

Forum:[Hack Forums](#)

Thread: [\[PentesterAcademy\] Linux Forensics course Downloading link](#)

spirited_wolf™ - August 10, 2016, 7:02 am

Hello HackForum members,

Today i am here to share a course on Linux Forensics

About this tutorial

This course will familiarize students with all aspects of Linux forensics. By the end of this course students will be able to perform live analysis, capture volatile data, make images of media, analyze filesystems, analyze network traffic, analyze files, perform memory analysis, and analyze malware all on a Linux system with readily available free and open source tools. Students will also gain an in-depth understanding of how Linux works under the covers.

Some topics that this course contain

Spoiler [\(Click to View\)](#)

Quote:A non-exhaustive list of topics to be covered includes:

Live response

First talk to the humans

What do they think happened

Details on victim system(s)

Mount response kit with known good tools

cdrom preferred as it was not likely part of compromise

USB MS can be used if no CDROM

Using netcat to minimize contamination

Collecting volatile data

date and time

network interfaces

funny networks

promiscuous mode?

network connections

open ports

programs associated with ports

running processes

open files

routing tables

mounted filesystems

loaded kernel modules

Collecting data to determine if dead analysis is justified

kernel version

uptime

filesystem datetime stamps

hash values for system files

current user logins

login history

system logs

- user accounts
- user history files
- hidden files and directories
- sending off suspicious files for further study
- Dumping RAM
- Making the decision to dump RAM
- Using fmem
- Using LiME
- Using /proc/kcore
- Acquiring filesystem images
- Using dd
- Using dcfldd
- Write blocking options
- Forensic Linux distros
- Udev rules based blocker
- Analyzing filesystem images
- Mounting images
- Files with basic system info
- Files with suspicious user info
- Examining logs
- Process-related files
- Authentication-related files
- Using standard Linux tools to find information
- Strange files
- Regular files in /dev
- User history files
- Hidden files
- SUID/SGID files
- Detecting backdated files
- Recovering deleted files
- Finding deleted files
- Attempting recovery
- Leveraging The Sleuth Kit (TSK) and Autopsy
- mmls
- fsstat
- dstat
- istat
- fls & mactime
- Timeline Analysis
- When was system installed, upgraded, booted, etc.
- Newly created files (malware)
- Changed files (trojans)
- Files in the wrong place (exfiltration)
- Digging deeper into Linux filesystems
- Disk editors
- Active@ Disk Editor
- Autopsy
- ExtX
- Basics
- Superblocks
- Directory entries
- Inodes
- Data blocks

Compatible, incompatible, and read-only compatible features
Experimental features may be installed
Boot code

==> [Sharing My Ebook collection for hackers/Penetration testers](#)<==
==> [Giving Reverse Engineering and Exploit Development Course](#)<= Worth \$99.99 USD for free
<==
==> [Giving one way to get Unlimited Free Hosting](#)<==
==> [Sharing Pentester Academy Pentesting iOS Applications Course](#)<==
==> [Giving PayPal Essential Training Course download link](#)<==
==> [A great collection on Cross Site Scripting\[XSS\] Tutorials](#)<==
==> [\[A huge collection\]Ethical Hacking and Penetration Testing \(Kali Linux\) tutorials](#)<==
==> [\[PentesterAcademy\] Linux Forensics course Downloading link](#)<==
==> [\[Course\]USB Forensics and Pentesting Downloading link](#)<==

Thanks ?

Online Sir - August 10, 2016, 7:23 am

Hey mate, I wouldn't mind getting this download!

Thanks pal!

spirited_wolf™ - August 10, 2016, 7:36 am

(Aug 10, 2016 07:23 AM)Webmaster Joey Wrote: [\[CITE\]](#) Hey mate, I wouldn't mind getting this download!

Thanks pal!

I have send you the download link brother ?

Numinous - August 11, 2016, 9:46 am

I wouldn't mind of you send me the link to download, Thanks

spirited_wolf™ - August 12, 2016, 2:11 am

(Aug 11, 2016 09:46 AM)MoneyMakerOnWeb Wrote: [\[CITE\]](#) I wouldn't mind of you send me the link to download, ThanksDone ?

Pmed you ?

Thanks ?

wise rushaan - August 12, 2016, 2:22 am

Can I please get the download link?

Thanks :)

spirited_wolf™ - August 12, 2016, 2:28 am

(Aug 12, 2016 02:22 AM)wise rushaan Wrote: [\[CITE\]](#) Can I please get the download link?

Thanks :)this is only for upgraded member bro ? sorry

i apologize ?

PH2000 - *January 23, 2018, 11:38 am*

Can I get this please?, Thank you so much bro.