

Advanced Linux Detection and Forensics Cheatsheet

by Defensive Security v0.1 [17/05/2024]



/proc:

/proc/modules → Displays a list of all modules loaded into the kernel

/proc/kallsyms → Displays addresses of kernel symbols

/proc/vmallocinfo → Gives mapping of virtual address space of the kernel

/proc/PID/maps → Lists of all the memory-mapped files of a process

/proc/PID/maps | grep '(deleted)' → Lists of deleted memory-mapped files of a process (ex. deleted shared libraries)

/proc/PID/fd/* → Get file descriptors per process

/proc/PID/fd/* | grep 'memfd' → Get processes with anonymous (memory-backed) file descriptors live in RAM

/proc/PID/fdinfo → Contains one entry for each file that the process has open

/proc/PID/map_files/* → Contains entries corresponding to memory-mapped files

€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

/proc/PID/environ → Display environment variables per process

/proc/PID/exe → A symbolic link containing the actual pathname of the executed command

/proc/PID/exe | grep 'deleted' → A symbolic link containing the actual unlinked pathname of the executed command

/proc/PID/comm → Exposes the process's comm value - that is, the command name associated with the process

/proc/PID/cmdline → Holds the complete command line for the process

/proc/PID/cwd → Gets a symbolic link to the current working directory of the process

/proc/PID/status → Status information about the process used by ps

/proc/PID/stack → Symbolic trace of the function calls in this process's kernel stack

/proc/net/unix → List UNIX sockets

/proc/mounts → Lists of all the filesystems currently mounted on the system

/proc/PID/fd/* | grep bpf-map → Get file descriptors per process with bpf-map type

/proc/PID/fd/* | grep bpf-prog → Get file descriptors per process with bpf-prog type

/proc/sys/kernel/tainted → Display the kernel-tainted state

/proc/PID/task/TID/children → Space-separated list of child tasks of this task

€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

/sys:

/sys/kernel/debug/tracing/enabled_functions → contains a list of kernel functions that are currently enabled for tracing

/sys/kernel/debug/tracing/trace →

/sys/kernel/tracing/available_filter_functions → Provides a list of available functions that you can use as filters when setting up tracing

/sys/module/* → List loaded kernel modules, compare with /proc/modules

/sys/module/\$module/parameters → Check available parameters per module

/sys/module/\$module/taint →

/sys/fs/bpf/* → List pinned eBPF progs

Black Hat USA 2024 Training → Practical Linux Attack Paths and Hunting for Red and Blue Team by Leszek Miś / AUGUST 3-6 2024



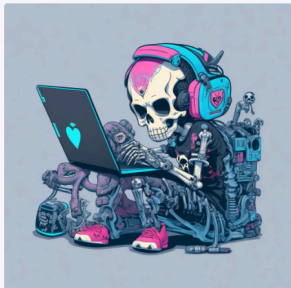
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now

A stylized illustration of a cyberpunk character. The character has a skull for a head, wearing a pink and blue headset. They are sitting at a desk with a laptop that has a blue heart icon on the screen. The character is wearing a blue and pink outfit with mechanical details. The background is a light blue gradient.

<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

"Practical Linux Attack Paths and Hunting for Red and Blue Team" training has been created with a focus on realistic hands-on experience in analyzing user space and kernel space Linux rootkits, including recent Linux APT campaigns, C2 frameworks for Linux with a focus on Sliver/Metasploit overview/behavior vs hunting/DFIR tooling in Linux ecosystem. This training helps create and understand low-level Linux attack paths, improve your Linux detection coverage, see in action many Open Source DFIR/defensive projects, and understand the need for Linux telemetry, especially including Linux/Docker/Kubernetes clusters where Runtime Security solutions are a must these days.

Register here:

<https://www.blackhat.com/us-24/training/schedule/#practical-linux-attack-paths-and-hunting-for-red-and-blue-team-36776>

Logs:

/var/log/messages → Contains global system messages, including the messages that are logged during system startup

/var/log/auth.log → Authentication logs

/var/log/kern.log → Kernel information and events

/var/log/secure → Authentication logs

/var/log/syslog → Contains messages that are recorded by the host about the system activity

/var/log/httpd/ → Apache logs

/var/log/daemon.log → Contains information about running system and application daemons

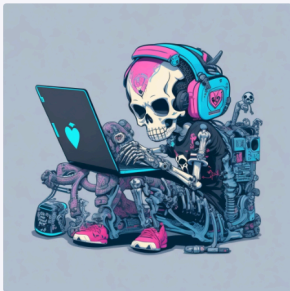
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

/var/log/cron → Cron logs

/var/log/auditd/audit.log | grep denied → Get SELinux alerts

/var/log/journal → journald systemd's logs

journalctl --file X.journal -o verbose > journal.txt → Dump journald logs with verbose output

CLI/tools:

lsmod → Display the status of modules in the Linux Kernel by reading /proc/modules

lsof → "list open files" tool is a robust interface for the information inside the /proc virtual filesystem

ls -al → find hidden files

env → Display environment variables

who / w / pinky → Show logged users

last → show a listing of the last logged-in users based on /var/log/wtmp

lastb → Show a listing of the last unsuccessful logins based on /var/log/btmp

ps -efwww → Get a full list of running processes

grep . FILENAME → single byte read to decloak the file

pstree → Display a tree of processes

find → Find files and directories

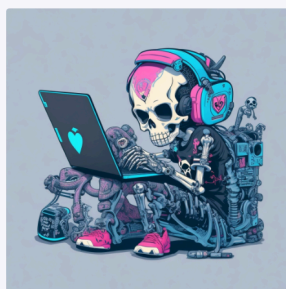
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

dd if=mem bs=1 skip=ADDRESS count=1000 of=/tmp/dumped_proc_file → Extract memory content (1000 bytes) at specified ADDRESS

service --status-all → Display System V services status information

stat → Display file or file system status

readelf → Display information about ELF files

objdump → Display information from object files

strings → Determines the contents of non-text files

capa → Tool to identify capabilities in executable files

yara → Identify and classify malware samples

strace → Trace system calls and signals

ltrace → intercepts and records the dynamic library calls which are called by the executed process and the signals which are received by that process

ip link show | grep xdp →

ip link show | grep qdisc →

sudoreplay → Replay sudo session logs

bpftool prog list → List loaded eBPF programs

bpftool map list → List eBPF maps

dmesg | grep bpf_probe_write_user → Check for the presence of bpf 'bpf_probe_write_user' helper

€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

dmesg | grep taint →

dmesg | grep systemtap → Check for the presense of systemtap

mount → Read /proc/mounts, watch for bind mounted PID dirs to random dir

top → Display current running processes

iptables -L -v -n → Collect firewall rules

iptables -t nat -L -v -n → Collect firewall rules from nat chain

ss → Display listening sockets

uptime → Display how long system has been running

auditctl -l → Display kernel's audit rules

ausearch → Query the audit daemon logs for events based on different search criteria

chkconfig --list → Display a list of all services and their current configuration

systemctl list-units → Display all systemd system units

systemctl list-timers --all → Display timer units currently in memory

systemctl list-unit-files → Display unit files installed on the system

loginctl user-status UID --full → May be used to introspect and control the state of the systemd login manager per user

getenforce → Display the current mode of SELinux

sestatus -v → Display the contexts of files and processes listed in the /etc/sestatus.conf file

€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

dnf list installed → Display installed packages

yum list installed → Display installed packages.

dpkg -I → Display installed packages.

rpm -V -a → Verify all packages to compare information about the installed files in the package with information about the files taken from the package metadata stored in the rpm database

debsums → Verify installed Debian package files against MD5 checksum lists from /var/lib/dpkg/info/*.md5sums

tc qdisc →

ext4magic → List/recover deleted files

log2timeline.py → extract events from individual files and creates a Plaso storage file

getcap -r / 2>/dev/null → displays the name and capabilities of each file

BPFhookdetect → Detect syscall hooking using eBPF

inotify → Provides a mechanism for monitoring filesystem events

lsattr → List file attribute ex. immutable bit

base64 → Encode/decode data and print to standard output

LKRG → Performs runtime integrity checking of the Linux kernel and detection of security vulnerability exploits against the kernel


€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Files/directories/attributes:

`.bash_history` →

`.mysql_history` →

`.ftp_history` →

`.git/logs` →

`/etc/passwd` →

`/etc/group` →

`/etc/fstab` →

`/etc/ssh/sshd_config` →

`/etc/sudoers` →

`.ssh/authorized_keys` →

`.ssh/known_hosts` →

`.viminfo` →

`.gitconfig` →

`/boot/initrd.img` →

`/etc/ld.so.preload` →

`/lib64/ld-2.X.so` → Dynamic linker

`/dev/shm/` →

€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

/dev/ →

suid → Search for files that have SUID bit set

sgid → Search for files that have SGID bit set

/etc/cron* /var/cron* /etc/at* → Linux scheduler

/etc/pam.d →

OSquery/Sunlight/osquery-defense-kit → OSquery queries for Detection & Incident Response:

deleted-or-replaced.sh → Reveal processes that are powered by deleted programs

maps-deleted.sh → Detect processes with loaded deleted shared libraries within memory address space

fake-name.sh → Uncover unexpected programs that are faking their names

hidden-files.sh → Reveal hidden files

hidden-parent-pid.sh → Find processes that have hidden parent IDs

hidden-pids.sh → Reveal rootkits that hide processes from `getdents()` calls to `/proc`

hidden-pids-mount.sh → Detect potential malicious behavior that hides processes from `ps` using `mount -o bind`

pid-hidden-by-rootkit.sh → Finds processes that are apparently hidden by a rootkit

hidden-sys-module.sh → Reveal if there is a hidden `/sys/module` entry

kernel-taint.sh → Diagnose tainted kernels

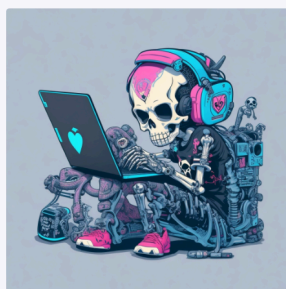
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

ld-so-preload.sh → Find preload entries

mystery-char-devices.sh → Uncover mysterious character devices in /dev

raw-packet-sniffer.sh → Detect raw socket sniffers

rootkit-signal-handler.sh → Detect rootkits, such as Diamorphine, that respond to exotic signals

root-socket-no-libraries.sh → Reveal processes running as root with a socket but no dependencies outside of libc

root-ssh-authorized-keys.sh → Find root SSH authorized keys

suspicious-cron.sh → Reveal suspicious crontab entries

suspicious-proc-env.sh → Find processes that have unusual environment variables

thieves.sh → Reveal programs whose process space may have been taken over by another program

unexpected-ebpf-hooks.sh → Discover suspicious behavior in eBPF

unexpected-run-locks.sh → Reveal processes with weird lock files open in /var/run

unexpected-trace-pipe.sh → Discover kernel modules logging to the trace pipe - this may be the sign of an eBPF-based rootkits

world-readable-run-locks.sh → Show world readable locks in /var/run

bpf-find-maps.sh → Find suspicious bpf maps

bpf-find-progs.sh → Find suspicious bpf programs

bpf-probe-write-user.sh → Find suspicious bpf write user in dmesg

€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

unexpected-ebpf-hooks.sh → Detect suspicious bpf hooks

overwritten-memory-map-ddexec-linux.sh → Detect processes with a memory map that suggests they might be code smuggling

listening-from-unusual-location.sh → Find unexpected programs listening from /tmp or other weird directories

low-fd-socket.sh → Find programs where fd0 (stdin), fd1 (stdout), or fd2 (stderr) are connected to a socket

reverse-shell-socket.sh → Detect potentially suspicious reverse-shell processes

unexpected-dns-traffic.sh → Catch DNS traffic going to machines other than the host-configured DNS server

unexpected-etc-executables.sh → Find unexpected executable files in /etc

unexpected-etc-hosts.sh → Find unexpected potentially suspicious /etc/hosts entries

unexpected-privilege-escalation_linux.sh → Find processes that run with a lower effective UID than their parent PID

unexpected-shell-parents.sh → Find unexpected process that spawns shell processes

unexpected-talkers-linux.sh → Find unexpected programs communicating over non-HTTPS protocols

unusual-process-name-linux.sh → Find processes with suspicious executable names

unexpected-dev-entries.sh → Find unexpected files in /dev

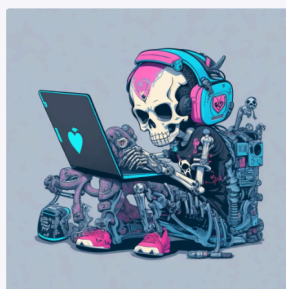
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

unexpected-active-systemd-units.sh → Unexpected systemd units, may be evidence of persistence

unexpected-execdir-linux.sh → Programs running out of unexpected directories

exotic-commands-linux.sh → Find exotic processes based on their command-line

unexpected-privileged-containers.sh → Detect the execution of privileged Docker containers which can be used to escape to the host

unexpected-libcurl-user-linux.sh → Find programs processes which link against libcurl

unexpected-https-linux.sh → Unexpected programs communicating over HTTPS

unexpected-hidden-system-paths.sh → Find unexpected hidden directories in system folders

unexpected-kernel-modules-linux.sh → Find kernel modules that are not part of the expected list

unexpected-setuid-process.sh → Detect running processes that originate from setuid/setgid programs

hidden-modules-filter-functions.sh → Find difference between available_filter_functions and loaded modules

yara-suspicious-strings-process-linux.sh → Find running processes with potentially malicious behavior

unexpected-var-executables-linux.sh → Find unexpected executables in /var

unexpected-tmp-executables-linux.sh → Find unexpected executables in /tmp

unexpected-dev-executables-linux.sh → Find unexpected executables in /dev

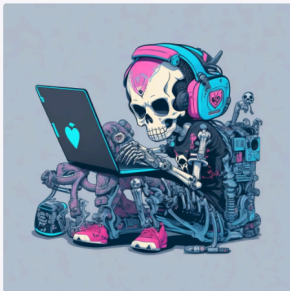
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

unusual-executable-name-linux.sh → Detect processes with executable names that are potentially suspicious

yara-recently-downloaded-go-crypt-exec.sh → Find running processes with recently downloaded cryptexec behavior

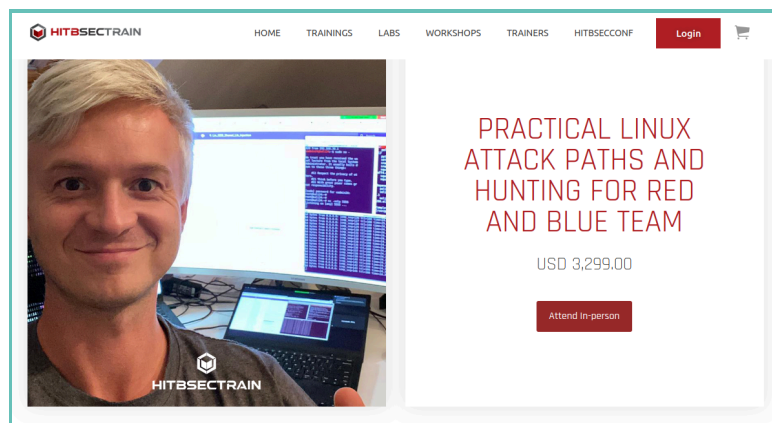
yara-unexpected-upx-process.sh → Find currently running processes backed by UPX executable

unexpected-icmp-socket.sh → Find processes with ICMP socket communication

sudo-preload.sh → Find LD_PRELOAD in /etc/sudoers:

sudo.d-preload.sh → Find LD_PRELOAD in /etc/sudoers.d/*

Hack In The Box Bangkok 2024 Training → Practical Linux Attack Paths and Hunting for Red and Blue Team by Leszek Miś / 26-28 August 2024



"Practical Linux Attack Paths and Hunting for Red and Blue Team" training has been created with a focus on realistic hands-on experience in analyzing user space and kernel space Linux rootkits, including recent Linux APT campaigns, C2 frameworks for Linux with a focus on

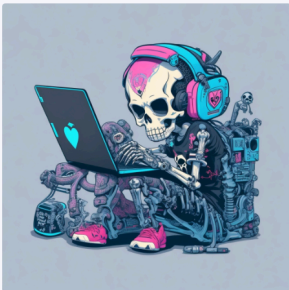
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Sliver/Metasploit overview/behavior vs hunting/DFIR tooling in Linux ecosystem. This training helps create and understand low-level Linux attack paths, improve your Linux detection coverage, see in action many Open Source DFIR/defensive projects, and understand the need for Linux telemetry, especially including Linux/Docker/Kubernetes clusters where Runtime Security solutions are a must these days.

Register here:

<https://conference.hitb.org/hitbsecconf2024bkk/product/practical-linux-attack-paths-bkk2024>

Runtime Security/Tracee → Linux Runtime Security and Forensics using eBPF:

Anti-Debugging Technique → Detects anti-debugging techniques

ASLR Inspection → Detects ASLR inspections

Cgroups notify_on_release File Modification → Monitors notify_on_release file changes in cgroups

Cgroups Release Agent File Modification → Detects changes to the cgroup release_agent

Core Dumps Config File Modification → Monitors core dump configuration alterations.

Default Dynamic Loader Modification → Tracks changes to the default binary loader.

Container Device Mount → Detects unauthorized container device mounts.

Docker Socket Abuse → Flags potential Docker socket misuse

Dropped Executables → Detects runtime-dropped executables.

Dynamic Code Loading → Monitors dynamic code loading events

Fileless Execution → Flags fileless execution techniques


€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Hidden Executable File Creation → Detects creation of hidden executable files

Illegitimate Shell → Flags unauthorized or unexpected shell executions

Kernel Module Loading → Monitors kernel module load events

Kubernetes API Server Connection → Detects connections to the Kubernetes API server

Kubernetes TLS Certificate Theft → Flags potential theft of Kubernetes certificates

LD_PRELOAD Code Injection → Monitors LD_PRELOAD injection attempts

File Operations Hooking on Proc Filesystem → Detects hooks on file operations in /proc

Kcore Memory File Read → Monitors reads of /proc/kcore

Process Memory Access → Flags unauthorized /proc/mem access.

Procfs Mem Code Injection → Detects code injections via /proc/mem

Process VM Write Code Injection → Monitors injections via process_vm_writew

Ptrace Code Injection → Detects ptrace-facilitated code injections.

RCD Modification → Monitors changes to the remote control daemon

Sched Debug Reconnaissance → Flags /proc/sched_debug reconnaissance

Scheduled Tasks Modification → Tracks modifications to scheduled tasks.

Process Standard Input/Output over Socket → Detects IO redirection over sockets

Sudoers File Modification → Monitors alterations to the sudoers file

Syscall Table Hooking → Detects syscall table hook attempts


€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

System Request Key Configuration Modification → Monitors system request key configuration changes

Runtime Security/Falco → Detects and alerts on abnormal behavior and potential security threats in real-time:

Disallowed outbound connection destination

Outbound connection to C2 server

Disallowed SSH Connection

Network connection outside authorized port and binary

Possible miner running

File created below /dev by untrusted program

File created below /etc by untrusted program

File below /etc opened for writing

File below / or /root opened for writing

Interactive root

Privileged container started

Excessively capable container started

Rpm database opened for writing by a non-rpm program


€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

[Buy now](#)



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Shell configuration file has been modified

Cron jobs were scheduled to run

Sensitive file opened for reading by non-trusted program

Database-related program spawned process other than itself

Program run with disallowed HTTP_PROXY environment variable

Known system binary sent/received network traffic

Redirect stdout/stdin to network connection

Interpreted program received/listened for network traffic

Unexpected UDP Traffic Seen

Unexpected setuid call by non-sudo, non-root program

Unexpected connection to K8s API Server from container

Network tool launched on host

Shell history had been deleted or renamed

Hidden file or directory created

Symlinks created over sensitive files

Hardlinks created over sensitive files

An userfaultfd syscall was successfully executed by an unprivileged user

Java process class file download


€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Outbound connection to IP/Port flagged by <https://cryptoioc.ch>

Mount was executed inside a privileged container

Detect Sudo Privilege Escalation Exploit (CVE-2021-3156)

Linux Kernel Module injection using insmod detected

Detect an attempt to exploit a container escape using release_agent file

Drift detected (open+create), new executable created in a container

Runtime Security/Kunai → Threat-hunting tool for Linux:

Execve →

Execve script →

Exit →

Exit group →

Clone →

Prctl →

Init module →

Bpf prog load →

Bpf Socket Filter Attached →

Mprotect exec →

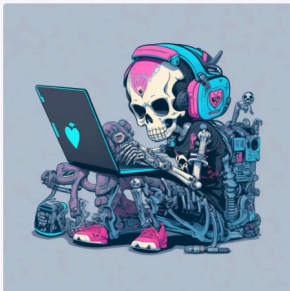
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Mmap exec →

Connect →

Dns query →

Send data →

Read →

Read config →

Write →

Write config →

File rename →

File unlink →

Runtime Security/Tetragon → eBPF-based Security Observability and Runtime Enforcement:

Process Lifecycle Monitoring via exec and exit

Binary Execution in /tmp

sudo Monitoring

Privileges Escalation via SUID Binary Execution

Privileges Escalation via File Capabilities Execution

€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Privileges Escalation via Setuid system calls

Privileges Escalation via Unprivileged User Namespaces

Privileges Change via Capset system call

Fileless Execution

Execution of Deleted Binaries

eBPF System Activity

Kernel Module Audit trail

Shared Library Loading

Network Activity of SSH daemon

Outbound Connections

Velociraptor IR → a tool for collecting host-based state information using The Velociraptor Query Language (VQL) queries:

Linux.Detection.MemFD

Linux.Detection.Yara.Process

Generic.Detection.Yara.Glob

Generic.Detection.Yara.Zip

Linux.Proc.Modules

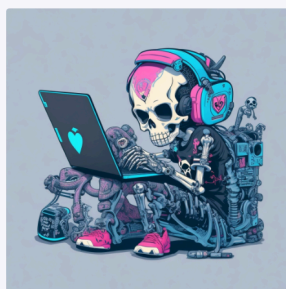
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Linux.Sys.Maps
Linux.Sys.Pslist
Linux.Sys.SUID
Generic.Detection.WebShells
Linux.Memory.AVML
Linux.Detection.IncorrectPermissions
Linux.Network.NM.Connections
Linux.Debian.GPGKeys
Linux.Debian.AptSources
Linux.Debian.Packages
Linux.RHEL.Packages
Generic.Forensic.LocalHashes.Query
Generic.Forensic.LocalHashes.Init
Generic.Forensic.LocalHashes.Glob
Linux.PrivilegeEscalationDetection
Exchange.Linux.Kunai
Linux.LogAnalysis.ChopChopGo
Generic.Collection.UAC


€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Linux.Detection.vRealizeLogInsightExploitation
Linux.Collection.Autoruns
Linux.Collection.BrowserExtensions
Linux.Collection.BrowserHistory
Linux.Collection.DBConfig
Linux.Collection.History
Linux.Collection.NetworkConfig
Linux.Collection.SysConfig
Linux.Collection.SysLogs
Linux.Collection.UserConfig
Linux.System.BashLogout
Linux.Sys.BashShell
Linux.Sys.LastUserLogin
Linux.Sys.Crontab
Linux.Forensics.RecentlyUsed
Linux.Sys.APTHistory
Linux.Sys.JournalCtl
Linux.Forensics.Journal

€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now

<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Linux.Sys.SystemdTimer
Linux.Remediation.Quarantine
Linux.Detection.ConfluenceLogs
Linux.Detection.CVE20214034
Linux.Sys.LogHunter
Linux.Sys.Services
Linux.Sys.Users
Linux.Users.InteractiveUsers
Linux.Users.RootUsers
Linux.Sysinternals.SysmonEvent
Linux.Sysinternals.Sysmon
Generic.Detection.log4jRCE
Linux.Collection.CatScale
Linux.Applications.WgetHSTS
Linux.Network.Netstat
Linux.Network.NetstatEnriched
Linux.Network.PacketCapture
Linux.OSQuery.Generic

€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now

<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

Generic.System.Pstree
Linux.Memory.Acquisition
Linux.Triage.ProcessMemory
Linux.Volatility.Create.Profile
Exchange.Linux.Detection.BPF
Exchange.Linux.System.PAM
Linux.Applications.Docker.Info
Linux.Applications.Docker.Version
Linux.Detection.AnomalousFiles
Linux.Mounts
Linux.Proc.Arp
Linux.Search.FileFinder
Linux.Ssh.AuthorizedKeys
Linux.Ssh.KnownHosts
Linux.Ssh.PrivateKeys
Linux.Syslog.SSHLogin
Linux.Detection.SSHKeyFileCmd

€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons


Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now

<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

44CON London 2024 Training → Practical Linux Attack Paths and Hunting for Red and Blue Team by Leszek Miś / 16–18 Sept 2024

[Home](#) / [44CON Shop](#) / [Training](#) / Practical Linux Attack Paths and Hunting for Red and Blue Team (16-18 Sept 2024)



Practical Linux Attack Paths and Hunting for Red and Blue Team (16–18 Sept 2024)

£2,500.00 ex VAT

Dive into the world of Linux attack paths, local and remote exploitation, process injection, process hiding, tunneling, network pivoting, and syscall hooking techniques. See hands-on how Linux malware, userspace, and kernel space rootkits work in well-prepared Detection PurpleLabs Cyber Range, analyze and modify the source codes, find interesting behavior patterns in binaries and logs, learn what telemetry is needed to catch modern Linux threat actors, and find how to proactively validate and improve detection coverage with step-by-step Linux adversary emulations. On top of that, run your VMs RAM acquisition 'on click' and analyze memory images with Volatility Framework 2/3 at any stage of the course.

This training is a walkthrough of the Open Source Linux offensive and defensive techniques and tooling in 2023/2024 that allows for chaining these TTPs together and understanding better the threat ecosystems in Linux. I trust this training compilation and hands-on experience will change the way you look at hardening and low-level monitoring of your critical Linux-based ecosystems. This course takes on An 'Attack vs. Detection' approach in a condensed format. This class is intended for students who have a basic understanding of Linux and have to deal with advanced threats. Furthermore, the course is also interesting for experienced DFIR/SOC/CERT Players who aim to dig deeper into understanding Linux internals and corresponding network attack analysis techniques, detection, and response. If you want to enhance your understanding of Linux x86/x64 internals and stay prepared for Linux threats, this training is a must-attend!

"Practical Linux Attack Paths and Hunting for Red and Blue Team" training has been created with a focus on realistic hands-on experience in analyzing user space and kernel space Linux rootkits, including recent Linux APT campaigns, C2 frameworks for Linux with a focus on Sliver/Metasploit overview/behavior vs hunting/DFIR tooling in Linux ecosystem. This training helps create and understand low-level Linux attack paths, improve your Linux detection coverage, and see in action many Open Source DFIR/defensive projects, and understand the need for Linux telemetry, especially including Linux/Docker/Kubernetes clusters where Runtime Security solutions are a must these days.

Register here:

<https://44con.com/product/practical-linux-attack-paths-and-hunting-for-red-and-blue-team/>

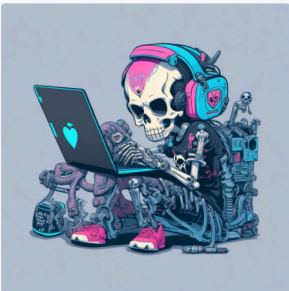
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

[Buy now](#)



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

DFIR/Triage Tools:

UAC → Live Response collection script for Incident Response

LinuxCatScale → Incident Response collection and processing scripts with automated reporting scripts

Fennec → Artifact collection tool for *nix systems

varc → Volatile Artifact Collector collects a snapshot of volatile data from a system

chkrootkit → Checks for signs of a rootkit

rkhunter → Rkhunter Malware Scanner for linux

lynis → Security auditing tool for Linux, macOS, and UNIX-based systems

Unhide → Forensic tool to find hidden processes and TCP/UDP ports by rootkits

GRR Rapid Response → Incident response framework focused on remote live forensics

sandfly-file-decloak → Decloak Linux stealth rootkits hiding data with this simple memory mapped IO investigation tool

sandfly-process-decloak → Utility to quickly scan for Linux Process IDs (PIDs) that are hidden by common and not-so-common loadable kernel module stealth rootkits and decloak them so they are visible

sandfly-entropyscan → Entropy scanner for Linux to detect packed or encrypted binaries related to malware

Sandfly Security → The greatest agentless Linux intrusion detection and incident response platform. Find Linux threats without endpoint agents instantly → <https://sandflysecurity.com/>

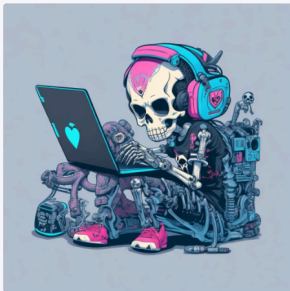
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn Linux attack, detection, and live forensics based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>

LINKS:

- <https://github.com/falcosecurity/falco>
- <https://github.com/aquasecurity/tracee>
- <https://github.com/cilium/tetragon>
- <https://github.com/Sysinternals/SysmonForLinux/>
- <https://why.kunai.rocks/>
- <https://github.com/chainguard-dev/osquery-defense-kit>
- <https://github.com/tstromberg/sunlight>
- <https://github.com/Velocidex/velociraptor>
- <https://github.com/lkrg-org/lkrg>
- <https://github.com/sandflysecurity/sandfly-file-decloak>
- <https://github.com/sandflysecurity/sandfly-processdecloak>
- <https://github.com/tclahr/uac>

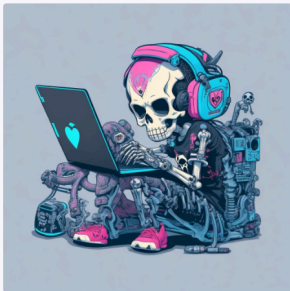
€449

Linux Attack, Detection and Live Forensics + 90 Days PurpleLabs Access

Course • 221 Lessons

Learn **Linux attack, detection, and live forensics** based on hands-on analyses of user space and kernel space Linux rootkits, C2 frameworks, and tools. Create low-level Linux attack paths, know better Linux internals, improve your Linux detection, understand the need for Linux telemetry, and stay prepared for Linux threats.

Buy now



<https://edu.defensive-security.com/linux-attack-live-forensics-at-scale>