Linux Privilege Escalation | 2 hours of content | 20 hours of practice | Final project

1. Linux Refresher

- Users
- Files & Directories
- File Permissions
- Special Permissions
- View Permissions
- Real, Effective, Saved GUID

2. Spawning root shells

- Rootbash Suid
- Custom Executable
- MSFvenom
- Native Reverse Shell

3. Tools

- Linux Smart Enumeration
- LinEnum
- LinuxPrivChecker
- BeRoot
- UnixPrivEscCheck
- Enumerating Kernel Exploits
- Compiling & Exploitation Kernel
- SSH Port Forwarding

4. Service Exploits & Permissions

- Service Running As Root
- Enumerating Program Versions
- MySQL Manipulating & Exploiting
- /etc/shadow
- Hash Cracking
- /etc/passwd
- Mkpasswd
- OpenSSL
- Backups
- SSH Keys

5. Sudo

- Useful commands
- Knows Passwords
- Shell Escape
- Abusing Intended Functionality
- Environment Variables
- LD Preload
- Limitations
- LD Library Path

6. Cron Jobs

- File Permissions
- /etc/crontab/
- Bash Reverse Shells
- Path Environment Variable
- Wild Cards
- Wild Cards & File Names
- Checkpoints

7. SetUID/SetGID Exploit Techniques

- What is SUID/SGID?
- Finding SUID/SGID Files
- Shell Escape Sequences
- LD Preload & LD Library Path
- Known Exploits
- Shared Object Injection
- Strings, Strace, Ltrace
- Abusing Shell Features
- Debugging with PS4

8. Password Keys & NFS

- History Files
- Config Files
- SSH Keys
- NFS
- Useful Commands
- Root Squashing
- Mounting NFS
- Manipulating NFS