

Vuln ubuntu

Lab Log: Building the Target Server

Target: Ubuntu Server

Goal: Create entry points for scanning, brute-forcing, and privilege escalation.

Basic Environment Setup

First, I need to get some users on the system so there is something to actually hack into.

```
# Update the system first
sudo apt update

# Create a 'noob' user with a really obvious password
sudo useradd -m -s /bin/bash noob
echo "noob:password123" | sudo chpasswd

# Set a weak root password
echo "root:root" | sudo chpasswd
```

Weakening SSH (Brute-Force Practice)

SSH is usually secure, so I have to manually break the config to allow root logins and password-based entry.

1. Open the SSH config file:

```
sudo nano /etc/ssh/sshd_config
```

2. Modify these specific lines:

- Find `PermitRootLogin` and set it to `yes`.
- Make sure `PasswordAuthentication` is set to `yes`.

3. Restart the service to apply the mess:

```
sudo systemctl restart ssh
```

Creating a Broken Samba Share (Anonymous Access)

This simulates a common corporate mistake: a file share that is wide open to anyone on the network.

1. Install Samba:

```
sudo apt install samba -y
```

2. Make a "public" folder and give it full permissions:

```
sudo mkdir -p /srv/samba/public_docs
```

```
sudo chmod 777 /srv/samba/public_docs
```

3. Add the share to the bottom of `/etc/samba/smb.conf`:

```
[Public]
path = /srv/samba/public_docs
browseable = yes
writable = yes
guest ok = yes
read only = no
force user = root
```

The "force user = root" part is the biggest flaw here, anything I upload as a guest gets root ownership.

4. Restart Samba:

```
sudo systemctl restart smbd
```

Privilege Escalation Setup (The SUID Flaw)

Once I get in as the `noob` user, I need a way to become root. I'll "misconfigure" the `find` command.

1. Find where the binary is:

```
which find
```

2. Set the SUID bit:

```
sudo chmod u+s /usr/bin/find
```