Vulnhub Privilege Escalation Cheatsheet

Abusing Sudo Rights

- tcpdump — Breach 2.1
- tcpdump — Temple of Doom
- tcpdump — Web Developer : 1
- teehee — DC-4
- vim — Serial: 1
- zip — Zico 2
- zip — HA: Dhanush
- cat — Sunset: Nightfall
- ftp — HA: Infinity Stones
- wine — Sunset-Sunrise
- php — Me and My Girlfreind:1
- dpkg — Symfonos:5
- service — Five86:2
- Diffrent for every user — Tempus Fugit:1
- dpkg — DevRandom CTF:1.1
- cp — Zion: 1.1
- script — Seppuku:1
- git — GitRoot: 1
- shutdown — Tre:1
- script — BlackRose: 1
- script — So Simple:1
- All — CryptoBank:1
- All — Star Wars:1
- Mercury
- script
- script — Durian:1
- gcc — nyx:1
- node — Relevant:1
- dpkg — Maskcrafter:1.1
- vim — Hogwarts:Bellatrix
- Ted:1 — apt-get
- KF1OFan : 1 — awk
- 21 LTR: Scene1 — cat
- Skytower — cat
- Matrix : 1 — cp
- Sputnik 1 — ed
- Sunset — ed
- DC-2 — git
- Kioptrix : Level 1.2 — ht
- Matrix-3 — manual
- symfonos : 2 — MySQL
- Development — nano
- SP ike — nmap
- DC6 — nmap
- Dina — perl
- Wakanda : 1 — pip
- Violator — proftpd
- Broken: Gallery — reboot/timedatectl
- DE-ICE:S1.120 — script
- Fristileaks — script
- DerpNStink — script
- Digitalworld.local : JOY — script
- PumpkinFestival — script
- The Ether: Evil Science — script
- HA:Rudra — script
- djinn:1 — script
- UA: Literally Vulnerable
- script
- PumpkinRaising — strace
- Unknowndevice64 : 1 — strace
- Holynix: v1 — tar

SUID

- cp — HA: Wordy
- find — bossplayersCTF 1
- script — In Plain Sight:1
- script — Five86:1
- base32 — Geisha:1
- nohup — Victim:1
- script — eLection: 1
- php7.2 — Photographer 1
- script — DMV :1
- cpulimit — ShellDredd #1 Hannah
- systemctl — KB-Vulnr:3
- register — Cybox:1
- Kevgir — cp
- digitalworld.local - BRAVERY — cp
- Happycorp : 1 — cp
- FourAndSix : 2 — doas
- tc:1 — find
- dpwwn:2 — find
- MinU: v2 — Micro Editor
- Toppo:1 — python 2.7/mawk
- Mr. Robot — nmap
- Covfefe — script
- /dev/random : K2 — script
- hackme1 — script
- Sunset: dawn — zsh

Kernel

- 39772 — Ubuntu 16.04 — Stapler
- 39772 — Ubuntu 16.04 — Sidney
- 39772 — Ubuntu 16.04 — DC-3
- 40616 — Dirty COW — Pluck
- 40847 — Dirty COW /proc/self/mem' Race Condition — Lampiao : 1
- 41154 — GNU Screen 4.5.0 — WinterMute :1
- 41154 — GNU Screen 4.5.0 — DC-5
- 41458 — Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free — BTRSys:sdr 2.1
- 43418 — Ubuntu 14.04/16.04 (KASLR / SMEP) — Nightmare
- 44298 — Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) — Trollcave
- 44298 — Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) — Prime: 1
- 8478 — Linux Kernel 2.6 — LAMPSecurity: CTF6
- 40616 — Dirty COW — My File Server:1
- 48106 — GUnet OpenEclass E-learning platform 1.7.3 — VulnUni 1.0.1
- 40839 — Dirty COW — Sumo: 1
- 37292 — Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' — CyberSploit: 1
- 45010 — Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) — Loly: 1
- 45010 — Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) — Tomato: 1
- pWnOS -1.0 — Linux Kernel 2.6.17 < 2.6.24.1 — 5092
- LAMPSecurity: CTF 5 — Linux Kernel 2.4/2.6 — 9479
- Kioptrix : Level 1.1 — CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) — 9542
- Hackademic-RTB1 — RDS Protocol' Local Privilege Escalation — 15285
- Hackademic-RTB2 — RDS Protocol' Local Privilege Escalation — 15285
- ch4inrulz : 1.0.1 — RDS Protocol' Local Privilege Escalation — 15285
- Kioptrix: 5 — FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation — 28718
- Simple — Apport/Abrt (Ubuntu / Fedora) — 36746
- SecOS: 1 — Ubuntu 12.04/14.04/14.10/15.04 — 37292
- Droopy — Ubuntu 12.04/14.04/14.10/15.04 — 37292
- VulnOS: 2.0 — Ubuntu 12.04/14.04/14.10/15.04 — 37292
- Fartknocker — Ubuntu 12.04/14.04/14.10/15.04 — 37292
- Super Mario — Ubuntu 12.04/14.04/14.10/15.04 — 37292
- Golden Eye:1 — Ubuntu 12.04/14.04/14.10/15.04 — 37292
- Typhoon : 1.02 — Ubuntu 12.04/14.04/14.10/15.04 — 37292
- GrimTheRipper:1 — Ubuntu 12.04/14.04/14.10/15.04 — 37292
- 6days — Ubuntu 12.04/14.04/14.10/15.04 — 37292
- Lord of the Root — Ubuntu 14.04/15.10 — 39166
- Acid Reloaded — Ubuntu 14.04/15.10 — 39166

Path Variable

- whoami — Beast 2
- ifconfig — HA:Arsenal Avengers
- whoami — Inclusiveness:1
- ls — MuzzyBox:1
- sl — TBBT:2
- service — Sunset: Midnight
- fdisk — Healthcare:1
- Pwnlab — cat
- USV — cat
- Zeus:1 — date
- The Gemini inc — date
- Ew-Skuzzu — id
- Nullbyte — ps
- symfonos : 1 — curl
- Silky-CTF: 0x01 — whoami

Enumeration

- Depth
- Bob: 1.0.1
- W34kn3ss 1
- Replay: 1
- Born2Root: 2
- CLAMP 1.0.1
- WestWild: 1.1
- 64base
- C0m80
- Gibson
- Quaoar
- Hacker Fest: 2019
- EVM: 1
- EnuBox:Matterman3
- 2much3
- mhz_cxf:c1f
- HA: Pandavas
- GreenOptic:1
- Cewlkid:1
- PowerGrid:1.0.1
- Insanity:1
- Tempus Fugit:3
- HA: Forensics
- HA: Vedas
- HA: Sherlock
- The Library:1
- The Library:2
- LAMPSecurity: CTF 4
- LAMPSecurity: CTF 7
- Xerxes: 1
- pWnOS -2.0
- DE-ICE:S1.130
- Tommyboy
- VulnOS: 1
- Spyder Sec
- Acid
- Necromancer
- Freshly
- Fortress
- Billu : B0x
- Defence Space
- Moria 1.1
- Analougepond
- Lazzysysadmin
- Bulldog
- BTRSys 1
- G0rmint
- Blacklight : 1
- The blackmarket
- Matrix 2
- Basic Pentesting : 2

MySQL

- Raven : 2
- Kioptrix : Level 1.3
- Raven

Cronjob

- Sar
- TBBT
- Glasgow Smile: 1.1
- LemonSqueezy:1
- Billy Madison
- BSides Vancuver: 2018
- Jarbas : 1
- SP:Jerome
- dpwwn: 1

Wildcard Injection

- Milnet
- Pipe

Capabilities

- Connect The Dots:1
- Katana
- Presidential:1
- Kuya : 1
- DomDom:1
- HA: Naruto

Writable files

- Nezuko:1
- Smfonos:3
- Tr0ll 1
- DC:7
- View2aKill
- CengBox:1
- Broken 2020:1
- CengBox:2
- HA:Narak
- Skydog
- Breach 1.0
- Bot Challenge: Dexter
- Fowsniff : 1
- Mercy
- Casino Royale
- SP eric
- PumpkinGarden
- Tr0ll:3

Writable /etc/passwd

- HA: ISRO
- Gears of War: EP#1
- DC:9
- Sahu
- Sunset Twilight
- Chilli:1
- Hackday Albania
- Billu Box 2
- Bulldog 2
- AI: Web: 1
- Westwild: 2
- Misdirection 1

Buffer Overflow

- ROP Primer
- CTF KF1OFAN:2
- Kioptrix : Level 1
- Silky-CTF: 0x02
- Tr0ll 2
- IMF
- BSides London 2017
- PinkyPalace

Docker

- Mumbai:1
- Sunset:dusk
- Pwned:1
- Donkey Docker
- Game of Thrones
- HackinOS:1
- HA: Chakravyuh

Chkrootkit

- HA: Chanakya
- Sunset: decoy
- SickOS 1.2
- Sedna

Bruteforce

- Cyberry:1
- Born2root
- Rickdiculously
- RootThis : 1
- LAMPSecurity: CTF 8

Writable /etc/shadow

- Basic Penetration
- W1R3S.inc
- DE-ICE:S1.140
- Minotaur
- Moonraker:1

NFS

- Orcus
- FourAndSix

Json

- MinU: 1 — Json Token
- Symfonos:4 — Json Pickle

Redis

- Gemini inc:2

LXD

- CyNix:1
- AI: Web: 2
- HA: Joker

ALL

- Jigsaw:1
- Lin.Security
- Escalate_Linux

Exim

- DC:8

Apache2 Writable

- HA: Natraj
- Torment
- HA: Armour

www.hackingarticles.in