FANSHAWE

INFO-6076

Web Security

Automation

FANSHAWE

Agenda

- Scripts
- Clam Anti-Virus
- SendMail
- Automation
- Lab 10 Overview

FANSHAWE

Scripts

FANSHAWE

Scripts

Systems can be automated using scripts

Scripts are written to be run in a particular environment

A shell will act as an interpreter

Linux: Bash, korn, etc.

Windows: cmd.exe, batch files, powershell, etc.

FANSHAWE

Shell Scripts

Unix-like operating systems can use different shells

The Bourne-Again shell or Bash is a free program that is used by most Linux distributions

#!/bin/bash

Specifies the bash shell

FANSHAWE

Shell Scripts

Bash scripts can be executed in sequence or conditionally, based on the desired functionality

Shell scripts can help you improve the efficiency of your system administration tasks

- Backups
- System updates
- Scans

FANSHAWE

Shell Scripts

Bash scripts will need to have the appropriate permissions to be executed

Execute permissions must be granted to the user invoking the script

During lab, change the permissions to 755

```
chmod 755 name_of_script.sh
```

FANSHAWE

Shell Scripts

Permissions are divided as follows:

R = 4 W = 2 X = 1

There are 3 sets of these (rwx)

1) Owner
2) Group
3) Other

```
root@artmack-uws:/etc/cron.hourly# ls -ail
total 16
1572888 drwxr-xr-x   2 root root 4096 Mar 27 10:27 .
1572865 drwxr-xr-x 100 root root 4096 Mar 27 09:23 ..
1578903 -rwxr-xr-x   1 root root 1690 Mar 27 10:27 auto_clam_scan
1573973 -rw-r--r--   1 root root  102 Nov 16  2017 .placeholder
```

FANSHAWE

Script permissions

auto_clam_scan has permissions of:

RWX R-X R-X *which is* 755

.**placeholder** has permissions of 644

```
root@artmack-uws:/etc/cron.hourly# ls -ail
total 16
1572888 drwxr-xr-x   2 root root 4096 Mar 27 10:27 .
1572865 drwxr-xr-x 100 root root 4096 Mar 27 09:23 ..
1578903 -rwxr-xr-x   1 root root 1690 Mar 27 10:27 auto_clam_scan
1573973 -rw-r--r--   1 root root  102 Nov 16  2017 .placeholder
```

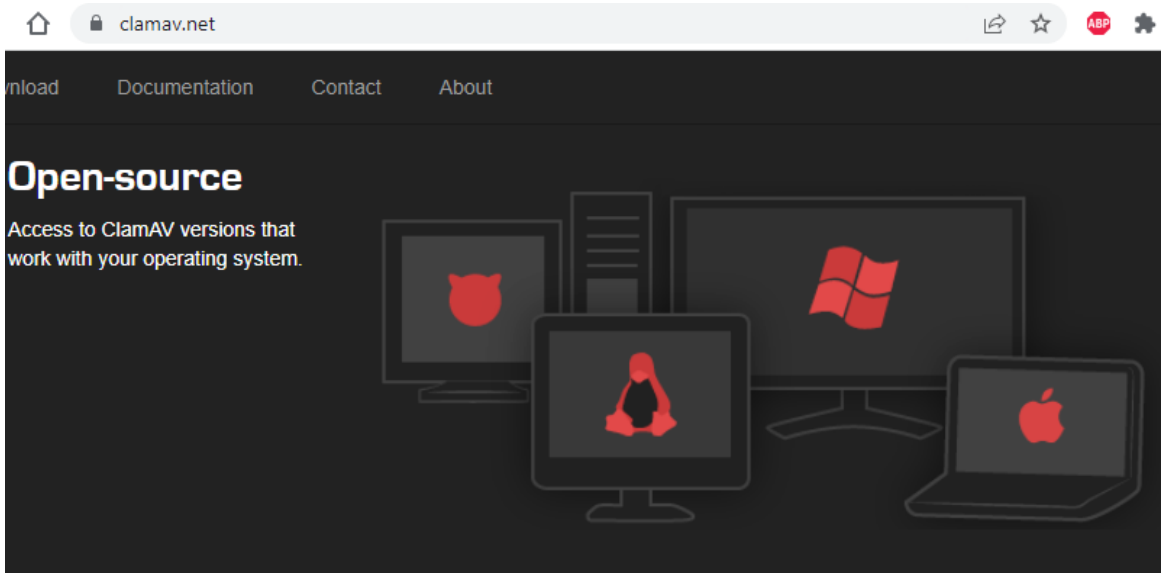
FANSHAWE

Clam Anti-Virus

Clam Anti-Virus

Clam Anti-Virus is an open source cross-platform software that can be used with the following Operating Systems:

- BSD
- Linux
- macOS
- Windows
- Etc.



FANSHAWE

Clam Anti-Virus

- Clam development is currently under the Cisco umbrella
- Originally developed by independent developers, it was then purchased by Sourcefire and added to their Vulnerability Research Team
- Cisco acquired Sourcefire and added the Clam VRT team to Cisco Talos

FANSHAWE

Clam Anti-Virus

When installing ClamAV on Ubuntu, there are a few components to keep in mind:

- clamav
- clamav-daemon
- clamav-freshclam

- FreshClam will update the signature database for viruses and malware

FANSHAWE

Clam Anti-Virus

ClamAV is good at targeting emails

It can be used to detect phishing scams, as well as scanning documents being transmitted by email

- HTML
- Rich Text Format (RTF)
- Portable Document Format (PDF)
- MS Office documents

FANSHAWE

Clam Anti-Virus

ClamAV can be customized to scan specific directories in the file system

This will scan everything in the /home directory

```
clamscan –ri /home
```

FANSHAWE

Clam Anti-Virus

You can use the remove option, but be careful since it can automatically remove any files that are detected as malicious…

clamscan –ri --remove /home

FANSHAWE

Clam Anti-Virus

If you want to scan all directories except for a few that you specify, you can use the **exclude** option to accomplish this

clamscan –ri --exclude-dir=^/sys\|^/proc\|^/dev /

This will exclude the /sys /proc and /dev directories

FANSHAWE

Send Mail

FANSHAWE

Send Mail

Send mail is a free and open source utility that allows your server to send SMTP messages

- Originally came out in 1986 and has improved since (mainly with security features)
- Cross platform and customizable
- We will use it on our Ubuntu Web Server

FANSHAWE

Send Mail

Send mail can be run in a shell making it useful for automating tasks that require email notifications

- Any task that can be executed from the Shell, can be incorporated into a script
- Scripts can be added to cron jobs (The equivalent of a task scheduled in Windows)

FANSHAWE

Send Mail

- In your lab you will use SendMail to send SMTP messages using Gmail as a relay
- This will involve you having to properly configure the /etc/mail/sendmail.mc configuration file
- Instructions for this will be included in the lab

FANSHAWE

Send Mail

- It is important to note that security settings may have to be lowered in Gmail in order for the relay to work properly
- You may want to use a new Gmail account other than your day to day (if you already have one)
- There are other methods of relaying the emails but our lab will use Gmail

FANSHAWE

Send Mail

- If you are using Windows or XAMPP for your testing, you will have to adjust the php.ini file to reflect the SMTP settings

FANSHAWE

Automation

FANSHAWE

Automation

- We will introduce simple automation for scanning our web server for malware/viruses and then logging the results
- This will be complimented with a script that runs on an hourly basis
  - Uses ClamAV to scan specified directories
  - Logs the results
  - Emails alerts based on configuration

FANSHAWE

Automation

- ClamAV has the capability to erase/delete any threats found on the system or simply log them
- You can adjust the scan script to do either
- Your script will include the option to have **Aggressive** set to 1 or 0

FANSHAWE

Automation

In a production environment, you may want to be careful when automatically attempting to remove files

- Could be legitimate files
- Might be used for testing by developers

Aggressive set to **1** will attempt to remove any files considered to be a threat

Aggressive set to **0** will not remove any files

Lab Details

LAB-10: Overview

FANSHAWE

Lab-10: Anti-Virus Automation

- Install Clam Anti-Virus
- Install and configure Send Mail
- Create a script to scan the web server
- Automate the AV scan and email alert with a cron job