Privilege Escalation

This lesson is going to cover the fourth stage in the MITRE ATT&CK framework, Privilege Escalation. These techniques are used to describe ways that adversaries will attempt to gain higher privileges, such as moving from a standard user to an administrator, or from an admin to a domain admin. At the time of writing currently includes 12 top-level techniques. **We will be looking at the following:**

- Valid Accounts (4 sub-techniques)
- Exploitation For Privilege Escalation

MITRE Technique T1078

It is completely plausible that an adversary can immediately gain access to privileged accounts such as administrators or domain administrators provide they can obtain the credentials in one form or another. This can be achieved by using phishing emails, specifically credential harvesters where the recipients are enticed to enter in their credentials to a website that appears to be a legitimate service, such as Outlook Web Access. These credentials would then be sent to the attacker who could attempt to log in to these accounts via remote service such as Remote Desktop protocol (RDP). It is crucial that credentials are not leaked, shared, or breached to protect the accounts from being accessed by unauthorised individuals.

Taking a look at the Procedure Example table we can see that all of these entries in the screenshot are examples of advanced threats that have utilised legitimate credentials to log in to systems. The entry from APT28 is a great example where they have launched a spear phishing campaign to obtain valid credentials and also used manufacturer default credentials to log into IoT devices, giving them a foothold in the network. There are lots of great examples, so we suggest you take a look at a few more.

Procedure Examples

Name	Description
APT18	APT18 actors leverage legitimate credentials to log into external remote services.[39]
APT28	APT28 has used legitimate credentials to gain initial access, maintain access, and exfiltrate data from a victim network. The group has specifically used credentials stolen through a spearphishing email to login to the DCCC network. The group has also leveraged default manufacturer's passwords to gain initial access to corporate networks via IoT devices such as a VOIP phone, printer, and video decoder.[37][38][39]
APT33	APT33 has used valid accounts for initial access and privilege escalation.[40][15]
APT39	APT39 has used stolen credentials to compromise Outlook Web Access (OWA).[22]
APT41	APT41 used compromised credentials to log on to other systems.[26]

In the Mitigations section there are three suggestions to prevent this technique from being as effective. Firstly, hardcoded credentials should not be used in applications or website, this is where developers will create an account and put the username and password in the code so they don't need to manually login whenever the code is run. Sometime this code can be uploaded to platforms such as Pastebin or Github where attackers can scrape it and identify credentials which they can later use to log into systems or applications. Next MITRE suggests applications using default credentials (from routers to IoT devices such as printers) should be immediately changed away from the default username and password to prevent attackers from using lists of known username and password pairs. Finally it is suggested that routine audits are conducted to identify accounts that have excessive permissions and privileges which could be a gold mine for attackers, and also identify accounts that have had their permissions changed, which could be a sign of privilege escalation through exploitation (we'll cover this below).

Mitigations

Mitigation	Description
Application Developer Guidance	Ensure that applications do not store sensitive data or credentials insecurely. (e.g. plaintext credentials in code, published credentials in repositories, or credentials in public cloud storage).
Password Policies	Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment. [18] When possible, applications that use SSH keys should be updated periodically and properly secured.
Privileged Account Management	Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. [17][19] These audits should also include if default accounts have been enabled, or if new local accounts are created that have not be authorized. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. [6]

MITRE Technique T1068

Certain software or operating system functions will typically run at a higher privilege than a normal user, and by exploiting these vulnerabilities the adversary may be able to escalate the current user's privileges, or run malicious code in the context of another program or process and gain a reverse shell at a higher level. Depending on the component that is vulnerable it could be possible for a standard user account to execute code in the context of SYSTEM on a Windows host, the highest level with unparalleled access and permissions. The same can be done to achieve ROOT permissions on a Linux-based system.

In the Procedure Examples table we can see a number of CVEs (Common Vulnerabilities and Exposures) which represent unique vulnerabilities. Let's take a deeper dive below and explore a couple of the CVEs that have been used by advanced threats in the past.

Procedure Examples

Name	Description
APT28	APT28 has exploited CVE-2014-4076, CVE-2015-2387, CVE-2015-1701, CVE-2017-0263 to escalate privileges.[31][32][33]
APT32	APT32 has used CVE-2016-7255 to escalate privileges.[34]
APT33	APT33 has used a publicly available exploit for CVE-2017-0213 to escalate privileges on a local system.[12]
Cobalt Group	Cobalt Group has used exploits to increase their levels of rights and privileges.[16]

APT28 has used CVE-2017-0263

You can find the page for this CVE here. You can find the Microsoft advisory page here.

This is an old vulnerability that occurs in the Windows operating system and is associated with the Windows kernel-mode driver failing to properly handle objects in memory. This allows an attacker to run malicious code in kernel mode (the absolute highest level), allowing them to install programs; view, change, or delete data; or create new accounts with full user rights (administrators).

To actually exploit this vulnerability the attacker would already need to have access to an account within the target environment. They could then run a specially crafted application (a 'payload') that could exploit the vulnerability and take control of an affected system.

APT32 has used CVE-2016-7255

You can find the page for this CVE here. You can find a third-party advisory page (with exploit code!) here.

This CVE is similar to the above one, as it is another vulnerability in kernel-mode drivers that could allow an attacker to execute code in the context of the Windows kernel. In the 3rd-party advisory linked above there is a tab for "Exploit" which provides an exploit file that can be used to execute the vulnerability and run commands in the context of kernel. Scripts like this are added to attack frameworks such as Metasploit so they can be used in penetration tests (but also abused by malicious actors!).

In the Mitigations section the suggestions here are based on preventing the attacker from exploiting vulnerabilities by patching them to remove the risk, developing a threat intelligence capability that will track which CVEs are actively being exploited by threat actors to provide situational awareness for the security team and prove to the business that security patching is crucial to prevent successful attacks, and also ensure that the built-in group of security tools called Exploit Guard is enabled on all Windows hosts to detect and prevent local exploitation activity.

Mitigations

Mitigation	Description
Application Isolation and Sandboxing	Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. Risks of additional exploits and weaknesses in these systems may still exist. [1]
Exploit Protection	Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. [1] Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. [2] Many of these protections depend on the architecture and target application binary for compatibility and may not work for software components targeted for privilege escalation.
Threat Intelligence Program	Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization.
Update Software	Update software regularly by employing patch management for internal enterprise endpoints and servers.

For Detection we are told to enforce deep logging using tools such as Sysmon from Sysinternals to allow us to detect process modification and creation. Endpoint detection and response (EDR) solutions can also notice and correlate changes to the operating system files that may represent exploitation activity.

Detection

Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Also look for behavior on the endpoint system that might indicate successful compromise, such as abnormal behavior of the processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution or evidence of Discovery.

Higher privileges are often necessary to perform additional actions such as some methods of OS Credential Dumping. Look for additional activity that may indicate an adversary has gained higher privileges.