# Special Modes

# Setuid

- When a process is started, it runs using the starting user's UID and GID.
- setuid = **S**et **U**ser **ID** upon execution.
- `-rwsr-xr-x 1 root root /usr/bin/passwd`
- `ping`
- `chsh`
- setuid files are an attack surface.
- Not honored on shell scripts.

# Octal Permissions

| setuid | setgid | sticky | |
|---|---|---|---|
| 0 | 0 | 0 | Value for off |
| 1 | 1 | 1 | Binary value for on |
| 4 | 2 | 1 | Base 10 value for on |

# Adding the Setuid Attribute

```
chmod u+s /path/to/file
```

```
chmod 4755 /path/to/file
```

# Removing the Setuid Attribute

```
chmod u-s /path/to/file
```

```
chmod 0755 /path/to/file
```

# Finding Setuid Files

```
find / -perm /4000

# Older style:
find / -perm +4000
```

# Finding Setuid Files

```
find / -perm /4000 -ls

# Older style:
find / -perm +4000 -ls
```

# Only the Owner Should Edit Setuid Files

| | Symbolic | Octal |
|---|---|---|
| Good: | `-rwsr-xr-x` | `4755` |
| Bad: | `-rwsrwxr-x` | `4775` |
| Really bad: | `-rwsrwxrwx` | `4777` |

# Setgid

- setgid = **S**et **G**roup **ID** upon execution.
- `-rwxr-sr-x 1 root tty /usr/bin/wall`
- `crw--w---- 1 bob  tty /dev/pts/0`

# Finding Setgid Files

```
find / -perm /2000 -ls

# Older style:
find / -perm +2000 -ls
```

# Adding the Setgid Attribute

```
chmod g+s /path/to/file
```

```
chmod 2755 /path/to/file
```

# Adding the Setuid & Setgid Attributes

```
chmod ug+s /path/to/file

chmod 6755 /path/to/file
```

# Removing the Setgid Attribute

```
chmod g-s /path/to/file
```

```
chmod 0755 /path/to/file
```

# Setgid on Directories

- setgid on a directory causes new files to inherit the group of the directory.
- setgid causes directories to inherit the setgid bit.
- Is not retroactive.
- Great for working with groups.

# Use an Integrity Checker

- Other options to `find`.
- Tripwire
- AIDE (Advanced Intrusion Detection Environment)
- OSSEC
- Samhain
- Package managers

# The Sticky Bit

- Use on a directory to only allow the owner of the file/directory to delete it.
- Used on /tmp:

```
drwxrwxrwt 10 root root 4096 Feb 1 09:47 /tmp
```

# Adding the Sticky Bit

```
chmod o+s /path/to/directory
```

```
chmod 1777 /path/to/directory
```

# Removing the Sticky Bit

```
chmod o-t /path/to/directory
```

```
chmod 0777 /path/to/directory
```

# Reading `ls` Output

- A capitalized special permission means the underlying normal permission is not set.
- A lowercase special permission means the underlying normal permission set.

# Reading `ls` Output

```
$ ls -l test
-rw-r--r-- 1 root root 0 Feb 14 11:21 test
$ chmod u+s test
$ ls -l test
-rwSr--r-- 1 root root 0 Feb 14 11:21 test
$ chmod u+x test
$ ls -l test
-rwsr--r-- 1 root root 0 Feb 14 11:21 test
```

# Reading `ls` Output

```
$ ls -l test
-rw-r--r-- 1 root root 0 Feb 14 11:21 test
$ chmod u+s test
$ ls -l test
-rwSr--r-- 1 root root 0 Feb 14 11:21 test
$ chmod u+x test
$ ls -l test
-rwsr--r-- 1 root root 0 Feb 14 11:21 test
```

# Reading `ls` Output

```
$ ls -l test
-rw-r--r-- 1 root root 0 Feb 14 11:21 test
$ chmod u+s test
$ ls -l test
-rwSr--r-- 1 root root 0 Feb 14 11:21 test
$ chmod u+x test
$ ls -l test
-rwsr--r-- 1 root root 0 Feb 14 11:21 test
```

# Reading `ls` Output

```
-rwxrwSr-- 1 root root 0 Feb 14 11:21 test

drwxr-xr-T 2 root root 0 Feb 14 11:30 testd
```