Current version: @ 7.01.2025

EDRmetry is an effective Linux EDR/SIEM Evaluation Testing Playbook that allows for examination and learning how to execute custom security validation checks mapped to MITRE ATT&CK™ Framework. We provide hands-on and cost-effective methods using open-source offensive tools and a collection of well-prepared Linux tricks and scripts to simulate attacks and better understand your EDR/SIEM technology of choice.

Understanding the effectiveness of your Linux cybersecurity measures is more critical than ever. While you invest in expensive security tools like EDR/XDR, set up Security Operations Centers (SOCs), and implement Security Information and Event Management (SIEM) systems, how can you truly assess their performance against real-world Linux threats and complex attacks? How do you choose and validate EDR/SIEM for your Linux needs?

Learn about EDRmetry and 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, find interesting behavior patterns in binaries and logs, learn what telemetry is needed to catch modern Linux threat actors, and how to proactively validate and improve detection coverage with step-by-step Linux adversary emulations.

Discovery:

- Kcore Memory File Read
- Enumerate kernel modules
- Execute nping
- Sudo Enumeration
- Local Network Discovery Scan
- Download and launch LinEnum
- Execute LinPEAS from /dev/tcp
- Check bpf settings from /proc
- C2 randomized hostname lookups
- /proc enumeration
- Read local file using curl
- Check ASLR configuration

- Check my public IP

Privilege Escalation:

- Socket Command Injection
- Exploit local suid binary
- Mount of host device FS in container
- Register LKM Char Device + LPE
- NFS SUID Escalation
- Docker socket LPE
- MySQL wsrep_provider CVE-2021-27928
- $PATH Hijacking
- Exploit vulnerable LKM driver
- Set setuid/setgid via chmod
- Execute Trap signals

Initial Access:

- ActiveMQ CVE-2023-46604 Exploitation
- Remote Use-after-free Exploitation
- Code Execution via SSH XZBackdoor
- MySQL Brute Force
- Apache Tomcat Manager Exploitation
- Solr Log4J JNDI Exploitation
- Kafka CVE-2023-25194 Exploitation
- Apache Tomcat Manager Brute Force
- Apache HTTP CVE-2021-41773 Exploitation
- Oracle WebLogic SSRF Exploitation
- HTTPD CVE-2014-6271 Shellshock RCE
- Spring CVE-2022-22963 Exploitation

Execution:

- Load/unload kernel module
- HTTP GET data with /dev/tcp
- MySQL UDF Command Execution
- Dump process memory via GDB
- Encrypted ELF implant

- Export proxy_http
- Bash - File download without curl
- Execute LKM call_usermodehelper() on ICMP
- Renice or Ulimit Execution
- At execution
- Modify core_pattern file
- Python - File download without curl
- Perl - File download without curl
- Install malicious rpm package
- Execute binary listening from a hidden directory as root
- OpenSSL - File download without curl
- Execute Linux Hack Tools
- Establish Unix Socket connection
- Simplest Proc Name Masquerading
- File Transfer to a hidden directory
- eBPF system(\"whoami\") Execution with bpftrace
- Enable MSR Write Access

Persistence:

- SSHD Dummy Cipher Suite
- PHP Obfuscated
- Webshell PHP Eval
- Webshell PHP Proc Open
- Webshell PHP p0wny-shell
- Webshell Tinyshell
- Webshell PHP Simple popen()
- PHP filter chain generator
- PHP POST method
- PHP GET method
- PHP Weevly
- Smallest PHP base64 Backdoor
- LKM Reveng Rootkit
- LKM Suterusu Rootkit
- Crontab root Backdoor
- Docker with host escape
- Run setcap+cap_setuid over linker
- At job persistence
- Execute Static Reverse SSH server
- Modify crontab with @reboot
- PAM rootok plugin
- Git hook persistence
- eBPF Boopkit Rootkit

- LKM KoviD Rootkit
- DNF Package Manager Persistence
- HTTPD mod_backdoor module
- Add Backdoor User - /etc/passwd modification
- Add User to Privileged Group
- Add new group
- SSH Authorized keys
- Modify Bash profile files
- PAM Static Password Backdoor
- Systemd Backdoor Timer Service
- Netfilter Hooking
- Udev+atd C2 persistence
- Yum package manager
- Systemd Backdoor service
- LKM rootkit - Diamorphine
- Modify /etc/ld.so.preload for syscall hooking
- Add backdoor user with uid=0
- eBPF mount bpffs
- Python .pth Extensions
- /etc/sudoers Modification
- HTTPD mod_authg Backdoor
- LKM Reptile Rootkit
- Revshell ~/.profile background
- Ftrace Hooking Rootkit
- SUID backdoor
- xt_conntrack.ko Rootkit
- eBPF TripleCross Rootkit
- eBPF sudo Rootkit
- eBPF Magic Port Tracepoint Execution with bpftrace
- Udev backdoor rule
- Systemd-run Backdoor Timer Service
- Systemtap creds() upgrade
- Copy Dynamic Linker

Credential Access:

- eBPF pamspy
- Sniff sshd with strace
- eBPF Sniff pam_get_authtok() with bpftrace
- Read /etc/shadow
- SSH Brute Force / Spraying
- Dump credentials via unshadow
- eBPF Sniff PTY with bpftrace

Defense Evasion:

- LD_PRELOAD Shared Library shell_reverse_tcp
- Create a hidden shared object file
- Execute Invisible SSH notty session
- Load BOF/ELF object in memory via ELFLoader
- Disable EDR/XDR sensor
- Block rsyslogd logging
- Process Name Masquerading with exec
- Process Injection over dd+/proc/PID/mem
- Disable .bash_history
- Disable/modify iptables rules
- Copy/move system binaries to exotic directory
- Space before command
- Load BOF with bof-launcher
- Bash script obfuscation
- File immutable with chattr
- eBPF Rename Loaded LKM module
- Clear kernel ring buffer
- Process Name Masquerading with prctl()
- Process Name Masquerading with argv[0] overwrite
- Process Name Masquerading with clear_env()
- Suspicious File/Directory Location
- Timestomping - Modifying the system date
- Timestomping - touch
- File immutable with mount
- Ptrace() Shared Object Process Injection
- Fileless memfd_create execution
- Modify /etc/hosts
- mount --bind process hiding
- Execute PRoot
- Delete file with shred
- In-memory LKM finit_module() Remote Load
- Hide process name
- Fileless Execution with memexec
- Execute fileless ELF with fee
- Ptrace Process Hiding with Zapper
- Proxy Execution with DDexec
- Hidden Executable File Creation in /dev/shm
- Disable ASLR
- Zombieant Preloading a decoy binary
- eBPF Hide PID

Exfiltration:

- ICMP_exfil + nping Exfiltration
- ICMP Python Scapy Exfiltration
- Upload data over HTTP/HTTPS
- Upload data over SMB
- PAM creds over HTTP Post
- Upload/download data over SSHFS
- Exfil data using rsync
- Python FTP Upload
- NTP Data Exfiltration
- DNS Exfiltration
- Upload/Exfil data over SCP/SFTP
- Exfil data using transfer.sh
- Upload data over WebDAV
- eBPF Magic String Tracepoint Execution with bpftrace

Command and Control:

- Mythic+Thanalos HTTP C2
- Mythic+Poseidon Websockets C2
- Upgrade a reverse shell to a PTY shell
- Revshell curl+telnet
- Revshell socat+bash
- Revshell curlshell
- Revshell mkfifo+nc
- Revshell Perl+socket
- Revshell python+socket+pty
- RMM Anydesk
- RMM ScreenConnect
- RMM Alpemix
- RMM TeamViewer
- openssl+bash+/dev/fd/3
- RMM Meshcentral
- Webshell PHP FFI
- Execute process via ProxyChains
- Sliver C2 MTLS
- Execute Offensive Linux Tunneling tools
- Base64 script
- Revshell perl+ENV keys

- XOR shell_reverse_tcp Loader
- Ngrok Tunneling
- Meterpreter reverse_tcp/https
- Shell Over Reverse SSH
- Shell over HTTP streams
- Revshell Python TLS
- Revshell over GDB
- PHP+bash
- Gsocket Secure Connection
- JSP+sh
- Make Non-standard port HTTP/HTTPS connection
- Process Masquerading as kworker+exec+/dev/tcp
- Merlin HTTPX C2
- Emp3r0r C2 Shadowsocks C2

Lateral Movement:

- SSH Linux Tunneling
- Generate egress SMB connection
- DNS Zone Transfer
- Hijack SSH Client Session
- Ligolo-ng Reverse TCP/TLS Tunneling
- Visit malicious Threat Intel URL
- Network ping sweep
- Make internal network connection via Telnet
- Socks Proxy from JSP
- Create malicious file remotely
- Establish TOR connection
- Execute Port Scanning
- Create a SOCKS proxy with ssh
- Reverse SOCKS5 proxy

Impact:

- Ransomware Black Basta
- Ransomware python
- Ransomware C
- Ransomware bash+openssl