# Linux Privilege Escalation

# Enumeration

. Operating System
. Kernel version
. Environment
. Printer and other devices
. Running services by root
. Installed applications
. Configuration files
. Scheduled jobs
. Networks
. Users and groups information
. Accessible files
. History
. Private keys
. Mounted or unmounted
. Programming languages installed
. Uploading ways …

# Tools

## . Open Source

## . Proprietary

# Demonstrations:

. Kernel exploitation

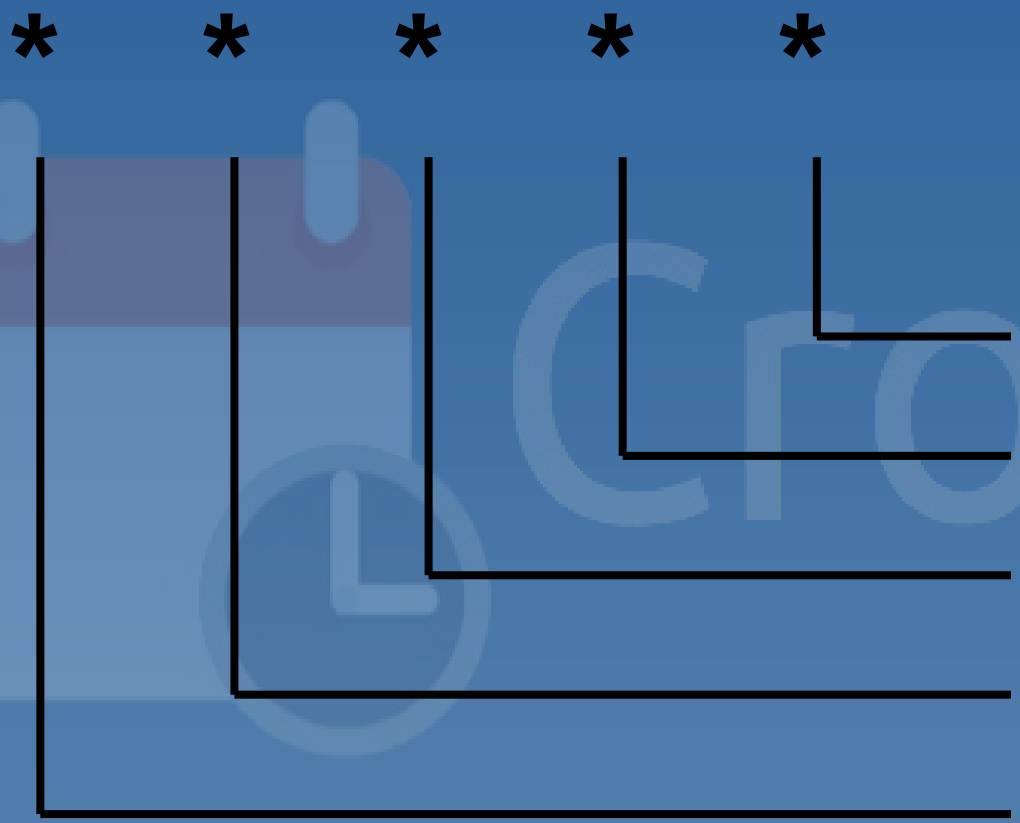
. Scheduled job exploitation

. Tracks exploitation

# Kernel

User Applications
GNOME
GTK/GNOME
KDE
Qt
Window Managers & Themes
X Window System
Netscape
Mozilla
XPCOM
Usenet
Gopher
Emacs
LYNX
Pine
mutt
elm
Freenet
Gnutella
Jabber
NetFilter & Firewalling
TCP/IP and other
Protocols, Standards & Data Formats
Loaders
Device Drivers
Kernel
COPS
Satan
SECURITY TOOLS
Tripwire
Hobgoblin
Samba
NFS
NIS
OpenLDAP
sendmail
postfix
qmail
Exim
fetchmail
Procmail
Mail List Managers
Free S/WAN
SSH/SSH2
ipchains
Secure Sockets Layer (SSL)
DNS & BIND
Apache
squid
DOM
CSS
HTML/XHTML
XML
MySQL
PostgreSQL
DBI
ZOPE
PHP
JDBC
Enhydra
Jakarta
Mason
mod_perl
WebDAV
Perl
Tcl
Python
awk
sed
bash
csh
tcsh
ELF
libstdc++
glibc
RCS
SCCS
CVS
Autoconf
Automake
make
Bugzilla
gdb
CC++
bison
flex

# THE TIME BASED JOB SCHEDULER




*path/to/script.**

| | |
|---|---|
| Day of week | 0-7 |
| Month | 1-12 |
| Day of month | 1-31 |
| Hour | 0-23 |
| Minute | 0-59 |

# Tracks

# Conclusion

. Education

. Update, update, update

. Be aware of the latest breaches

. Audit

## Want to dig more on this topic?

Hack The Box

Try Hack Me