

Penetration Test

Milestone 3, 2010

Produced by

Robert Song, Yaser, Michael Zhao, Echo Xie

Penetration Instruction

There are few things we need to check before the penetration test: the client and server are connected to network, and the configuration of the network is correct. And then we need to start the OPENVPN by running: `sudo /etc/init.d/openvpn start` both in client and server machine, also to ensure the VPN connection is built up properly, we can check that by running `ifconfig` command. If the `tun0` is shown then the connection is fine. For the test, we used Zenmap to do the port scanning and the traffic security test.

Step1:

Installing the Zenmap package downloaded from <http://nmap.org/dist/nmap-5.21-setup.exe>, the installation will include installing WinPcap. The installation will finish step by step.

Step2:

Start the NMAP Zenmap GUI and input the target address, then we can choose different types of scan for testing target. To discover the hosts, NMAP uses a simple ICMP ping to locate hosts on its internal networks.

Step3:

Modify the Command of scan. This step is to set up the parameters of the scanning.

Step4:

Start the scan, and we can get the result once the scan is finish. When switching to the Ports/Hosts tab, the details of opened ports are shown including the services, protocols and other information.

Results

The outcome would show the ports and services has been exposed. The following list shows the results of several groups.

Group AUT

The AUT's image's VPN connection is working properly, and the firewalls of the windows XP client and Linux Ubuntu server have not unnecessary ports open.

Group 1

The following table shows the ports of the windows XP client are opened and the server left some ports as well.

ports

The 996 ports scanned but not shown below are in state: **closed**

Port	State	Service	Reason	Product	Version	Extra info
135	tcp	open	syn-ack			
139	tcp	open	netbios-ssn			
445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds		
2869	tcp	open	http	Microsoft HTTPAPI httpd	1.0	SSDP/UPnP

remote operating system guess

```
used port 22/tcp (open)
used port 1/tcp (closed)
used port 41105/udp (closed)
os match: Linux 2.6.17 - 2.6.31
accuracy: 100%
reference fingerprint line number: 20921
```

Group 4 (our own images)

The following table shows the ports of the Linux client and server (Ubuntu) are opened.

Port		State	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	5.3p1 Debian 3ubuntu4	protocol 2.0
10000	tcp	open		syn-ack			

Discussion

From the result, all these teams' images above have OPENVPN connection working, and the difference is the configuration of the virtual machines' firewall. For our image, we had installed OPENSSH server in the previous stage because of the IO issues of VirtualBox. OPENSSH server allows the remote windows client log onto the Linux desktop, and we forget to disable it. And it brings vulnerability for attack. Also as what we mention in our milestone 2 report, there are several ways to configure the Linux firewall, and we used iptables command to restrict the traffic. And it makes us easier to see the rules.

In the meantime, the Group1 has several unnecessary ports opening and it's possible that the firewall has not been configured or the image might not be the latest version. Also, we had used windows7 for implementing the VPN client and science the permission setting of the system, the OPENVPN was not working properly in windows7. Also windows7 doesn't expose unnecessary ports by default, so the system is more secure. So the solution of this situation is to re-configure the firewall.

OPENVPN connection is secure, once the server build up the certificates and keys for clients, the clients use the server's certificate and key to get the connection working. If the client doesn't have any corresponding key and certificate, the connection cannot be created. After the connection being built up, the client and server use the tunnel to communicate with each other. So the unnecessary ports open is an important factor affecting the security of the connection. Ports exposed will provides hackers and virus opportunities to threaten the security of the communication.