Level 0x06

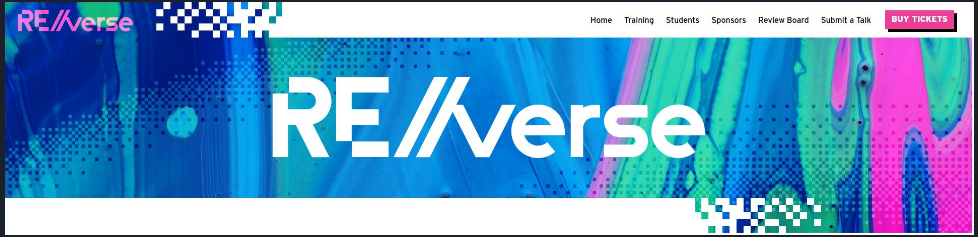
Privilege Escalation

Topics

- Events
- Privilege Escalation
- Some Fails

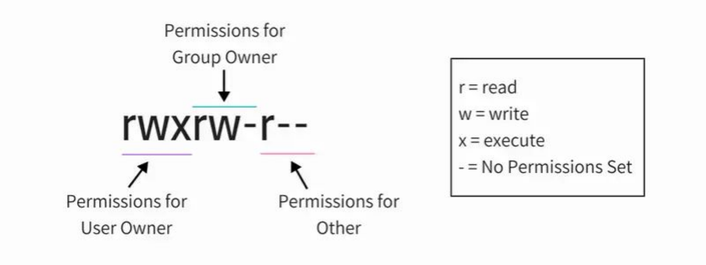
Laurie Kirk aka LaurieWired

- Reverse Engineer at ~~Microsoft~~ Google
- FSU Computer Science Major
- Malware researcher (mobile)
- Youtuber
- Many presentations
- Keynote presenter at RE//verse
  - March 5-7th, 2026 in Orlando, FL
  - $2,000 / ticket
  - Student Scholarship Program
  - Hosted by Vector35
  - 2024 talks online

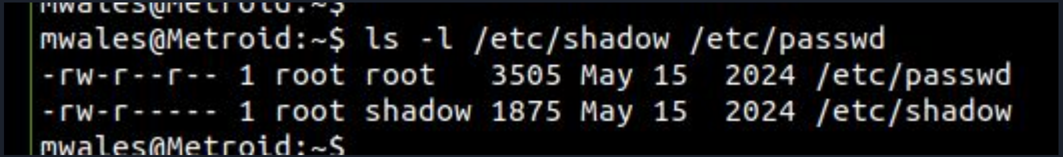


File Permissions

- Linux has file permissions for 3 different classes of user
    - User ~~Owner~~
    - Group
    - Other
- We can add execute permission:
    - For user: **`chmod u+x`**
    - For all: **`chmod a+x`**
- Remove write permission:
    - For others: **`chmod o-w`**



In practice

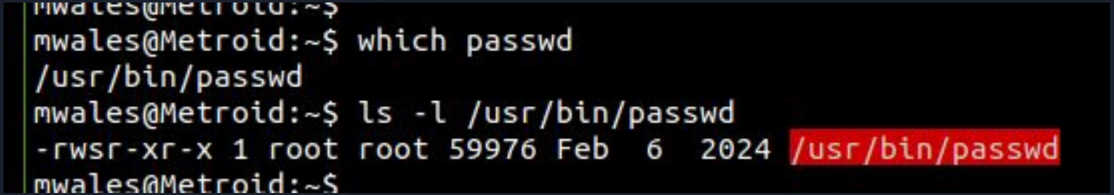


```
mwales@Metroid:~$
mwales@Metroid:~$ ls -l /etc/shadow /etc/passwd
-rw-r--r-- 1 root root   3505 May 15  2024 /etc/passwd
-rw-r----- 1 root shadow 1875 May 15  2024 /etc/shadow
mwales@Metroid:~$
```

- **`/etc/passwd`** has a list of users, and what groups they belong to
  - Any user on the system can see the contents of this file, but only root can write or change it
- **`/etc/shadow`** has password hashes
  - Only the root user or shadow group is allowed to read the file (you don’t want other users to see password hashes, they might try to crack them)
  - Only the root user can change the file

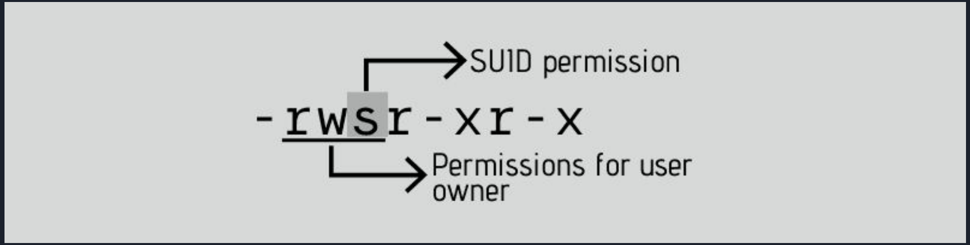
How does a user *change* their password then?

SUID bit

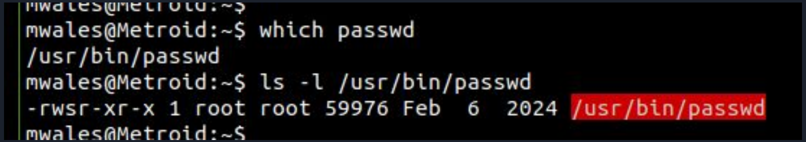


```
mwales@Metroid:~$
mwales@Metroid:~$ which passwd
/usr/bin/passwd
mwales@Metroid:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 59976 Feb  6  2024 /usr/bin/passwd
mwales@Metroid:~$
```

- This program can be read and executed by anyone on the system
  - Anyone can change their password
- Only root can change/write to the **`/usr/bin/passwd`** file itself
  - We don't want just anyone changing how the program works



SUIDs additional super power



```
mwales@Metroid:~$
mwales@Metroid:~$ which passwd
/usr/bin/passwd
mwales@Metroid:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 59976 Feb  6  2024 /usr/bin/passwd
mwales@Metroid:~$
```

- When SUID bit is set…
  - will be executed with the same permissions as the **owner** of the executable file
  - Turns the ‘x’ permission to ‘s’ for setuid
- What does this mean?
  - Anyone can execute the passwd program
  - This one file executes effectively as root
  - For the passwd program specifically
    - Can read the shadow file to get your old passwd hash
    - It asks you to verify you know the old password (compares to the hash in the file)
    - It asks you to create a new password
    - It then writes new passwd hash to shadow file (root is allowed even though your user isn’t)
- It is really important
  - For SUID programs to not have any bugs
  - Only programs that need SUID power to have it

Dangers of the SUID bit

- It is really important
  - For SUID programs to not have any bugs
  - Only programs that need SUID power to have it
  - Not let other users have write permission
- Pwn.college has 51 challenges at the end of the “Playing with Programs” dojo
  - Need to steal the **`/flag`** file
  - 51 different common programs with SUID bit set
    - What if **`cat`** is SUID?
    - What about **`vim`**?
    - What about **`date`**?
- Defenders should audit which programs have suid
  - **`find / -perm -u=s -type f 2>/dev/null`**

Playing With Programs

4 Modules

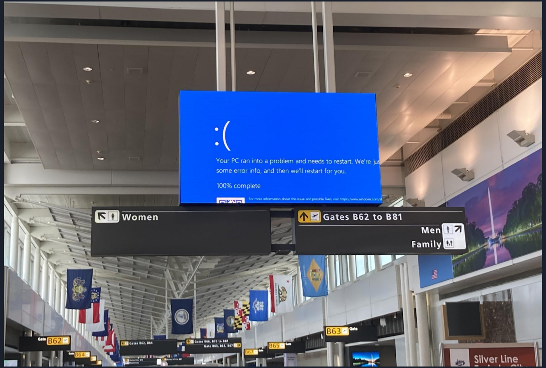
116 Challenges

Program Misuse

0 / 51

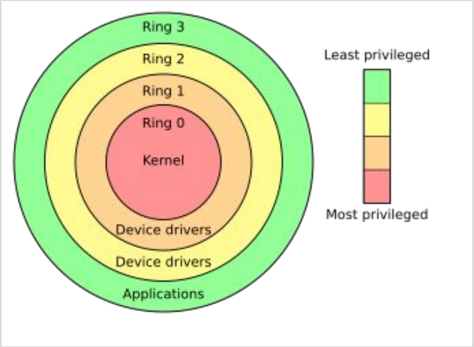
What about Windows?

- Principle of least privilege
  - Don’t run you desktop as admin (yeah, we used to do this ALL THE TIME)
- runas (very different permission model system)
  - runas for shell commands to have higher privilege (instead of sudo)
  - Right-click run as administrator
- Background services running as other users
  - XP and NT used to have IIS Web services running by default
    - Code Red worm.
  - Defenders should minimize services running (for any OS)
- Security token theft
- Malicious registry edits


:(
Your PC ran into a problem and needs to restart. We're ju
some error info, and then we'll restart for you.
100% complete
Women
Gates B62 to B81
Men
Family
B62
B63
Silver Line

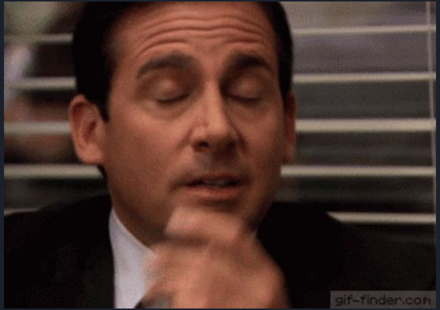
Privilege Escalation

- Abusing a SUID program can get us from a regular user to user level that is root
  - We *ELEVATED* from unprivileged user to privileged user
- Are their other privilege escalations?
  - Breaking an application… / jailbreaking
    - app user -> system user
    - Tony Hawk's Pro Strcpy Video
  - Local administrator -> Network administrator
    - Access more files / secrets / keys than just 1 PC
  - What other tiers / levels on regular system?



Impact of Genshin Impact

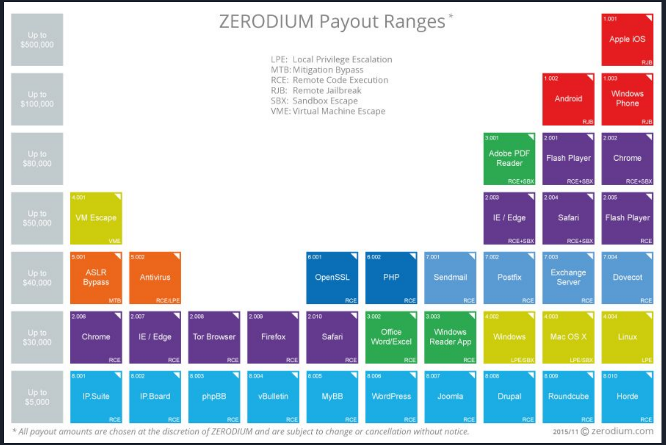
- State of Windows online gaming
  - Too many cheaters
  - Developers create anti-cheat guards / monitors
  - Runs with higher privilege to catch the cheat tools
- Genshin Impact Kernel level anti-cheat
  - Runs inside kernel / kernel level permissions
  - Has terrible bugs, kernel level privilege escalation
  - Is signed / white-listed by Microsoft to allow easy installation for game
    - But now is just brought with malware as easy way to elevate to kernel level
    - You don’t need to own this game to be affected



- Video Game Anti-Cheat plague
  - Shouldn’t be inside of kernel at all (largely non-existent on Linux systems)
  - Does it even work?
  - How will future attacks be prevented?

Other Escalations

- Application to system user / jailbreak
- User to root / admin
- (Browser) sandbox escape
- Linux capability settings (like SUID bit, but less well understood)
- From hypervisor guest into hypervisor host (tier 2 VM like VMWare)
- From hypervisor guest into hypervisor host (tier 1 ESXi / KVM / cloud systems)
- From kernel into bios
- From kernel to hardware management / BMC
- Altering firmware itself on hardware (hard drives, FPGAs)
- Supply chain



ZERODIUM Payout Ranges *

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape

Up to $500,000										1.001 Apple iOS RJB
Up to $100,000									1.002 Android RJB	1.003 Windows Phone RJB
Up to $80,000								3.001 Adobe PDF Reader RCE+SBX	2.001 Flash Player RCE+SBX	2.002 Chrome RCE+SBX
Up to $50,000	4.001 VM Escape VME							2.003 IE / Edge RCE+SBX	2.004 Safari RCE+SBX	2.005 Flash Player RCE
Up to $40,000	5.001 ASLR Bypass MTB	5.002 Antivirus RCE/LPE			6.001 OpenSSL RCE	6.002 PHP RCE	7.001 Sendmail RCE	7.002 Postfix RCE	7.003 Exchange Server RCE	7.004 Dovecot RCE
Up to $30,000	2.006 Chrome RCE	2.007 IE / Edge RCE	2.008 Tor Browser RCE	2.009 Firefox RCE	2.010 Safari RCE	3.002 Office Word/Excel RCE	3.003 Windows Reader App RCE	4.002 Windows LPE/SBX	4.003 Mac OS X LPE/SBX	4.004 Linux LPE
Up to $5,000	8.001 IP.Suite RCE	8.002 IP.Board RCE	8.003 phpBB RCE	8.004 vBulletin RCE	8.005 MyBB RCE	8.006 WordPress RCE	8.007 Joomla RCE	8.008 Drupal RCE	8.009 Roundcube RCE	8.010 Horde RCE

* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.

2015/11 © zerodium.com

Links

- https://linuxhandbook.com/suid-sgid-sticky-bit/
- https://www.youtube.com/watch?v=Pjqw1Gwk0jg
- https://securityaffairs.com/42136/hacking/zerodium-hacking-pricelist.html