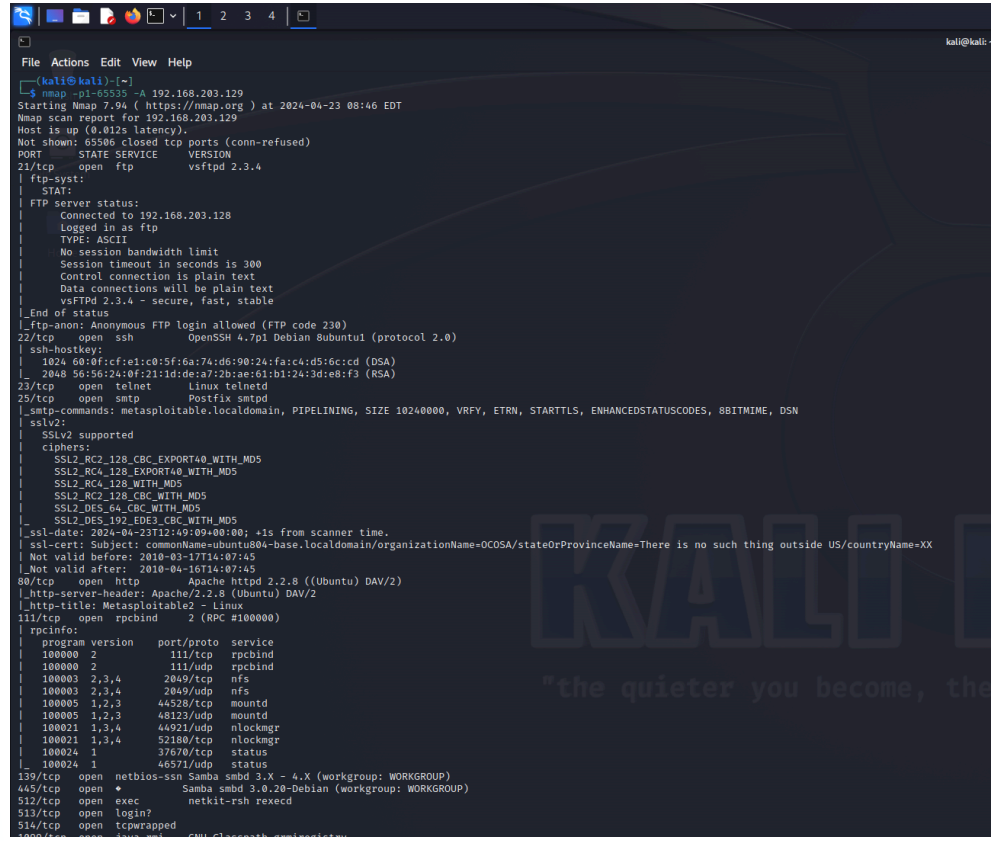
資安檢測技術與實務

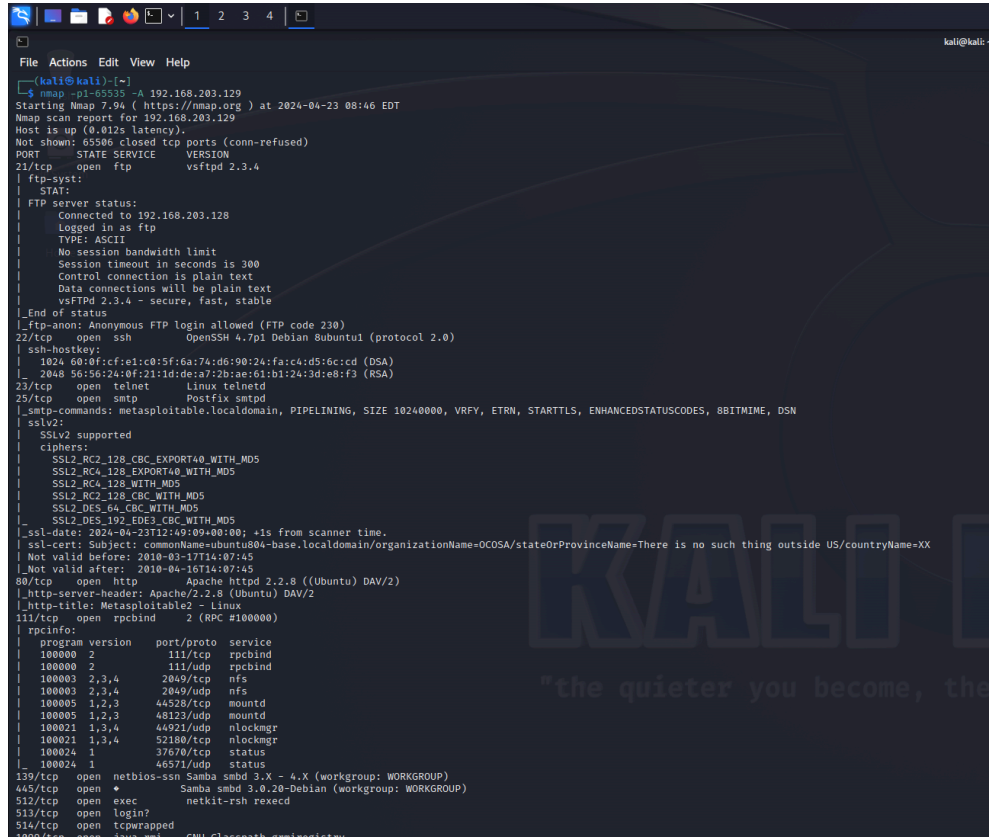
期中滲透測試報告　洪晙宸, 邵靖翔

開始測試


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: 65506 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| 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 8ubuntu1 (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-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, 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+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-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 1,3,4 44921/udp nlockmgr
| 100021 1,3,4 52180/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

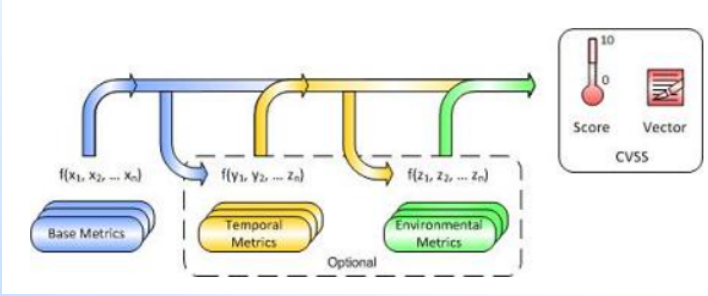
開始測試

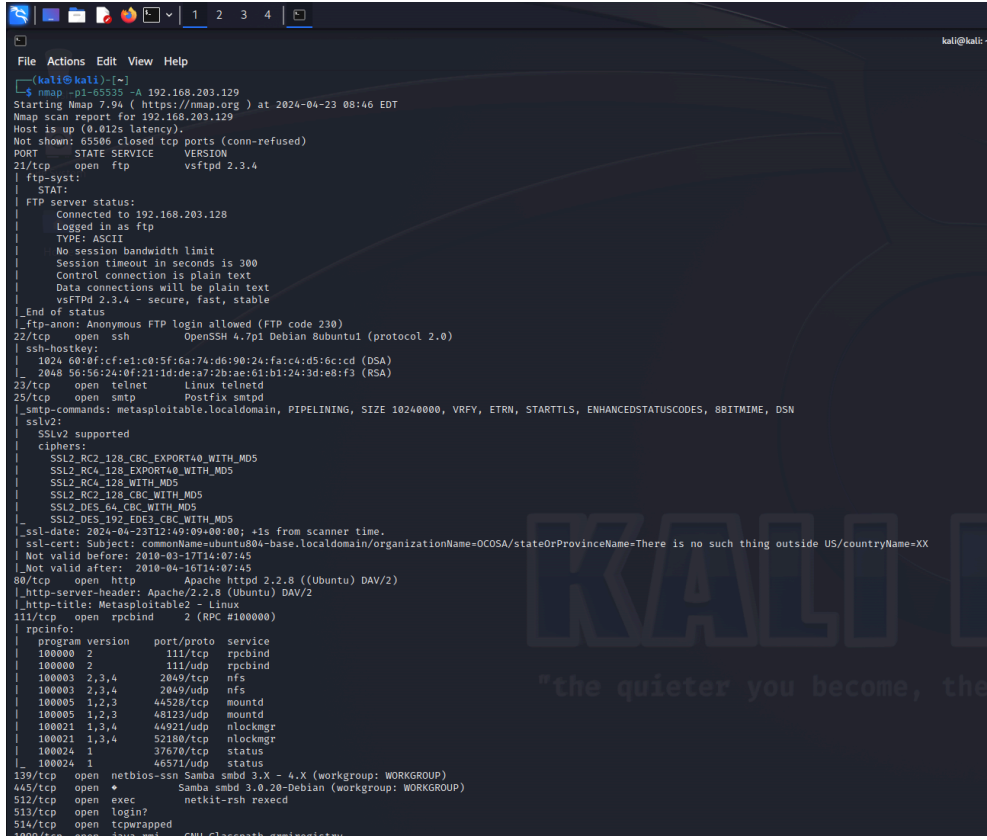
- 使用 `nmap` 對 Metasploitable 2 進行掃描
  - Telnet
  - UnrealIRCd (3.2.8.1)
  - Sambz (3.0.20-Debian)



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)
- 使用CVSS評分作為嚴重性參考





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

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

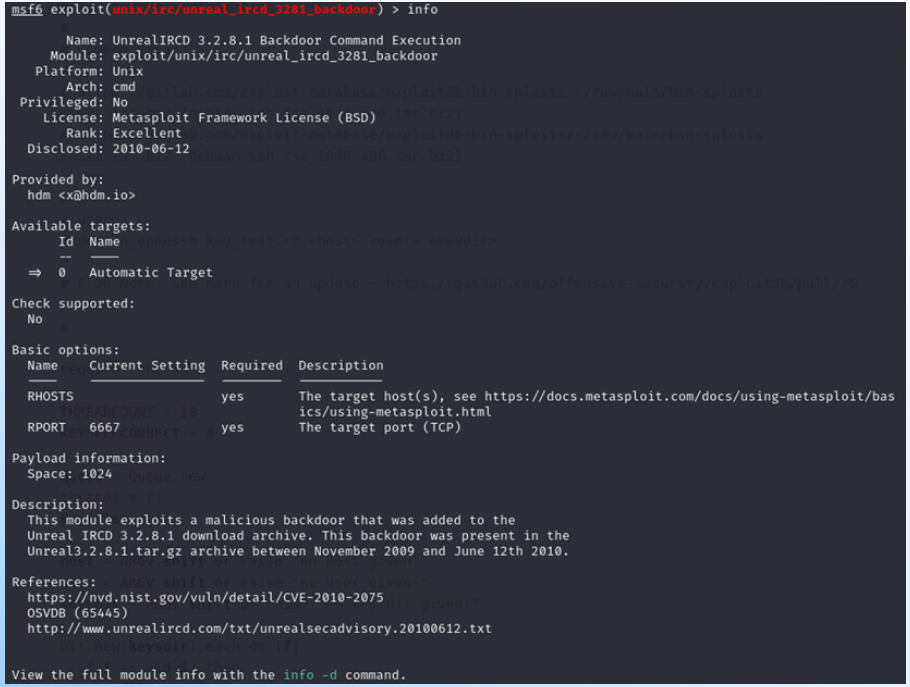
- 由於 Telnet 服務中的資訊是以明文傳輸，因此我們能夠透過 sniffer 監聽來獲得 Telnet 的帳號密碼，可能導致 root 權限帳號與密碼皆被竊取進而導致權限外洩 (CVE-2018-10698)
- 此漏洞在 CVSS 3.1 中獲得 9.8 分評估為 CRITICAL ，CVSS 2.0中獲得10.0分評估為 HIGH
- Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H。

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。

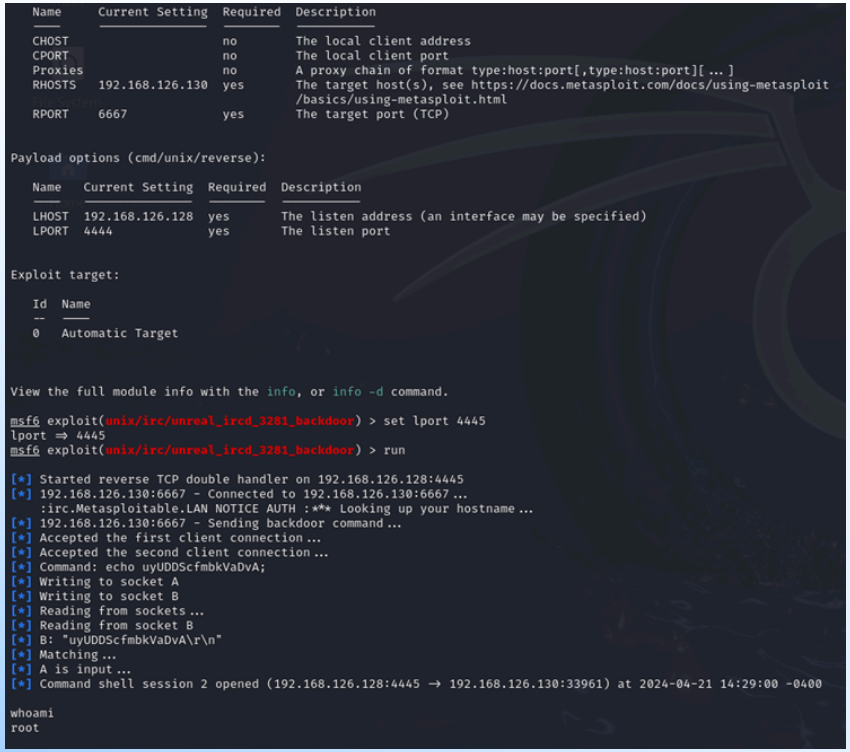
UnrealIRCd 滲透測試過程

- 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` 。



UnrealIRCd 滲透測試過程

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



UnrealIRCd 發現的漏洞和風險評估

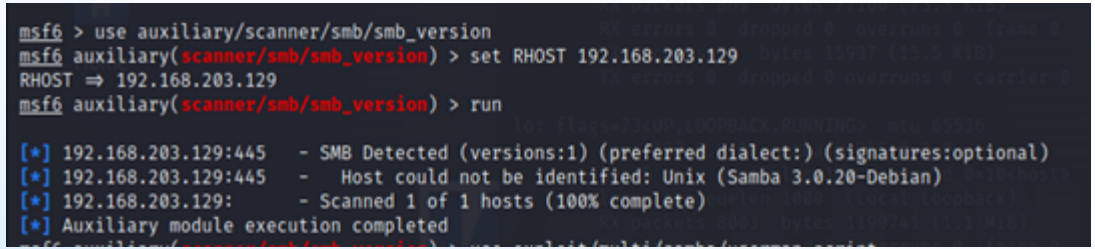
- UnrealIRCd 3.2.8.1 在 `DEBUG3_DOLOG_SYSTEM` 巨集中包含外部引入的修改（特洛伊木馬），該修改允許遠端攻擊者執行任意命令 (CVE-2010-2075)
- 此漏洞在 CVSS 3.x 中尚未評分，CVSS 2.0 中獲得 7.5 分評估為 HIGH
- Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P)。

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

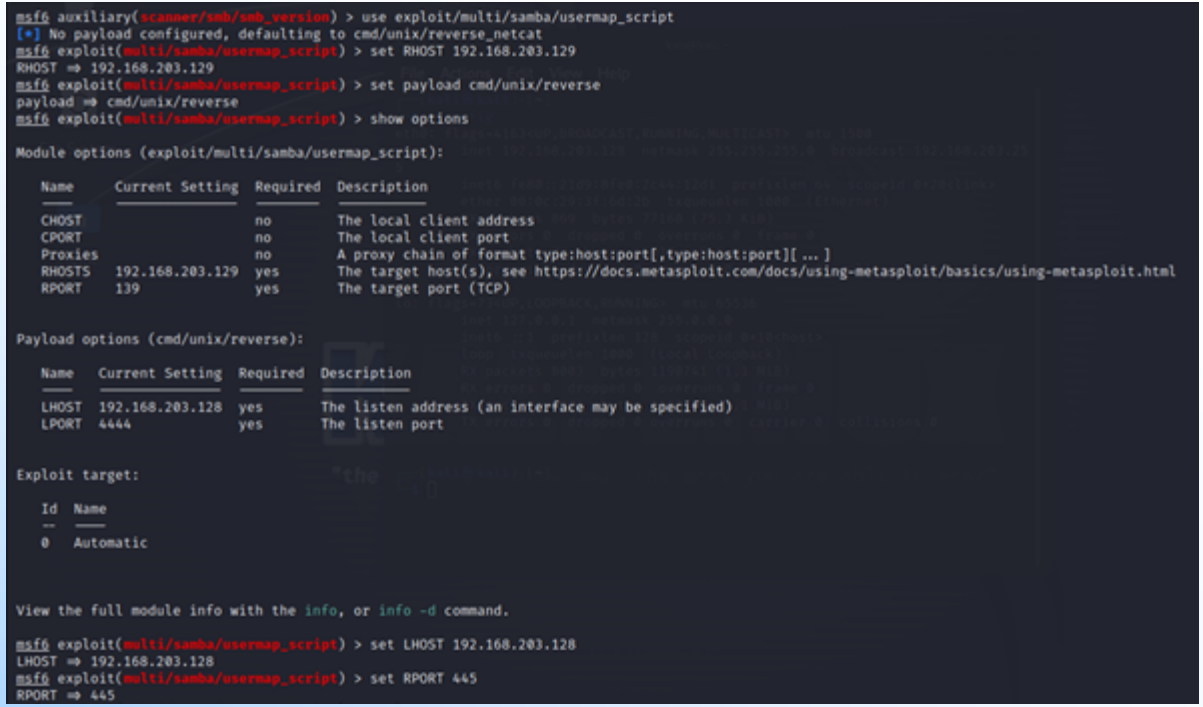
Samba 滲透測試過程

- 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。



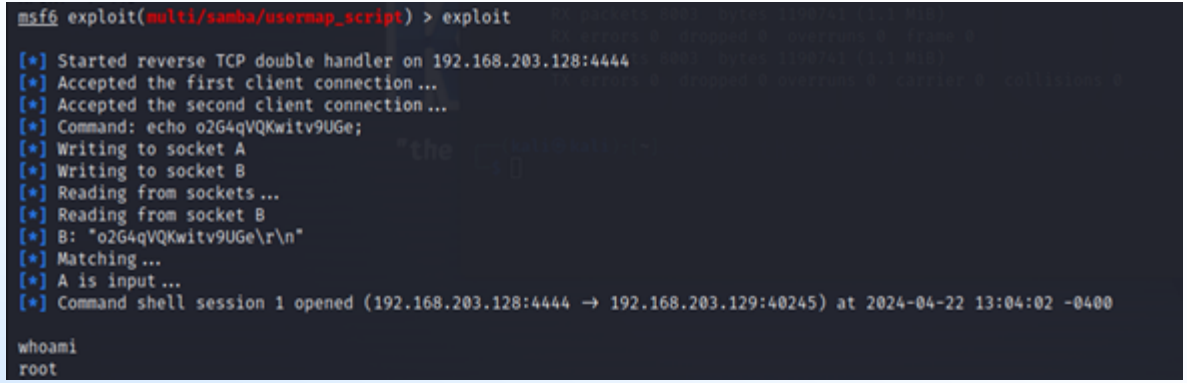
Samba 滲透測試過程

- 設定此exploit的options



Samba 滲透測試過程

- 在metasploit中run此exploit並得到root身分



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