNs).

References

TestOut Ethical Hacker Pro - 8.2 Privilege Escalation
[e_priv_escalation_eh1.exam.xml Q_PRIV_ESCALATION_TECHNIQUES_02_EH1]

Question 5: Correct

An attacker installed a malicious file in the application directory. When the victim starts installing the application, Windows searches in the application directory and selects the malicious file instead of the correct file. The malicious file gives the attacker remote access to the system. Which of the following escalation methods best describes this scenario?

- Clear text credentials in LDAP
- DLL hijacking
- Kerberoasting
- Unattended installation

Explanation

DLL hijacking can happen during an application installation. Windows applications usually search the application directory from which they were loaded before they attempt a fully qualified path when loading an external DLL library. If an attacker has installed a malicious DLL in the application directory before the application installation has begun, then the application will search the Windows system directory and choose the malicious DLL. Then the attacker has remote access to the system.

If the administrator fails to go back and clean up after the unattended installation, a file called Unattended is left on the individual workstations. The Unattended file is an XML file and has configuration settings used during the installation that can contain the configuration of individual accounts to include admin account, making privilege escalation on each computer an easy task.

Kerberos is a protocol that allows authentication over an unsecure network using tickets or service principal names. Any authorized user can log into an Active Directory domain and request a service ticket. An encrypted ticket will be returned, and brute force can be used offline to crack this ticket and reveal the service account password in plain text.

With clear text credentials in LDAP the data is transferred unencrypted or in clear text is vulnerable to hackers. Beware however, most domain controllers allow clear text credentials to be transmitted over the network, even to and from the local directory. You can check for clear text transfers by using the insecure LDAP bind script in PowerShell. PowerShell will deliver a CSV file as output, showing you which accounts are vulnerable.

References

TestOut Ethical Hacker Pro - 8.2 Privilege Escalation
[e_priv_escalation_eh1.exam.xml Q_PRIV_ESCALATION_TECHNIQUES_03_EH1]

Question 6: Incorrect

Which of the following is the name of the attribute that stores passwords in a Group Policy preference item in Windows?

- SPNs
- cPasswords
- ~~SAM~~

- LSASS

Explanation

cPasswords is the name of the attribute that stores passwords in a Group Policy preference item in Windows. This attribute is easy to exploit because Microsoft publishes the public key for the encryption of the account credentials in the group policy preferences. These preferences allow domain admins access to create and deploy in any local user or local admin accounts. The cpasswords are stored in the SYSVOL folder on the domain controllers in an encrypted XML file. Any user can view the public key and decrypt the passwords to escalate their security privileges.

Security Account Manager (SAM) is a database that stores user passwords in Windows as an LM hash or a NTLM hash. This database is used to authenticate local users and remote users. It doesn't store the domain system user credentials like the LSASS database does; rather, it stores the system's administrator recovery account information and passwords.

Service Principal Names are tickets or a unique identifier of a service instance.

Local Security Authority Subsystem Service (LSASS) is a file in the directory that performs the system's security protocol. It's an essential part of the security process, as it verifies user logins, creates access tokens, and handles password changes.

References

TestOut Ethical Hacker Pro - 8.2 Privilege Escalation
[e_priv_escalation_eh1.exam.xml Q_PRIV_ESCALATION_TECHNIQUES_04_EH1]

Question 7: Correct

Which of the following privilege escalation risks happens when a program is being installed without the constant supervision of the IT employee and fails to clean up after?

- Unattended installation
- DLL hijacking
- Gaining credentials in LSASS
- Kerberoasting

Explanation

While being able to install a program throughout a network without having to sit at every computer and having to stay involved with the process during the installation is often necessary, the process comes with risks. If the administrator fails to go back and clean up after the installation, a file called Unattended is left on the individual workstations. The Unattended file is an XML file and has configuration settings used during the installation that can contain the configuration of individual accounts to include admin accounts, making privilege escalation easy on each computer.

Kerberos is a protocol that allows authentication over an unsecure network using tickets or service principal names (SPNs). Any authorized user can log into an Active Directory domain and request a service ticket (TGS). An encrypted ticket will be returned, and brute force can be used offline to crack this ticket to reveal the service account password in plain text. This process is called Kerberoasting.

DLL hijacking can happen during an application installation. Windows applications usually search the application directory from which they were loaded before they attempt a fully qualified path when loading an external DLL library. If an attacker has installed a malicious DLL in the application directory before the application installation has begun, then the application will search the Windows system directory and choose the malicious DLL. Then the attacker has remote access to the system.

In Microsoft Windows, the local security authority subsystem service (LSASS) is a file in the directory that performs the system's security protocol. It's an essential part of the security process as it verifies user logins, creates access tokens, and handles password changes.

References

TestOut Ethical Hacker Pro - 8.2 Privilege Escalation
[e_priv_escalation_eh1.exam.xml Q_PRIV_ESCALATION_TECHNIQUES_05_EH1]

Question 8: Correct

A hacker has gained physical access to a system and has changed an administrator's account password. Which of the following tools did the hacker most likely use to accomplish this?

- CCleaner
- Timestomp
- StegoStick
- Ultimate Boot CD

Explanation

Ultimate Boot CD is a tool that you can put on a disc or a flash drive that has many tools to facilitate recovering a machine. The intended use is to help people who have lost data, forgotten their password, or corrupted their operating system. For us, it's a treasure trove of hacking tools. One of its capabilities is to change an administrator's account passwords.

Timestomp is a tool for modifying or deleting a time stamp on a file in order to hide when it was created, accessed, or modified. Attackers change times and dates to blend in with existing time stamps so as to not alert digital forensic investigators of access or exploitation.

A document steganography tool allows a file to be hidden within any image, audio, or video file, or even in PDFs and EXE files.

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.

References

TestOut Ethical Hacker Pro - 8.2 Privilege Escalation
[e_priv_escalation_eh1.exam.xml Q_PRIV_ESCALATION_TECHNIQUES_06_EH1]

Question 9: Incorrect

Which of the following is a tool for cracking Windows login passwords using rainbow tables?

- GreyFish
- ~~Trinity Rescue Kit~~
- Ophcrack
- ERD Commander

Explanation

Ophcrack is a tool for cracking Windows login passwords. It uses rainbow tables and has the capability to receive hashes in many formats. It is an open-source program and free to download.

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.

Trinity Rescue Kit helps with repair and recovery operations on Windows machines. It can reset passwords, scan for viruses, run a disk cleanup, and fix bugs.

GrayFish is a rootkit tool that runs within the Windows operating system. It contains hidden storage and has invisible malicious command execution.

References

TestOut Ethical Hacker Pro - 8.2 Privilege Escalation
[e_priv_escalation_eh1.exam.xml Q_PRIV_ESCALATION_TOOLS_01_EH1]