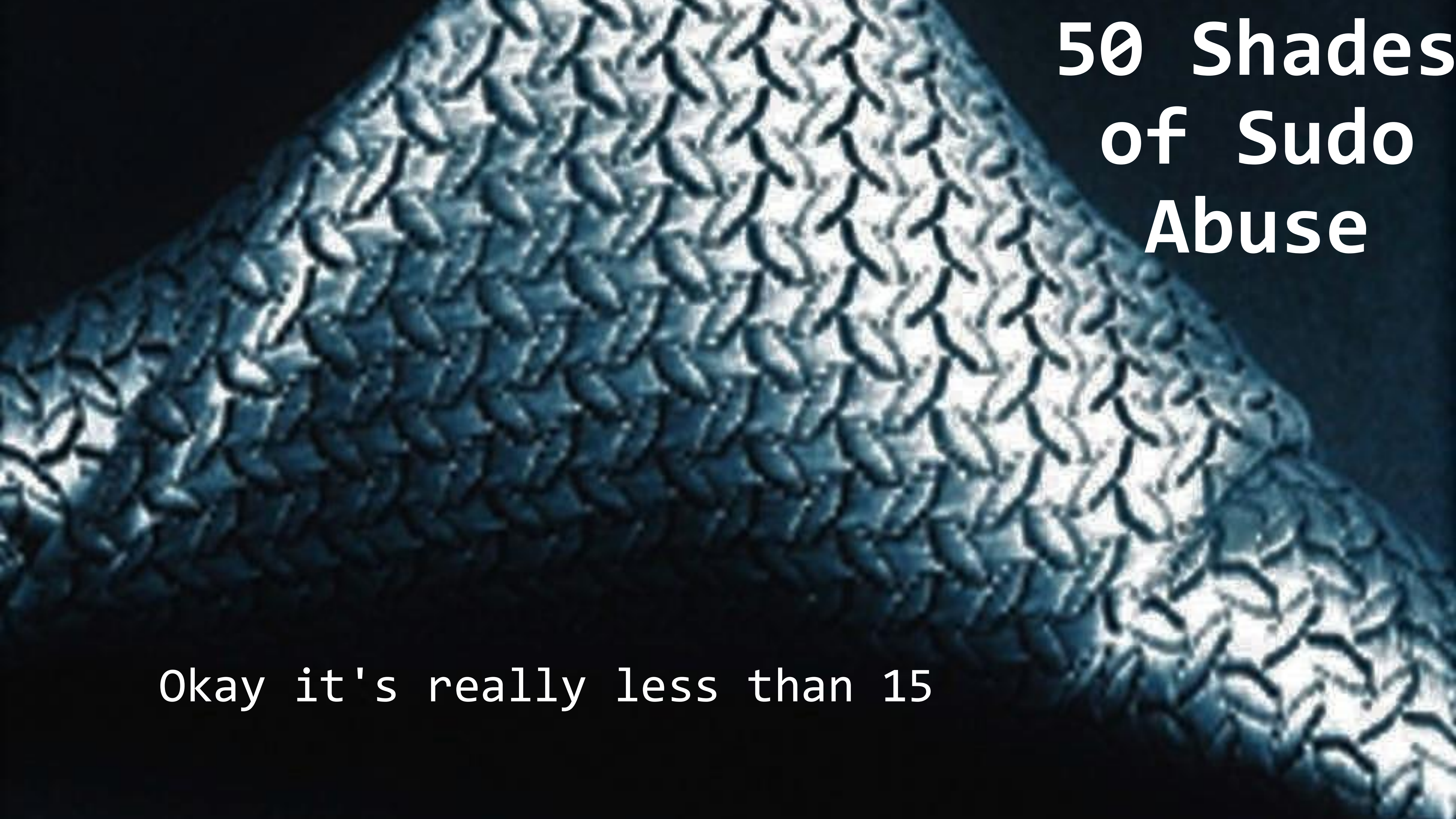
50 Shades of Sudo Abuse



Okay it's really less than 15

- TL;DR Obligatory about me section
- killchain info
- A very brief crash course on Sudo and Sudoers
- Example + Explanation
    - 1. Open Sudo
    - 2. Application Abuse (the easy stuff)
    - 3. Application Abuse pt2 (more subtle gotcha's)
    - 4. Abusing Pagers
    - 5. Abusing Cron
    - 6. LD_PRELOAD
    - 7. Installers (pip)
    - 8. Path in Sudoers (wildcards)
    - 9. Abusing editors (vim, nano, sudoedit)
    - 10. Application Abuse pt3 (leveraging bugs)
    - 11. CVE-2019-18634: Pwdfeedback
    - 12. Overcoming Limited Shells
    - 13. Misconfigured ***secure_path*** in sudoers
    - 14. CVE-2019-14287: security bypass

TL;DR About me

- Ag (class of 09)
- CommO (MOS: 0602)   MACS4 / 1MAW
- Network Engineer
- Security Engineer

@CaptBoykin

KILLCHAIN:~#

Sudo

The sudoers file, `/etc/sudoers`, describes which users can run which commands and from which terminals. This also describes which commands users can run as other users or groups. This provides the idea of least privilege such that users are running in their lowest possible permissions for most of the time and only elevate to other users or permissions as needed, typically by prompting for a password. However, the sudoers file can also specify when to not prompt users for passwords with a line like

```
    user1 ALL=(ALL) NOPASSWD: ALL
```

- Ref: https://attack.mitre.org/techniques/T1169/

Sudo

- ID: T1169
- Tactic: Privilege Escalation
- Platform: Linux, macOS
- Permissions Required: User
- Effective Permissions: root
- Data Sources: File monitoring
- Version: 1.0
- Created: 14 December 2017
- Last Modified: 18 July 2019

SUDO:~#

Crash course Sudo pt 1

- "**sudo** allows a permitted user to execute a *command* as the superuser or another user, as specified by the security policy."

- " The security policy determines what privileges, if any, a user has to run **sudo**. The policy may require that users authenticate themselves with a password or another authentication mechanism. If authentication is required, **sudo** will exit if the user's password is not entered within a configurable time limit. This limit is policy-specific; the default password prompt timeout for the *sudoers* security policy is 5 minutes."

- Ref: https://www.sudo.ws/man/1.8.13/sudo.man.html

Crash course Sudo pt 2

- "When **sudo** executes a command, the security policy specifies the execution environment for the command. Typically, the real and effective user and group and IDs are set to match those of the target user, as specified in the password database, and the group vector is initialized based on the group database (unless the **-P** option was specified)…"
- "...real and effective user ID, real and effective group ID, supplementary group IDs, the environment list, current working directory, file creation mode mask (umask), SELinux role and type, Solaris project, Solaris privileges, BSD login class, scheduling priority (aka nice value)"
- Ref: https://www.sudo.ws/man/1.8.13/sudo.man.html

Crash course Sudo pt3

- "There is no easy way to prevent a user from gaining a root shell if that user is allowed to run arbitrary commands via sudo. Also, many programs (such as editors) allow the user to run commands via shell escapes, thus avoiding sudo's checks. However, on most systems it is possible to prevent shell escapes with the sudoers(5) plugin's noexec functionality."

- Ref: https://www.sudo.ws/man/1.8.13/sudo.man.html

SUDOERS:~#

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/
instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/s
bin:/usr/bin:/sbin:/bin"


# Host alias specification


# User alias specification


# Cmnd alias specification
```

Super high level Sudoers pt1

- *The* primary configurable file by which sudo permissions are made
- Resides in /etc/sudoers by default
- It *can* be edited with whatever editor by root
- It *should* be edited using something more secure (ie *visudo*)
- It's picky on syntax, errors affects all users.
  - Best to make a copy, perform edits, and then use visudo for syntax checking
  - **`visudo -cf /var/tmp/sudoers.new`**

Super high level Sudoers pt2

- `Error in syntax`

```
>>> /etc/sudoers.myedits: syntax error near line 15 <<<
parse error in /etc/sudoers.myedits near line 15
```

- `OK`

```
/etc/sudoers.myedits: parsed OK
/etc/sudoers.d/README: parsed OK
```

Sudoers pt1

- "The *sudoers* security policy requires that most users authenticate themselves before they can use **sudo**. A password is not required if the invoking user is root, if the target user is the same as the invoking user, or if the policy has disabled authentication for the user or command. "
- "Unlike su(1), when *sudoers* requires authentication, it validates the invoking user's credentials, not the target user's (or root's) credentials. This can be changed via the *rootpw*, *targetpw* and *runaspw* flags, described later."

- Ref: https://www.sudo.ws/man/1.8.15/sudoers.man.html

Sudoers pt2

- "The sudoers file is composed of two types of entries: aliases (basically variables) and user specifications (which specify who may run what). "
- "When multiple entries match for a user, they are applied in order. Where there are multiple matches, the last match is used (which is not necessarily the most specific match)."

- Ref: https://www.sudo.ws/man/1.8.15/sudoers.man.html

Sudoers pt3

- "The *sudoers* grammar will be described below in Extended Backus-Naur Form (EBNF). Don't despair if you are unfamiliar with EBNF; it is fairly simple, and the definitions below are annotated."

- EBNF is a concise and exact way of describing the grammar of a language. Each EBNF definition is made up of production rules. E.g.,

```
symbol ::= definition | alternate1 | alternate2 ...
```

? Means that the preceding symbol (or group of symbols) is optional. That is, it may appear once or not at all.

***** Means that the preceding symbol (or group of symbols) may appear zero or more times.

+ Means that the preceding symbol (or group of symbols) may appear one or more times.

- Parentheses may be used to group symbols together. For clarity, we will use single quotes ('') to designate what is a verbatim character string (as opposed to a symbol name).

Ref: https://www.sudo.ws/man/1.8.15/sudoers.man.html

Sudoers pt4

Aliases: There are four kinds of aliases: User_Alias, Runas_Alias, Host_Alias and Cmnd_Alias.

```
Alias_Type NAME = item1, item2, item3 : NAME = item4, item5
```

- Defaults: Certain configuration options may be changed from their default values at run-time via one or more Default_Entry lines. These may affect all users on any host, all users on a specific host, a specific user, a specific command, or commands being run as a specific user.

- Ref: https://www.sudo.ws/man/1.8.15/sudoers.man.html

Sudoers pt5

- sudo allows shell-style wildcards (aka meta or glob characters) to be used in host names, path names and command line arguments in the sudoers file. Wildcard matching is done via the glob(3) and fnmatch(3) functions as specified by IEEE Std 1003.1 ("POSIX.1").

***** Matches any set of zero or more characters (including white space).

? Matches any single character (including white space).

[...] Matches any character in the specified range.

[!...] Matches any character not in the specified range.

\x For any character 'x', evaluates to 'x'. This is used to escape special characters such as: '*', '?', '[', and ']'.

- **Note that these are not regular expressions.**
- Unlike a regular expression there is no way to match one or more characters within a range.

- Ref: https://www.sudo.ws/man/1.8.15/sudoers.man.html

Sudoers pt6

- User specification: A user specification determines which commands a user may run (and as what user) on specified hosts. By default, commands are run as root, but this can be changed on a per-command basis. The basic structure of a user specification is

```
who where = (as_whom) what
```

- Runas_Spec: A Runas_Spec determines the user and/or the group that a command may be run as. A fully-specified Runas_Spec consists of two Runas_Lists (as defined above) separated by a colon (':') and enclosed in a set of parentheses. A Runas_Spec sets the default for the commands that follow it. What this means is that for the entry:

```
Dgb boulder = (operator) /bin/ls, /bin/kill, /usr/bin/lprm
```

- Ref: https://www.sudo.ws/man/1.8.15/sudoers.man.html

Sudoers pt7

- SELinux_Spec: On systems with SELinux support, sudoers entries may optionally have an SELinux role and/or type associated with a command. If a role or type is specified with the command it will override any default values specified in sudoers. A role or type specified on the command line, however, will supersede the values in sudoers.

- Tag_Spec: A command may have zero or more tags associated with it. There are ten possible tag values: EXEC, NOEXEC, FOLLOW, NOFOLLOW, LOG_INPUT, NOLOG_INPUT, LOG_OUTPUT, NOLOG_OUTPUT, MAIL, NOMAIL, PASSWD, NOPASSWD, SETENV, and NOSETENV. Once a tag is set on a Cmnd, subsequent Cmnds in the Cmnd_Spec_List, inherit the tag unless it is overridden by the opposite tag (in other words, PASSWD overrides NOPASSWD and NOEXEC overrides EXEC).
  - NOPASSWD often used

- Ref: https://www.sudo.ws/man/1.8.15/sudoers.man.html

DEMO@EXAMPLES:~#

Though process…

- "How can I do something not permitted?"
- "How can I read something off limits?"
- "How can I write something off limits?"
- "Are there any features that are often overlooked?"
- "Can I escalate laterally?"
- "Can I escalate vertically?"

1. Open Sudo

- "Wide open". Default for root. Can run anything on the system as root as long as they can authenticate (even worse if NOPASSWD is used)

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
section1_opensudo ALL=(ALL:ALL) ALL
```

DEMO

2. Application Abuse pt1 (the easy stuff)

- Anything that directly spawns shells, (sh, ksh, zsh, dash, bash, etc)
- Any programming language (python, ruby, php, perl, java, etc etc)

```
# User privilege specification
Section2_apps ALL=(root) /bin/su
section2_apps ALL=(root) /bin/sh
section2_apps ALL=(root) /usr/bin/python
section2_apps ALL=(root) /usr/bin/ruby
```

DEMO

3. Application Abuse pt2 (slightly more hacky)

- Anything with features that were intended for a benevolent purpose but can be twisted
- Anything with features that function as intended but have side effects that can benefit the attacker

```
# User privilege specification
section3_apps2 ALL=(root) /usr/bin/wget
section3_apps2 ALL=(root) /usr/bin/base64
section3_apps2 ALL=(root) /usr/bin/tree
section3_apps2 ALL=(root) /usr/bin/gcc
```

3. Application Abuse pt2 (slightly more hacky)

```
/usr/bin/wget
```

```
/usr/bin/base64
```

```
/usr/bin/tree
```

```
/usr/bin/gcc
```

-wrapper
  Invoke all subcommands under a wrapper program.
  The name of the wrapper program and its parameters
  are passed as a comma separated list.

DEMO

4. Abusing Pagers

- "A terminal pager, or paging program, is a computer program used to view (but not modify) the contents of a text file moving down the file one line or one screen at a time. Some, but not all, pagers allow movement up a file. A popular cross-platform terminal pager is more. More can move forwards and backwards in text files but cannot move backwards in pipes.[1] less is a more advanced pager that allows movement forward and backward, and contains extra functions such as search.[2]"
  - **Examples: more, less, man, systemctl, service**

```
# User privilege specification
section4_pagers ALL=(root) /usr/bin/man
section4_pagers ALL=(root) /usr/sbin/service
```

Ref: https://en.wikipedia.org/wiki/Terminal_pager

DEMO

5. Abusing Cron

- Services that run as root are an avenue of approach for someone looking to escalate
- If the user can manipulate the service itself

```
# User privilege specification
section5_cron ALL=(root) /usr/sbin/service cron *
section5_cron ALL=(root) /usr/bin/crontab
```

DEMO

6. LD_PRELOAD (probably my favorite) pt1

- "The LD_PRELOAD trick exploits functionality provided by the dynamic linker on Unix systems that allows you to tell the linker to bind symbols provided by a certain shared library *before other libraries*. For this, remember that upon program execution, the operating system's ***dynamic loader*** will first load dynamic libraries you link to into the process's memory (address space), such that the *dynamic linker* can then resolve symbols at load or run time and bind them to actual definitions."

    - **http://www.goldsborough.me/c/low-level/kernel/2016/08/29/16-48-53-the_-ld_preload-_trick/**

6. LD_PRELOAD (probably my favorite) pt2

- TL;DR or still unfamiliar with dynamic linking
  - Methods and functions that are called by the binary can be overwritten with **custom functionality.**
  - Obviously "custom functionality" and "sudo" are a "**fun**" mix
- Sudoers file require a particular default in place for this to be utilized.
  - `Defaults:section6_ldpreload      env_keep+=LD_PRELOAD`
- Syntax for the above
  - *`Sudo LD_PRELOAD=/path/to/my/shared_obj <binary>`*
  -

DEMO

7. Abusing Installers (pip, etc)

- Installers can also be manipulated to run extra commands or install attacker-controlled software
- A python setup script allows for additional setup steps to be taken = prime code execution

```
# User privilege specification
section7_installers ALL=(root) /usr/bin/pip
```

Ref: **https://root4loot.com/post/pip-install-privilege-escalation/**

DEMO

* Rev Shell

Pronouncing it as "Sudo"
Pronouncing it as "Sudo"

8. Misconfigured executable path in Sudoers (wildcards) pt1

- Recall the section on wildcards...

<u>*</u> Matches any set of zero or more characters (including white space).

<u>?</u> Matches any single character (including white space).

<u>[...]</u> Matches any character in the specified range.

<u>[!...]</u> Matches any character not in the specified range.

<u>\x</u> For any character ‘x’, evaluates to ‘x’. This is used to escape special characters such as: ‘*’, ‘?’, ‘[’, and ‘]’.

8. Misconfigured executable path in Sudoers (wildcards) pt2

```
# User privilege specification
section8_path ALL=(root) /bin/*
```

DEMO

9. Abusing editors(vim, nano, sudoedit) pt1

- An obvious avenue for exploitation, could result in sensitive file read/write and up to elevated shells.
- Piggybacking off the editor

```
# User privilege specification
section9_editors ALL=(ALL:ALL) /usr/bin/vim
section9_editors ALL=(ALL:ALL) /usr/bin/nano
```

-

Ref: https://root4loot.com/post/pip-install-privilege-escalation/

9. Abusing editors(vim, nano, sudoedit) pt2

- Sudo 1.8.14 (RHEL 5/6/7 / Ubuntu) - 'Sudoedit' Unauthorized Privilege Escalation

"It seems that sudoedit does not check the full path if a wildcard is used twice (e.g. /home/*/*/file.txt), allowing a malicious user to replace the file.txt real file with a symbolic link to a different location (e.g. /etc/shadow)"

```
# User privilege specification
section9_editors
ALL=(ALL:ALL) /home/section9_editors/bin/sudoedit /h
ome/section9_editors/*/*/protected.txt
```

Ref: https://www.exploit-db.com/exploits/37710

DEMO

10. Application Abuse pt 3 (leveraging bugs)

- Applications with bugs running sudo can be leveraged.

```
# User privilege specification
section10_apps3 ALL=(root)
/home/section10_apps3/mycat
```

- In the example above, a command injection vulnerable can be leveraged to run arbitrary commands (in addition to other avenues)

DEMO

11. CVE-2019-18634: Pwdfeedback

" In Sudo before 1.8.26, if pwfeedback is enabled in /etc/sudoers, users can trigger a stack-based buffer overflow in the privileged sudo process. (pwfeedback is a default setting in Linux Mint and elementary OS; however, it is NOT the default for upstream and many other packages, and would exist only if enabled by an administrator.) The attacker needs to deliver a long string to the stdin of getln() in tgetpass.c."

TL;DR: A pretty simple buffer overflow with ascii commands at the end :)

```
# User privilege specification
section11_pwfeedback ALL=(ALL:ALL) ALL
```

Ref: https://nvd.nist.gov/vuln/detail/CVE-2019-18634

DEMO

* **Rev Shell**

12. Overcoming Limited Shells pt1

- In some instances, the attacker/tester has a limited shell and for whatever reason cannot elevate to a full TTY.
- If any kind of password can be provided, *expect* can be leveraged to run commands as a sudo/su user.

- In this demo, a limited shell complicates leveraging an open sudo as authenticating requires a TTY. Expect provides another option.

```
expect -c 'spawn sudo -S cat "/root/root.txt";expect
"*password*";send "section12_limited_shell";send
"\r\n";interact'
```

Ref: https://likegeeks.com/expect-command/

12. Overcoming Limited Shells pt2

"Commands are listed alphabetically so that they can be quickly located. However, new users may find it easier to start by reading the descriptions of **spawn**, **send**, **expect**, and **interact**, in that order."

"The spawn command is used to start a script or a program like the shell, **FTP**, Telnet, SSH, SCP, and so on.

The send command is used to send a reply to a script or a program.

The Expect command waits for input.

The interact command allows you to define a predefined user interaction"

Ref: https://likegeeks.com/expect-command/

Ref: https://linux.die.net/man/1/expect

12. Overcoming Limited Shells pt3

```
expect -c 'spawn sudo -S cat "/root/root.txt";expect
"*password*";send "section12_limited_shell";send
"\r\n";interact'
```

- `expect –c`
  - A command to be executed before any in the script...
- `spawn sudo -S cat "/root/root.txt";`
  - 'Spawn' sudo and supply the command "cat...."
- `expect "*password*";`
  - 'Expect' many permuations of password...
- `send "section12_limited_shell";`
  - 'Send' the supplied password to STDOUT...
- `send "\r\n";`
  - 'Send' \r\n (enter)...
- `Interact`
  - 'Interact' thereby outputting what expect see's from the terminal

DEMO

* Rev Shell

13. Misconfigured ***secure_path*** in sudoers

"secure_path: Path used for every command run from sudo. If you don't trust the people running sudo to have a sane PATH environment variable you may want to use this. Another use is if you want to have the “root path” be separate from the “user path”. Users in the group specified by the exempt_group option are not affected by secure_path. This option is not set by default. "

- If the secure_path is set and misconfigured == potential for fun :)

```
Defaults:section13_path2
secure_path=/tmp:/usr/local/sbin:/usr/local/bin:/usr
/sbin:/usr/bin:/sbin:/bin
```

DEMO

14. CVE-2019-14287: security bypass

"Description :Sudo doesn't check for the existence of the specified user id and executes the with arbitrary user id with the sudo priv -u#-1 returns as 0 which is root's id and /bin/bash is executed with root permission"

```
# User privilege specification
section14_2019-14287 ALL=(ALL,!root) /bin/sh
```

DEMO

Recap

- A very brief crash course on Sudo and Sudoers
  - Sudo
  - Sudoers File
- Example + Explanation
  - 1. Open Sudo
  - 2. Application Abuse (the easy stuff)
  - 3. Application Abuse pt2 (more subtle gotcha's)
  - 4. Abusing Pagers
  - 5. Abusing Cron
  - 6. LD_PRELOAD
  - 7. Abusing Installers (pip)
  - 8. Misconfigured executable path in Sudoers (wildcards)
  - 9. Editors (vim, nano, sudoedit)
  - 10. Application Abuse pt3 (leveraging bugs)
  - 11. CVE-2019-18634: Pwdfeedback
  - 12. Overcoming Limited Shells
  - 13. Misconfigured ***secure_path*** in sudoers
  - 14. CVE-2019-14287: security bypass

References, Links, Goodies

- Sudo 1.8.14 (RHEL 5/6/7 / Ubuntu) - 'Sudoedit' Unauthorized Privilege Escalation
  - https://www.exploit-db.com/exploits/37710
- Sudo 1.8.25p - 'pwfeedback' Buffer Overflow (PoC)
  - https://www.exploit-db.com/exploits/47995
- Sudo Manual
  - https://www.sudo.ws/man/1.8.15/sudoers.man.html
- Sudo Manual – Sudoers File
  - https://www.sudo.ws/man/1.8.15/sudoers.man.html
- GTFO Bins
  - https://gtfobins.github.io/
- Python Pip Priv Esc via Sudo
  - https://root4loot.com/post/pip-install-privilege-escalation/

- Sudo (LD_PRELOAD) (Linux Privilege Escalation)
  - https://touhidshaikh.com/blog/2018/04/sudo-ld_preload-linux-privilege-escalation/
- sudo 1.8.27 - Security Bypass
  - https://www.exploit-db.com/exploits/47502
- Abusing SUDO
  - https://recipeforroot.com/abusing-sudo/
- Terminal Pager
  - https://en.wikipedia.org/wiki/Terminal_pager
- Expect Command
  - https://likegeeks.com/expect-command/
  - https://linux.die.net/man/1/expect
- GCC –wrapper
  - https://stackoverflow.com/questions/14039669/what-does-gccs-wrapper-flag-do