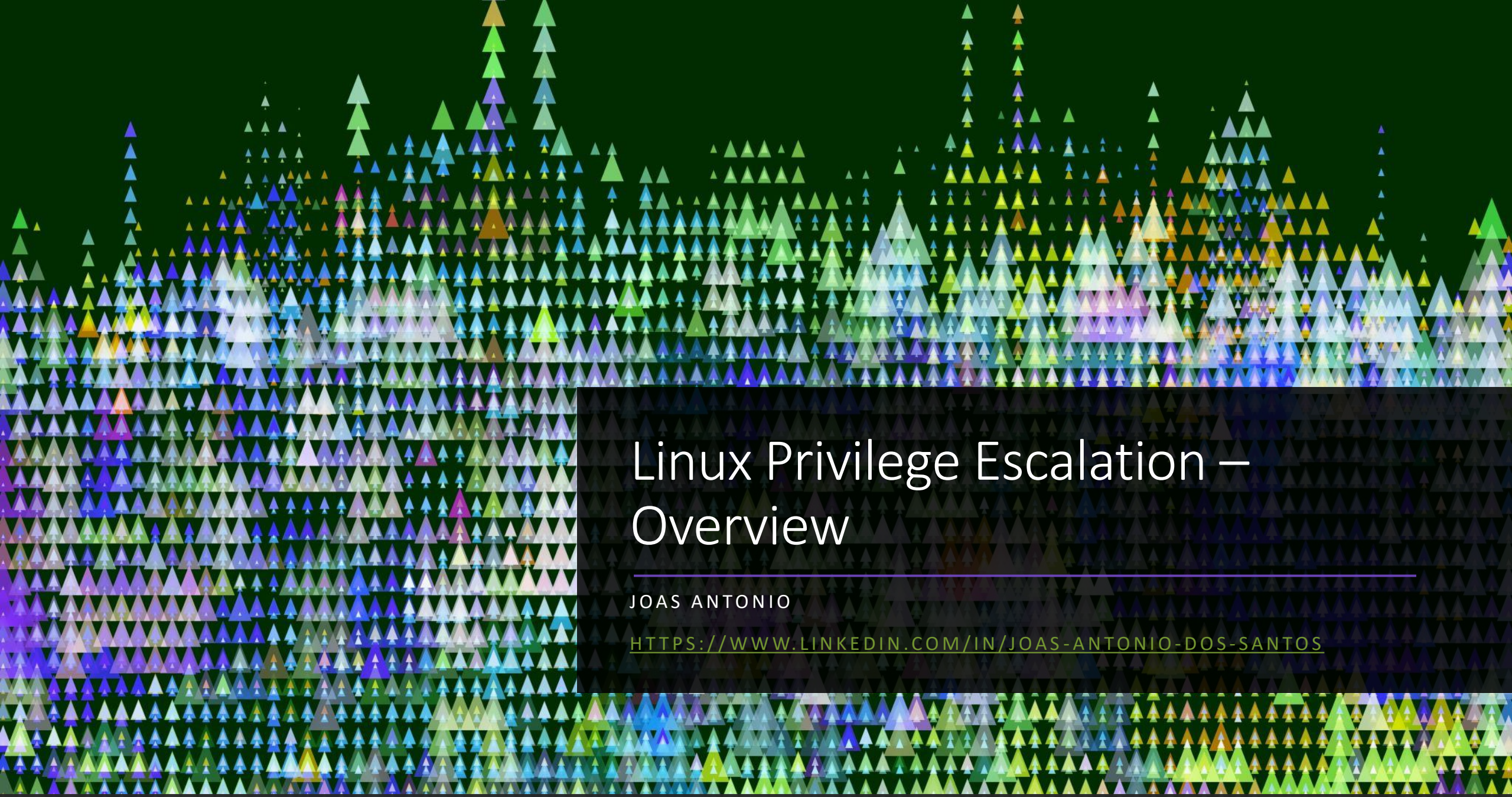

Linux Privilege Escalation – Overview

JOAS ANTONIO

HTTPS://WWW.LINKEDIN.COM/IN/JOAS-ANTONIO-DOS-SANTOS

What is Privilege Escalation?

In general, attackers exploit privilege escalation vulnerabilities in the initial attack phase to override the limitations of their initial user account in a system or application. There are two main types of privilege escalation: *horizontal privilege escalation* to access the functionality and data of a different user and *vertical privilege escalation* to obtain elevated privileges, typically of a system administrator or other power user.

https://www.netsparker.com/blog/web-security/privilege-escalation/

What is Privilege Escalation? 2

With horizontal privilege escalation, malicious actors remain on the same general privilege level but can access data or functionality of other accounts or processes that should be unavailable to them. For example, this may mean using a compromised office workstation to gain access to other office users' data. For web applications, one example of horizontal escalation might be using session hijacking to bypass authentication and get access to another user's account on a social site, e-commerce platform, or e-banking site.

More dangerous is vertical privilege escalation (also called *privilege elevation*), where the attacker gains the rights of a more privileged account – typically the administrator or system user on Microsoft Windows or root on Unix and Linux systems. With this elevated level of access, the attacker can wreak all sorts of havoc in your computer systems and applications: steal access credentials and sensitive data, download and execute ransomware, erase data, or execute arbitrary code. Advanced attackers will use elevated privileges to cover their tracks by deleting access logs and other evidence of their activity, leaving the victim unaware that an attack took place at all. That way, cybercriminals can covertly steal information and plant backdoors or other malware in company systems.

Linux Privilege Escalation Techniques

- Kernel exploits
- Programs running as root
- Installed software
- Weak/reused/plaintext passwords
- Inside service
- Suid misconfiguration
- Abusing sudo-rights
- World writable scripts invoked by root
- Bad path configuration
- Cronjobs
- Unmounted filesystems

Enumeration Scripts

- https://github.com/rebootuser/LinEnum
- https://pentestmonkey.net/tools/audit/unix-privesc-check
- https://github.com/reider-roque/linpostexp/blob/master/linprivchecker.py
- https://github.com/carlospolop/PEASS-ng
- https://raw.githubusercontent.com/redcode-labs/Bashark/master/bashark.sh
- https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
- https://raw.githubusercontent.com/rtcrowley/linux-private-i/master/private-i.sh
- https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh

Enumeration Scripts

- https://github.com/rebootuser/LinEnum
- https://pentestmonkey.net/tools/audit/unix-privesc-check
- https://github.com/reider-roque/linpostexp/blob/master/linprivchecker.py
- https://github.com/carlospolop/PEASS-ng
- https://raw.githubusercontent.com/redcode-labs/Bashark/master/bashark.sh
- https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
- https://raw.githubusercontent.com/rtcrowley/linux-private-i/master/private-i.sh
- https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh
- https://github.com/AlessandroZ/BeRoot
- https://github.com/TH3xACE/SUDO_KILLER

Checklist

- Kernel and distribution release details
- System Information:
  - Hostname
  - Networking details:
  - Current IP
  - Default route details
  - DNS server information

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md

Checklist 2

- User Information:
  - Current user details
  - Last logged on users
  - Shows users logged onto the host
  - List all users including uid/gid information
  - List root accounts
  - Extracts password policies and hash storage method information
  - Checks umask value
  - Checks if password hashes are stored in /etc/passwd
  - Extract full details for 'default' uid's such as 0, 1000, 1001 etc
  - Attempt to read restricted files i.e. /etc/shadow
  - List current users history files (i.e .bash_history, .nano_history, .mysql_history , etc.)
  - Basic SSH checks

Checklist 3

- Privileged access:
  - Which users have recently used sudo
  - Determine if /etc/sudoers is accessible
  - Determine if the current user has Sudo access without a password
  - Are known 'good' breakout binaries available via Sudo (i.e. nmap, vim etc.)
  - Is root's home directory accessible
  - List permissions for /home/

Checklist 4

- Environmental:
  - Display current $PATH
  - Displays env information
- Jobs/Tasks:
  - List all cron jobs
  - Locate all world-writable cron jobs
  - Locate cron jobs owned by other users of the system
  - List the active and inactive systemd timers

Checklist 5

- Services:
  - List network connections (TCP & UDP)
  - List running processes
  - Lookup and list process binaries and associated permissions
  - List inetd.conf/xined.conf contents and associated binary file permissions
  - List init.d binary permissions
- Version Information (of the following):
  - Sudo
  - MYSQL
  - Postgres
  - Apache
    - Checks user config
    - Shows enabled modules
    - Checks for htpasswd files
    - View www directories

Checklist 6

- Default/Weak Credentials:
  - Checks for default/weak Postgres accounts
  - Checks for default/weak MYSQL accounts
- Searches:
  - Locate all SUID/GUID files
  - Locate all world-writable SUID/GUID files
  - Locate all SUID/GUID files owned by root
  - Locate 'interesting' SUID/GUID files (i.e. nmap, vim etc)
  - Locate files with POSIX capabilities
  - List all world-writable files
  - Find/list all accessible *.plan files and display contents
  - Find/list all accessible *.rhosts files and display contents
  - Show NFS server details
  - Locate *.conf and *.log files containing keyword supplied at script runtime
  - List all *.conf files located in /etc
  - Locate mail
- Platform/software specific tests:
  - Checks to determine if we're in a Docker container
  - Checks to see if the host has Docker installed
  - Checks to determine if we're in an LXC container

Privilege Escalation - Links

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

https://sushant747.gitbooks.io/total-oscp-guide/content/privilege_escalation_-_linux.html

https://book.hacktricks.xyz/linux-unix/privilege-escalation

https://payatu.com/guide-linux-privilege-escalation

https://patchthenet.com/articles/linux-privilege-escalation-three-easy-ways-to-get-a-root-shell/

https://medium.com/swlh/linux-privilege-escalation-in-four-ways-eedb52903b3

https://blog.ikuamike.io/posts/2021/package_managers_privesc/

https://johnjhacking.com/blog/linux-privilege-escalation-quick-and-dirty/

Privilege Escalation – Links 2

https://tbhaxor.com/linux-privilege-escalation/

https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/

https://www.exploit-db.com/docs/49411

https://blog.pentesteracademy.com/breaking-out-of-a-restricted-shell-linux-privilege-escalation-3fb2700cb85e

https://steflan-security.com/linux-privilege-escalation-exploiting-capabilities/

https://infosecwriteups.com/write-up-11-common-linux-privilege-escalation-92528853b616

https://www.darkreading.com/vulnerabilities-threats/nearly-all-linux-oses-have-a-pair-of-privilege-escalation-flaws

https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/

Privilege Escalation – Links 3

https://www.detectx.com.au/linux-privilege-escalation/

https://netsec.ws/?p=309

https://tryhackme.com/room/linuxprivesc

https://hackerculture.com.br/?p=1114

https://www.youtube.com/watch?v=bDjiTnBtp88

https://www.youtube.com/watch?v=QZhz64yEd0g

https://www.youtube.com/watch?v=VpNaPAh93vE

https://www.youtube.com/watch?v=JRI9OD0c5DQ

https://www.youtube.com/watch?v=PjjuZwVvCgc

https://www.youtube.com/watch?v=d_FWNmEeeBg

https://www.youtube.com/watch?v=IX9psKsmXcE

https://www.youtube.com/watch?v=9t0XL6Ywo0w

https://www.youtube.com/watch?v=WKmbIhH9Wv8

Privilege Escalation – Links 4

https://www.youtube.com/watch?v=tFhfph_KbTk&list=PLCLxMnnAnGil85NEbGa7ZWFmOPq4V7t2w

https://www.youtube.com/watch?v=mbXztdcrA7o&list=PLV_npv_S1L92aOCv1K0Ui1stydPNMdhnh

https://www.youtube.com/watch?v=7WQndt-1WzE

https://www.youtube.com/watch?v=7JECV2b-a0w

https://www.youtube.com/watch?v=-8joUO7arzU

Kernel Exploits

https://github.com/lucyoa/kernel-exploits

https://github.com/xairy/linux-kernel-exploitation

https://github.com/bcoles/kernel-exploits

https://steflan-security.com/linux-privilege-escalation-kernel-exploits/

https://www.exploit-db.com/search?q=Linux+Kernel+

Services Exploits and Weak File Permissions

https://www.youtube.com/watch?v=nKYy2Smio7s

https://www.youtube.com/watch?v=mbXztdcrA7o

https://www.youtube.com/watch?v=8IjTq7GBupw

https://attack.mitre.org/techniques/T1574/010/

https://gtfobins.github.io/

https://dmcxblue.gitbook.io/red-team-notes/privesc/file-system-permissions-weakness

https://atom.hackstreetboys.ph/linux-privilege-escalation-weak-file-permission/

https://www.youtube.com/watch?v=EqSyI3k98K8

https://www.youtube.com/watch?v=ZKi0bpKo9DA

https://infinitelogins.com/2021/02/24/linux-privilege-escalation-weak-file-permissions-writable-etc-passwd/

https://pentestlab.blog/2017/03/30/weak-service-permissions/

https://codeh4ck3r.github.io/posts/weak-file-permissions-1/

Sudo

https://medium.com/schkn/linux-privilege-escalation-using-text-editors-and-files-part-1-a8373396708d

https://steflan-security.com/linux-privilege-escalation-vulnerable-sudo-version/

https://www.bleepingcomputer.com/news/security/new-linux-sudo-flaw-lets-local-users-gain-root-privileges/

https://github.com/TH3xACE/SUDO_KILLER

Cron jobs

https://materials.rangeforce.com/tutorial/2020/04/17/Cron-Privilege-Escalation/#:~:text=Cron%20Privilege%20Escalation&text=When%20a%20script%20executed%20by,is%20in%20%2Fetc%2Fcrontab%20.

https://medium.com/swlh/privilege-escalation-via-cron-812a9da9cf1a

https://www.hackingarticle s.in/linux-privilege-escalation-by-exploiting-cron-jobs/

https://steflan-security.com/linux-privilege-escalation-scheduled-tasks/

https://atom.hackstreetboys.ph/linux-privilege-escalation-cron-jobs/

https://www.youtube.com/watch?v=ewWBJCd6hRY

https://www.youtube.com/watch?v=EhEWDm2HpvI

https://tbhaxor.com/exploiting-the-cron-jobs-misconfigurations2/

Password & Keys

https://atom.hackstreetboys.ph/linux-privilege-escalation-password-and-keys/

https://steflan-security.com/linux-privilege-escalation-credentials-harvesting/

https://martinkubecka.github.io/posts/thm/linux-privilege-escalation/

https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

https://hackmag.com/coding/linux-privileges-escalation/