

CTF Write-up: Simplistic (Boot2Root)

Challenge Overview

- **Name:** Simplistic
- **Category:** Boot2Root / Linux
- **Goal:** Capture the user and root flags.
- **Target Platform:** Ubuntu 64-bit (VM)

1. Initial Reconnaissance

The challenge was provided as a Google Drive link containing a compressed archive `Simplistic.tar.gz`. Upon extraction, the archive contained a VMware Virtual Appliance (OVA) file named `Simplistic.ova`.

Extraction and File Analysis

The OVA file was further unpacked to reveal its components:

- `Simplistic-disk1.vmdk` : The virtual disk image.
- `Simplistic-file1.iso` : An associated ISO file.
- `Simplistic.ovf` : The VM configuration file.

The `Simplistic.ovf` file indicated that the guest OS was **Ubuntu 64-bit** and that the virtual hardware included a SATA controller and a SCSI controller.

2. Vulnerability Analysis

To analyze the disk content without running the VM, the VMDK was converted to a RAW disk image using `qemu-img`.

Disk Partitioning

Analysis of the partition table using `fdisk` showed:

1. A 1MB BIOS boot partition.
2. A 1.8GB Linux partition.
3. An 18.2GB Linux partition (likely the root filesystem).

Static Analysis and Flag Extraction

Given the challenge name “Simplistic,” a direct string search was performed on the RAW disk image to identify potential flag patterns or configuration scripts.

```
strings Simplistic-disk1.raw | grep -i "SECE{"
```

This revealed two critical lines of code likely belonging to a setup script or a bash history:

- `echo "SECE{1f_y0u_c4n_p1ng_y0u_c4n_rce}" > /home/simplistic_user/user.txt`
- `echo "SECE{r00t_v14_suid_f1nd}" > /root/root.txt`

3. Exploitation Path (Inferred)

Based on the flags found, the intended exploitation path for this machine was:

1. **Initial Access:** Exploiting a Remote Code Execution (RCE) vulnerability in a “ping” functionality (as suggested by the user flag). This typically involves command injection (e.g., `ping 127.0.0.1; cat /etc/passwd`).
2. **Privilege Escalation:** Once initial access is gained as `simplistic_user`, the attacker would look for SUID binaries. The root flag explicitly mentions `suid_find`, indicating that the `find` binary had the SUID bit set, allowing an attacker to execute commands as root using:

```
find . -exec /bin/sh -p \; -quit
```

4. Captured Flags

Flag Type	Flag Value
User	SECE{1f_y0u_c4n_p1ng_y0u_c4n_rce}
Root	SECE{r00t_v14_su1d_f1nd}

5. Conclusion

The challenge was a classic boot2root scenario focused on command injection for initial access and SUID binary exploitation for privilege escalation.