8.2.5 Privilege Escalation in Windows Facts

Every computer network has levels of privileges that give each user appropriate access for the user's function in the organization and the security of the network. Privilege escalation occurs when an attacker accesses the network as a non-administrator level user and gains access to administrative-level privileges. An attacker seeks privilege escalation in order to access sensitive information, to delete files, or to install programs like worms, viruses, or Trojan horses.

This lesson covers the following topics:

- Privilege escalation techniques
- Tools
- Countermeasures

Privilege Escalation Techniques

Hackers can escalate privileges in the following ways:

Method	
cPassword	cPassword 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 Group Policy preferences account credentials. These preferences allow domain admins access to create and change any local user or local admin account. Cpasswords are stored in an encrypted XML file in the SYSVOL folder on the domain controllers. This allows any domain authenticated user access to decrypt the password.
Clear text credentials in LDAP	Data 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 unsecure LDAP bind script in PowerShell. PowerShell will deliver a CSV file as output, showing you which accounts are vulnerable.
Kerberoasting	Kerberos is a protocol that allows authentication over a non-secure network by using tickets or service principal names (SPNs). A user authenticates to the server, which forwards the user name to the key distribution center (KDC). The KDC issues a ticket-granting ticket (TGT) that is encrypted using the ticket granting service (TGS). An encrypted ticket will be returned. A brute force can be used offline to crack this ticket to reveal the service account password in plain text. This process is called Kerberoasting. There is no risk of detection and no need for escalated privileges, and the process is easy to perform.
Credentials in LSASS	In Microsoft Windows, the local security authority sub-system 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. This file is susceptible to corruption by viruses or Trojan horses. LSASS is a critical component of domain authentication, Active Directory management on the domain system, and the initial security authentication procedure. If it's compromised, an attacker can easily escalate privileges in the network.
SAM database	Security Account Manager (SAM) is a database that stores user passwords in Windows as an LM hash or an 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 an offsite location where the passwords can be decrypted with a brute force method.
Unattended installation	While it is convenient and sometimes necessary, to install a program throughout a network without having to sit at every computer, there are risks. If the administrator fails to 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 including admin accounts. This makes privilege escalation easy. To avoid additional risks: ▪ Give only the privileges needed for the installation when creating the answer file for an unattended installation. ▪ Ensure credentials are encrypted when a network admin is installing over a network. ▪ Secure the image created for the installation.
DLL hijacking	DLL hijacking can happen during an application installation. When loading an external DLL library, Windows usually searches the application directory from which the application was loaded before attempting a fully qualified path. If an attacker has installed a malicious DLL in the application directory before the application installation has begun, then the application will choose the malicious DLL.

Tools

The following table identifies tools hackers can use to elevate privilages.

Tool	Description
Trinity Rescue Kit	Trinity Rescue Kit (TRK) helps with repair and recovery operations on Windows machines. It is a great tool for maintenance. It has many functions, including resetting passwords, scanning for viruses, running a disk cleanup, and fixing bugs.
ERD Commander	ERD Commander software is 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.
OPH Crack	A tool for cracking Windows login passwords. It uses rainbow tables and has the capability to crack hashes from many formats. It is an open-source program and free to download.

Countermeasures

The most effective way to protect against privilege escalation is to tighten privileges to make sure that users have only the privileges that they need. This prevents escalation if an attacker gains access to an account that has higher privileges than it needs. Once privileges are tightened, focus on these steps:

- Encrypt sensitive information.
- Implement multi-factor authentication and authorization.
- Restrict interactive logon privileges.
- Scan the operating system and application coding regularly for bugs and errors.
- Frequently perform updates on the operating system and applications.
- Install auditing tools to continuously monitor file system permissions.
- Use fully qualified paths in Windows applications.
- Select Always Notify in the UAC settings.
