[PowerSploit]

1. PowerSploit(파워스플로잇)
: PowerShell 모듈과 스크립트로 구성된 오픈 소스의 공격적인 보안 프레임워크로 코드 실행, 지속성, 바이러스 제거, 재봉 및 유출과 같은 침투 테스트와 관련된 광범위한 작업을 수행
: 침투 테스트를 수행하는 자에게 도움이 될 수 있는 PowerShell Module들을 모아 놓은 것

- ➔ PowerShell script로 만든 각종 Exploit Tool들의 집합
- ➔ * PowerShell? MS사에서 시스템 관리 작업을 자동으로 처리하기 위하여 개발한 Shell. 윈도우 OS에 기본 탑재. 윈도우 OS 및 윈도우 응용 프로그램의 관리를 쉽게 제어하고 자동화 가능. OS가 제공하는 모든 주요한 기능들을 쉽게 access 가능
- ➔ PowerShell을 활용한 툴킷, 합법적인 침투 테스트 용도로 사용됨 – powersploit, powershell empire

2. 파워스플로잇 사용
1) 깃허브에서 파워스플로잇 다운
(깃허브 : https://github.com/PowerShellMafia/PowerSploit)
2) 실행 후 Import-Module 명령어 실행

PS C:>Import-Module .₩PowerSploit.psd1

3) 백신이 설치되어 있는 상태에서 설치를 하면, 백신이 각 모듈을 바이러스 프로그램으로 인식하기 때문에 설치 작업이 완료되지 않음. PowerShell script가 외부로부터 다운로드 되어 실행되지 못하도록 설정이 된 경우는, “Script Execution Policy”를 off 한 상태에서 설치해야 함

“Script Execution Policy”를 off 하기 위해서는 관리자 권한으로 PowerShell을 실행한 후, 아래와 같은 명령어를 실행(Prompt가 나오면 Y 키를 누른 후 Enter-Key)

PS C:> Set-ExecutionPolicy -ExecutionPolicy Bypass

3. 제공하는 기능
1) Code Execution(코드 실행): Target Machine 에서 Code 를 실행(execution)하는 기능

- ◆ Invoke-DllInjection: 선택한 프로세스 ID에 Dll을 삽입합니다.
- ◆ Invoke-ReflectivePEInjection: Windows PE 파일(DLL/EXE)을 파워쉘 프로세스에 반사적으로 로드하거나 원격 프로세스에 DLL을 반사적으로 삽입합니다.
- ◆ Invoke-Shellcode: 로컬에서 선택한 프로세스 ID 또는 PowerShell 내에 셸코드를 삽입합니다.
- ◆ Invoke-WmiCommand: 대상 컴퓨터에서 PowerShell ScriptBlock을 실행하고 WMI를 C2 채널로 사용하여 포맷된 출력을 반환합니다. WMI를 사용하여 파워셸 페이로드에서 출력을 실행하고 검색합니다.

2) Script modification(스크립트 수정): 침투한 시스템에서 script가 실행되는 방식을 수정하는 기능. 예를 들면, payload에 대한 인코딩, 압축, 암호화

- ◆ Out-EncodedCommand: 압축, Base-64 인코딩 및 PowerShell 페이로드 스크립트에 대한 명령줄 출력을 생성합니다.
- ◆ Out-CompressdDll: 압축, Base-64 인코딩 및 생성된 코드를 출력하여 관리되는 dll을 메모리에 로드합니다.
- ◆ Out-EncryptScript: 텍스트 파일/스크립트를 암호화합니다.
- ◆ Remove-Comment: 스크립트에서 주석과 추가 공백을 제거합니다.

3) Persistence(지속): 대상 script에 지속성 기능을 추가

- New-UserPersistenceOption: 추가 지속성 기능에 대한 사용자 수준 지속성 옵션을 설정합니다.
- New-ElevatedPersistenceOption: 추가 지속성 기능에 대한 높은 지속성 옵션을 설정합니다.
- Add-Persistence: 스크립트에 지속성 기능을 추가합니다.
- Install-SSP: SSP(보안 지원 공급자) dll을 설치합니다.
- Get-SecurityPackages: 로드된 모든 보안 패키지(SSP)를 열거합니다.

4) Antivirus bypass(안티바이러스 우회): 안티바이러스 S/W를 찾아내는 기능

- Find-AVSignature: 단일 바이트 안티 바이러스 서명을 찾는 데 사용합니다.

5) Exfiltration(탈출?): 시스템에서 데이터를 찾아서 추출하는 기능. 예를 들면, Mimikatz를 실행하는 module 또는 keystrokes를 훔치는 module.

- Invoke-TokenManipulation: 엑세스 토큰 조작
- Invoke-CredentialInjection: 의심스러운 이벤트 ID 4648(명시적 자격 증명 로그온)을 트리거하지 않고 텍스트 자격 증명이 있는 로그온을 만듭니다.
- Invoke-NinjaCopy: 원시 볼륨을 읽고 NTFS 구조를 구문 분석하여 NTFS 분할 된 볼륨에서 파일을 복사합니다.
- Invoke-Mimikatz: PowerShell을 사용하여 메모리에 Mimikatz 2.0을 반사적으로 로드합니다. 디스크에 아무 것도 쓰지 않고 자격 증명을 덤프하는 데 사용할 수 있습니다. 미미카츠와 함께 제공되는 모든 기능에 사용할 수 있습니다.
- Get-Keystrokes: 키를 누르고 시간 및 활성 창을 기록합니다.
- Get-GPPPassword: 그룹 정책 기본 설정을 통해 푸시된 계정에 대한 일반 텍스트 암호 및 기타 정보를 검색합니다.
- Get-GPPAutologon: 그룹 정책 기본 설정을 통해 푸시한 경우 registry.xml에서 자동 사용 법 사용자 이름과 암호를 검색합니다.
- Get-TimedScreenshot: 정규 간격으로 스크린샷을 가져와 폴더에 저장하는 함수입니다.
- New-VolumeShadowCopy: 새 볼륨 그림자 복사본을 만듭니다.
- Get-VolumeShadowCopy: 모든 로컬 볼륨 그림자 복사본의 장치 경로를 나열합니다.
- Mount-VolumeShadowCopy: 볼륨 그림자 복사본을 마운트합니다.
- Remove-VolumeShadowCopy: 볼륨 그림자 복사본을 삭제합니다.
- Get-VaultCredential: 지우개 웹 자격 증명을 비롯한 Windows 자격 증명 개체를 표시합니다.
- Out-Minidump: 프로세스의 전체 메모리 미니 덤프를 생성합니다.
- Get-MicrophoneAudio: 시스템 마이크에서 오디오를 기록하고 디스크에 저장합니다.

6) Mayhem(대혼란): 일반적인 혼란(mayhem)을 유발시키는 기능. 예를 들면 Master boot record 덮어쓰기, blue screen 발생시키기

- Set-MasterBootRecord: 선택한 메시지와 함께 마스터 부팅 레코드를 덮어쓰는 개념 증명 코드입니다.
- Set-CriticalProcess: PowerShell을 종료할 때 컴퓨터가 파란색 화면으로 표시됩니다.

7) Privesc: Target 시스템에서 권한 상승을 할 수 있도록 도와주는 기능. 이러한 기능을 PowerUp이라고 부릅니다.

- PowerUp: 일부 무기화 벡터와 함께 공통 권한 에스컬레이션 검사의 집을 정리합니다.

8) recon(정찰): 침투한 시스템에서 추가 정찰을 수행하는 기능. 이러한 기능을 PowerView라고 부릅니다. 이러한 기능을 활용하면, 네트워크 및 Windows 도메인 정보 수집 및 exploitation을 수행할 수 있습니다.

- Invoke-Portscan: nmap에서 느슨하게 (예쁜) 기반으로 일반 소켓을 사용하여 간단한 포트 스캔을 수행합니다.
- Get-HttpStatus: 사전 파일이 제공될 때 지정된 경로에 대한 HTTP 상태 코드 및 전체 URL을 반환

합니다.

- ◆ Invoke-ReverseDnsLookup: DNS PTR 레코드에 대한 IP 주소 범위를 검사합니다.
- ◆ PowerView: 네트워크 및 Windows 도메인 열거 및 악용을 수행하는 일련의 기능입니다.

위에서 언급한 Mimikatz 기능, PowerUp 기능, PowerView 기능을 수행하기 위해 어떤 명령어를 사용하는 지 추가 설명을 드리면 아래와 같습니다.

Mimikatz : //자격증명을 추출하는 tool. Windows에서 사용하는 LSASS.exe의 cache를 읽어오는 기능을 수행. LSASS.exe(Local Security Authority Subsystem Service)는 Windows에서 제공하는 Service 중의 하나로, 사용자가 로그인 한 후, 시스템이 어떤 작업을 할 때마다 매번 인증을 받지 않아도 되도록 사용자의 credential을 caching 하는 기능을 제공

PS C:> Invoke-Mimikatz

PowerUp :

PS C:> Invoke-AllChecks

PowerView :

PS C:> Get-NetComputer (도메인에 소속된 모든 Server에 대한 list를 알 수 있음)

PS C:> Invoke-UserHunter (local 도메인에 있는 시스템에 접속한 사용자를 알 수 있음)

PS C:> Get-NetUser <username> (사용자에 대한 정보를 알 수 있음)

[출처 :
https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=aepkoreanet&logNo=221632178858
GitHub - PowerShellMafia/PowerSploit: PowerSploit - A PowerShell Post-Exploitation Framework
https://attack.mitre.org/software/S0194/
]