

Lab - Launch a Graphic Console Window Using SSH and XTERM

Overview

In this short lab, you have compromised a remote Linux/UNIX target and now wish to display the targets terminal on your local machine. There is a quick and dirty way to do this if the target and the attack machine are running Linux using SSH and XTERM.

XTERM

The XTERM program is a terminal emulator for the X Window System. It was initially developed in the mid-1980s to provide DEC VT102 and Tektronix 4014 compatible terminals for programs that cannot use the window system directly.

Lab Requirements

- One installation of VirtualBox
- One virtual install of Kali Linux
- One virtual install of Metasploitable2

Ensure your VirtualBox adapters are set to either Host-only or Nat Network for both machines.

Discover the IP address for the target by logging onto your VM of Metasploitable2 and at the prompt typing either **ifconfig** or **ip addr**.

Back at your attack machine, open a terminal, and at the prompt, type the following.

```
ssh -L4444:127.0.0.1:6000 -X msfadmin@<TARGET_IP> xterm
```

In this example, my target has an IP address of 10.0.2.11.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f6:69:30
          inet addr:10.0.2.11  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef6:6930/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2764  errors:0  dropped:0  overruns:0  frame:0
          TX packets:1495  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3422597 (3.2 MB)  TX bytes:135335 (132.1 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```

At my Kali terminal, I type in the following command:

```
ssh -L4444:127.0.0.1:6000 -X msfadmin@10.0.2.11 xterm
```

```
File Actions Edit View Help
└─(root👤kali)-[~]
# ssh -L4444:127.0.0.1:6000 -X msfadmin@10.0.2.11 xterm
```

I am asked for the SSH password for the msfadmin password. The password for msfadmin is msfadmin. On Linux, you cannot see the password being typed at the prompt.

```
(root@kali) - [~]  
# ssh -L4444:127.0.0.1:6000 -X msfadmin@10.0.2.11 xterm  
msfadmin@10.0.2.11's password: msfadmin
```

Press enter.

I am immediately presented with the terminal of my remote target. I am limited to whatever privileges the user msfadmin is limited to. Currently, I am logged on as root.

```
(root@kali) - [~]  
# ssh -L4444:127.0.0.1:6000 -X user@10.0.2.11 xterm  
user@10.0.2.11's password:  
  
user@metasploitable: /root (on metasploitable)  
user@metasploitable:~$ ls  
user@metasploitable:~$ cd /root  
user@metasploitable:/root$ ls  
Desktop  reset_logs.sh  vnc.log  
user@metasploitable:/root$ whoami  
user  
user@metasploitable:/root$ sudo msfadmin  
[sudo] password for user:  
user is not in the sudoers file. This incident will be reported.  
user@metasploitable:/root$
```

Summary -

In this short lab, you learned how to launch a graphic console window from a remotely compromised host using ssh and xterm.