‹ Dashboard

Why this topic?

Windows and Linux constitute the majority of production servers in deployment today. Over the last two decades, the security features on these operating systems have evolved and improved, making it more difficult for hackers to do damage. Concepts such as Linux capabilities mean that most services and applications no longer require root privileges to run. Thus, when such a service is compromised, the attacker only gets a low-privileged shell on the machine. To get access to other applications and data, the attacker then must be able to perform privilege escalation.

This section covers advanced Windows privilege escalation techniques such as DLL Hijacking and UAC Bypass.

DLL Hijacking

A DLL or a Dynamic Link Library is a library that contains code and data that can be used by more than one program at the same time. Much of the operating system and application functionality resides in the DLLs. In this section, we will take a look at how to identify missing DLL paths used by applications, and perform DLL Hijacking to escalate privileges.

UAC Bypass

User Account Control or UAC is a security feature of Microsoft Windows. It enforces mandatory access control to prevent unauthorized changes to the operating system. For a user application to make any changes, administrator authorization is required. UAC prevents malware and other malicious programs from compromising the operating system. In this section, we will take a look at various UAC bypass techniques and use them to attain administrative privileges.

What will you learn?

- Understanding Dynamic Link Library (DLL) and User Account Control (UAC)
- Performing DLL Hijacking and escalating privileges to the Administrator user
- Leveraging Windows components to bypass UAC and escalate privileges to the Administrator user

References:

1. Dynamic Link Library (https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/dynamic-link-library)
2. User Account Control (https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-overview)
3. Network Pentesting (https://www.pentesteracademy.com/course?id=6)

Labs:

DLL Hijacking:

- DLL Hijacking: DVTA
    - Objective: Identify Hijackable DLL location referenced by DVTA application, perform DLL Hijacking and Gain access to administrator privilege meterpreter session.

- Objective: Leverage the FodHelper binary, bypass the UAC, and Gain access to administrator privilege meterpreter session.
- UAC Bypass: SilentCleanup
    - Objective: Leverage the SilentCleanup predefined scheduled task, bypass the UAC, and Gain access to administrator privilege meterpreter session.
- UAC Bypass: IFileOperation AutoRun
    - Objective: Leverage various IFileOperation Interface methods to bypass the UAC, and Gain access to administrator privilege meterpreter session.
- UAC Bypass: IFileOperation FileZilla
    - Objective: Leverage various IFileOperation Interface methods to bypass the UAC, and Gain access to administrator privilege meterpreter session.
- UAC Bypass: CMSTP
    - Objective: Leverage the CMSTP binary, bypass the UAC, and Gain access to administrator privilege meterpreter session.