2017-18 Round 1 (Ubuntu 14)

Vulns - 21/21 - 100/100 Points
Forensic Question 1 correct - 8pts
Forensic Question 2 correct - 8pts
Removed unauthorized user fawful - 4pts
Removed unauthorized user petey - 4pts
Removed unauthorized user koji - 4pts
User lemmy is not an administrator - 4pts
Changed user account pakkun - 4pts
Changed insecure root password - 4pts
Guest account is disabled - 4pts
Firewall protection has been enabled - 5pts
FTP Service has been disabled or removed - 4pts
The system automatically checks for updates - 4pts
Install updates from important security updates - 4pts
The Linux Kernel has been updated - 5 pts
OpenSSH has been updated - 4pts
Firefox has been updated - 5pts
LibreOffice has been updated - 5pts
Prohibited MP3 files are removed - 4pts
Prohibited software john the ripper removed - 6pts
Prohibited software hydra-gtk removed - 5pts
SSH root login has been disabled - 5pts

2017-18 Round 2 (Ubuntu 14)

Vulns - 36/36 - 100 Points
Forensic Question 1 correct - 5pts
Forensic Question 2 correct - 5pts
Forensic Question 3 correct - 5pts
Removed unauthorized user scotty - 2pts
Removed unauthorized user chekov - 2pts
User pauline is not an Administrator - 2pts
Changed insecure password for User OR Changed max pass age for User - 3pts
Created user account penguru - 2pts
User penguru is an Administrator - 2pts
Created user group pipefitters - 2pts
Users added to group pipefitters - 2pts
A default maximum password age is set - 3pts
A minimum password length is required - 4pts
Insecure sudo configuration fixed - 3 pts
IPv4 TCP SYN cookies have been enabled - 3 pts
IPv4 forwarding has been disabled - 3 pts
Firewall protection has been enabled - 2pts
Postgresql has been disabled or removed - 3pts
Apache2 service has been disabled or removed - 4pts
Linux Kernel has been updated - 2pts
Sudo has been updated - 2pts
Vsftpd has been updated - 2 pts
Firefox has been updated - 2pts
Prohibited MP3 files are removed - 2pts
Stellarium has been installed - 3pts
Prohibited software hydra removed - 2 pts
Prohibited software aircrack-ng removed - 2pts
Prohibited software Freeciv removed - 2pts
Removed netcat backdoor - 4pts
Firefox displays warning on known malware sites - 2pts
SSH Protocol 1 has been disabled - 3pts
FTP local users must log in as anonymous - 3 pts (anonymous_enable=YES/NO & local_enable=NO)
FTP anonymous write commands are disabled - 3pts (A| anon_mkdir_write_enable=NO & anon_other_write_enable=NO & write_enable=NO)
FTP PASV security checks enabled - 3 pts (A| pasv_enable=YES)
FTP anonymous user is not root - 3pts (A| guest_username=ftp & ftp_username=ftp & chown_username=FTP & nopriv_user=FTP)
Insecure permissions on FTP root directory fixed - 3pts (A| sudo chmod 640 CHROOT_DIR)

2017-18 State Round (Ubuntu 16)

Vulns - 44/44 - 100/100 Points
Forensics Question 1 correct - 5 pts
Forensics Question 2 correct - 5 pts
Forensics Question 3 correct - 5 pts
Forensics Question 4 correct - 5 pts
Removed unauthorized user bwayne - 1 pts
Removed unauthorized user brainiac - 1 pts
Removed unauthorized user lluthor - 1 pts
User wwest is not an administrator - 1 pts
User savitar is not an administrator - 1 pts
Changed insecure password for user jwells - 1 pts
Changed max password age for user - 1 pts
Previous passwords are remembered - 3 pts
Null passwords do not authenticate on insecure consoles - 3 pts
A default minimum password age is set - 2 pts
Syncookies is enabled - 2 pts
Ignore broadcast ICMP echo requests enabled - 2 pts
IPv4 TCP SYNACK retires reduced - 2 pts
Sudo requires authentication - 2 pts
Uncomplicated Firewall (UFW) protection has been enabled - 3 pts
Insecure permissions on shadow file fixed -2 pts
OpenSSH service has been installed and started - 3 pts
IRC daemon has been stopped and disabled - 2 pts
DNS service is disabled or removed - 2 pts
OpenArena service has been disabled or removed - 2 pts
Remote Desktop Sharing has been disabled - 2 pts
The system automatically checks for updates daily - 2 pts
Linux kernel has been updated - 2 pts
Bash has been updated - 2 pts
Firefox has been updated - 2 pts
OpenSSH has been updated - 2 pts
Samba has been updated - 2 pts
Prohibited MP3 files are removed - 2 pts
Prohibited software ophcrack removed - 2 pts
Prohibited software medusa removed - 2 pts
Prohibited software Minetest removed - 2 pts
Removed netcat backdoor - 3 pts
SSH listens on port 222 - 3 pts
SSH allows only public key authentication - 3 pts
SSH does not permit empty passwords - 2 pts
SSH root login has been disabled - 2 pts

Anonymous Samba access is disabled - 2 pts (restrict anonymous = 2 & guest ok = no)
Unauthorized Samba share is disabled - 2 pts (Delete all extra shares like [printer share])
Samba blank passwords are disabled - 2 pts (lanman auth = no & client lanman auth = no & ntlm auth = ntlmv2-only & client NTLMv2 auth = yes)
Samba SMB1 protocol is disabled - 2 pts (in global: min protocol = SMB2 &/OR protocol = SMB2)

2017-18 Semifinals Round (Ubuntu 16)

Vulns - 40/52 - 76/100 Points
Forensics Question 1 - 4 pts
Forensics Question 2 - 4 pts
Forensics Question 3 - 4 pts
Forensics Question 4 - 4 pts
Unauthorized user odestruct - 1 pts
Unauthorized user strange - 1 pts
User qwark is not an administrator - 1 pts
Changed insecure password for user orvus - 1 pts
User grazz can not login without a password - 1 pts
Root password is no longer blank - 1 pts
Password for clank is hashed with a secure algorithm - 1 pts
Extra dictionary based password strength checks - 2 pts
A secure password hashing algorithm is used - 2 pts
Null passwords do not authenticate - 2 pts
An account lockout policy is configured - 2 pts
A default maximum password age is set - 2 pts
Insecure sudo configuration fixed - 2 pts
IPv4 forwarding has been disabled - 2 pts
Restrict unprivileged access to kernel syslog - 2 pts
Firewall protection has been enabled - 2 pts
GRUB configuration is not world readable - 2 pts
Resolver checks for IP spoofing - 2 pts
SNMP service has been disabled/removed - 2 pts
Samba service has been disabled/removed - 2 pts
Rsync service has been disabled/removed 2 pts
Automatic daily updates - 1 pts
Glibc has been updated - 1 pts
Apache has been updated - 1 pts
PHP has been updated - 1 pts
Removed plaintext file containing passwords - 2 pts
Removed phpinfo() php file - 2 pts
SSH root login has been disabled - 1 pts
SSH user environment processing is disabled - 2 pts
Firefox displays warnings on known malware sites - 2 pts
Prohibited software ëknockerí removed - 2 pts
MySQL remote access is disabled - 2 pts
PHP expose is Off - 2 pts
PHP system function is disabled - 2 pts
Apache server signature is disabled - 2 pts
Apache trace requests disabled - 2 pts

2018-19 Practice Round (Ubuntu 16)
Vulns - 11/11 - 100/100

Forensics 1 Correct - 14
Forensics 2 Correct - 14
Removed unauthorized user rsharpe - 8
User grodd is not an administrator - 8
Changed insecure password for user jwells - 8
Firewall protection has been enabled - 8
FTP service has been disabled or removed - 8
System automatically checks for updates daily - 8
Install updates from important security updates - 8
Prohibited mp3 media files have been removed - 8
Prohibited software Nmap and Zenmap have been removed - 8

2018-19 Round 1 (Ubuntu 16)

Vuln - 22/22 - 100/100
Forensics Question 1 correct - 8 pts
Forensics Question 2 correct - 8 pts
Created user account zachary - 4 pts
Guest account is disabled - 4 pts
Removed unauthorized user vladimir - 4 pts
Removed unauthorized user pedro - 4 pts
User samantha is not an administrator - 4 pts
User ivan is not an administrator - 4 pts
Changed insecure password for user conrad - 4 pts
A default maximum password age is set - 3 pts
Firewall protection has been enabled - 5 pts
Apache2 service has been disabled or removed - 4 pts
The system automatically checks for updates daily - 4 pts
Bash has been updated - 4 pts
Firefox has been updated - 4 pts
LibreOffice has been updated - 4 pts
OpenSSH has been updated - 4 pts
Prohibited MP3 files are removed - 5 pts
Prohibited software Kismet removed - 5 pts
Prohibited software ophcrack removed - 5 pts
Prohibited software Freeciv removed - 5 pts
SSH root login has been disabled - 4 pts

2018-19 Round 2 (Ubuntu 16)

Vulns - 30/30 - 100/100
Forensics Question 1 correct - 7 pts
Forensics Question 2 correct - 7 pts
Created user account zachary - 3 pts
Guest account is disabled - 2 pts
Removed unauthorized user himiko - 2 pts
Removed ftp user - 2 pts
User samantha is not an administrator - 2 pts
User nadia is not an administrator - 2 pts
Changed insecure password for user conrad - 2 pts
A minimum password length is required - 4 pts
A default minimum password age is set - 4 pts
An account lockout policy is configured - 4 pts
IPv4 forwarding has been disabled - 4 pts
Firewall protection has been enabled - 3 pts
Apache2 service has been disabled or removed - 4 pts
Samba service has been disabled or removed - 4 pts
Install updates from important security updates - 2 pts
Linux kernel has been updated - 2 pts
OpenSSL shared libraries have been updated - 2 pts
7zip has been updated - 3 pts
Pure FTP has been updated - 3 pts
Prohibited MP3 files are removed - 2 pts
Prohibited Software Kismet removed - 3 pts
Prohibited software Nmap removed - 3 pts
Prohibited software Freeciv removed - 3 pts
Removed netcat backdoor - 5 pts
SSH root login has been disabled - 4 pts
FTP anonymous access is disabled - 4 pts
FTP plain-text authentication disabled - 4 pts

2018-19 State Round (Ubuntu 14)
Vulns - 36/36 - 100/100
FORENSICS:
- Q1 - 139, 445, 53, 5800
- Q2 - 108
- Q3 - 1125

USER AUDITING:
- Guest account is disabled
- Removed unauthorised user raven
- Removed hidden user toor
- User wildcat is not an administrator
- User izza can not login without a password
- Banshee's password expires

ACCOUNT POLICY:
- A default minimum password age is set
- Previous passwords are remembered
- Extra non-dictionary password strength checks enabled
- An account lockout policy is configured

LOCAL POLICY:
- Greeter does not enumerate user accounts
- IPv4 sending ICMP redirects disabled
- Restrict unprivileged access to kernel syslog enabled
- Insecure sudo configuration fixed
- ASLR is enabled

UNCATEGORIZED OPERATING SYSTEM SETTINGS:
- Stricter defaults have been enabled for shared memory

SERVICE AUDITING:
- Minetest service has been disabled or removed
- SNMP service has been disabled or removed

OPERATING SYSTEM UPDATE:
- The system automatically checks for updates daily
- Linux kernel has been updated
- Glibc has been updated

APPLICATION UPDATE:
- Samba has been updated

PROHIBITED FILE:
- Prohibited MP3 files are removed
- Removed plain text file containing passwords

UNWANTED SOFTWARE:
- Prohibited software Minetest removed
- Prohibited software p0f is removed

MALWARE:
- Removed python backdoor

APPLICATION SECURITY:

Firefox warns when sites try to install add-ons

Unauthorised Samba share is disabled (Remove all extra shares such as [printer share]

SMB share is not world writeable (writeable = no &/OR read only = yes)

Encrypt smb traffic is enabled/Encrypt passwords enabled (smb encrypt = required & Encrypt passwords = yes & Obey pam restrictions = no)

ntlm authentication is disabled (client NTLMv2 auth = no & ntlm auth = disabled OR client NTLMv2 auth = yes, ntlm auth = ntlmv2-only)

SSH does not permit empty passwords

2018-19 Semifinals Round (Ubuntu 14)

Vulns - 30/30 - 100/100

Forensics:

- 1- 22,631,17071,17072,1707,30000
- 2- Frosty Flights
- 3- 38f3b03e-4415-43d2-bc22-1e1b12941c27

User Auditing:

- Remove user raven
- Remove user dusk
- Wildcat should not be admin
- Calamity must login with a password (/etc/group remove from nopasswdlogin group)

Account Policy:

- PASS_MAX_DAYS corrected in login.defs
- Previous passwords are remembered
- Extra dictionary password strength checks are enabled
- Account Lockout policy is configured

Local Policies:

- Dmesg restrict set to 1
- Ipv4_forward contains 0(disable ipv4 forwarding)
- Sysrq is set to 0(disable sysrq)
- Xserver-allow-tcp set to false in /etc/lightdm/lightdm.conf

Uncategorized operating system updates:

- /etc/shadow not world readable

Services:

- Postfix - removed
- Minetest - removed

Operating system update:

- bash
- Kernel
- Daily updates

Application update:

- Sshd
- Firefox

Prohibited files:

- Prohibited mp3 files

Software:

- Minetest removed - /usr/games/minetest removed
- NBTscan removed - /usr/bin/nbtscan removed

Malware:

- /usr/lib/gvfs/gvfs-trash removed, /etc/rc.local has ONLY exit 0, Removed Netcat backdoor

Application security:

- SSH - PermitUserEnvironment No sshd_config

- SSH - Set to Protocol 2 in sshd_config
- Firefox - Block dangerous and deceptive content

2018-19 Semifinals Round (Debian 8)

Vulns - 40/40 - 100/100

FORENSICS:
- F1- Flash Missing,? Wanishes in Crisis
- F2- savitar, ethawne, iwest
- F3- C2P!ctureN#ws

USER AUDITING:
- man- Does not have a login shell (change from /bin/sh)
- Root user - has a password
- iwest- pass encrypted with a secure hash
- hwells- password expires i think
- mrory- take out of sudo
- debian user is removed

ACCOUNT POLICY:
- password complexity - added gecoscheck to cracklib line
- Secure hashing algorithm - Added sha512 to unix.so line
- nullok password do not authenticate - Removed nullok from all pam.d files

LOCAL POLICY:
- /proc/sys/net/ipv4/tcp_synack_retries - contains a value 1-4
- /proc/sys/net/ipv4/tcp_rfc1337 - contains 1
- /proc/sys/kernel/unprivileged_userns_clone - contains 0
- /etc/sudoers.d/README - Does not have Default !authenticate

UNCATEGORIZED OPERATING SYSTEM SETTINGS:
- /boot/grub/grub.cfg - contains set superusers= and password_pbkdf2 grub
- /boot/grub/grub.cfg - not world readable
- /proc/mounts - contains tmpfs & none with noexec & nosuid
- /etc/host.conf - contains nospoof on

SERVICE AUDITING:
- bind9 service is stopped and removed
- nfs services is stopped and removed

OPERATING SYSTEM UPDATE:
- sources.list has valid debian lists
- kernel is updated

APPLICATION UPDATE:
- Apache2 is updated
- PHP5 is updated
- Wordpress is updated

PROHIBITED FILES:
- /usr/share/wordpress/info.php is removed, file /usr/share/wordpress/wp-login.php EXISTS (DO NOT DELETE THIS FILE)

UNWANTED SOFTWARE:
- Tcpspray - /usr/bin/tcpspray is removed
- Dsniff - /usr/sbin/dsniff is removed

MALWARE:
- Perl and LPD are removed - /usr/bin/perl & /usr/bin/lpd are REMOVED

php backdoor /usr/share/wordpress/wp-admin/webroot.php is removed, php file /usr/share/wordpress/wp-admin/admin.php EXISTS (DO NOT DELETE THIS FILE)
/sbin/sforce SUID backdoor removed (the file /sbin/sforce is removed)
APPLICATION SECURITY:
SQL bind address to localhost OR skip-networking
SQL is not ran as root
Expose php is off
php allow url fopen is off
php session.use_strict_mode is on
Apache serverSignature is off
Apache fileEtag none

2019-20 Practice Round (Ubuntu 16)
Vulns - 14/14 - 100

Forensics Question 1 Correct - 10
Forensics Question 2 Correct - 10
Forensics Question 3 Correct - 10
Removed unauthorized user rsharpe - 5
Removed unauthorized user kdanvers - 5
User csnow is not an administrator - 10
Changed insecure password for user jwells - 5
Firewall protection has been enabled - 10
FTP service has been disabled or removed - 10
System automatically checks for updates daily - 5
Install updates from important security updates - 5
Prohibited mp3 media files have been removed - 5
Prohibited software Nmap and Zenmap have been removed - 5
Firefox pop up blocker has been enabled - 5

2019-20 Round 1 (Ubuntu 14)
Vulns - 17/17 - 100

Forensics Question 1 Correct - 8
Removed unauthorized user mfreeze - 6
Removed unauthorized user joker - 6
Removed unauthorized user rghul - 6
User harold is not an administrator - 6
Changed insecure password for user bgordon - 6
Created new user ace - 6
A default maximum password age is set - 5
Uncomplicated Firewall (UFW) protection has been enabled - 6
Apache2 Service has been disabled or removed - 5
The system automatically checks for updates daily - 5
Install updates from important security updates - 5
OpenSSH has been updated - 6
Removed plain text file containing passwords - 6
Prohibited software Wireshark removed - 6
Prohibited software Zenmap and Nmap removed - 6
SSH root login has been disabled - 6

2019-20 Round 2 (Ubuntu 14)

Vulns - 30/30 - 100
Forensics Question 1 Correct - 8
Forensics Question 2 Correct - 8
Removed unauthorized user mfreeze - 2
Removed unauthorized user joker - 2
Removed unauthorized user rghul - 2
User harold is not an administrator - 2
User skyle is not an administrator - 4
Changed insecure password for user bgordon - 2
Created user ace - 2
A default maximum password age is set - 2
A default minimum password age is set - 4
IPv4 TCP SYN Cookies have been enabled - 4
Ignore broadcast ICMP echo requests enabled - 4
Sudo requires authentication - 4
Uncomplicated Firewall (UFW) protection enabled - 2
Insecure permissions on shadow file fixed - 4
Apache2 service has been disabled or removed - 2
Postgresql has been disabled or removed - 4
The system automatically checks for updates daily - 2
Install updates from important security updates - 2
OpenSSH has been updated - 2
7zip has been updated - 4
Removed plain text file containing passwords - 2
Prohibited software Wireshark removed - 2
Prohibited Software Zenmap and Nmap removed - 2
Stellarium has been installed - 5
Prohibited software Freeciv removed - 5
Removed Netcat backdoor - 5
SSH Root Login has been disabled - 2
Firefox displays warning on known malware sites - 5

2019-2020 State Round (Ubuntu 16)

Vulns listed - 42/42 - 100/100
Forensics Question 1 - 5
Forensics Question 2 - 5
Forensics Question 3 - 5
Forensics Question 4 - 5
Removed hidden user kpaulus - 1
User espence is not an administrator - 1
Changed insecure password for user jcousteau - 1
User pdiole has a maximum password age - 2
Disabled shell login for user syslog - 2
A default maximum password age is set - 2
Previous passwords are remembered - 2
Extra dictionary-based password strength checks enabled - 2
An account lockout policy is configured - 2
Null passwords do not authenticate on insecure consoles -2
IPV4 forwarding has been disabled - 2
Address space layout randomization enabled - 2
IPV4 Time Wait Assassination protection enabled - 2
IPV4 source route verification enabled - 2
Insecure Sudo configuration fixed - 2
Firewall protection has been enabled - 2
TMP has been mounted securely - 2
OpenSSH service has been installed and started - 3
Nginx service has been disabled or removed - 2
Samba service has been disabled or removed - 2
WorldForge service has been disabled or removed - 2
Install updates from important security updates - 2
Linux Kernel has been updated - 2
Bash has been updated - 2
BusyBox has been updated - 2
Pro FTP Daemon has been updated - 2
Prohibited mp3 files removed - 2
Removed file containing password hashes - 2
Prohibited software hunt removed - 2
Prohibited software dsniff removed - 2
Prohibited software Endless Sky removed - 2
Removed Netcat backdoor - 3
Firefox malware protection enabled - 2
FTP Anonymous access is disabled -3
FTP requires TLS is enabled - 3
FTP service is not running as root - 3

FTP Server identity is off -3
SSH allows only public key authentication - 3

2019-2020 Semifinals Round (Debian 8)

Vulns listed - 40/40 - 100/100
Forensics Question 1 Correct - 8
Forensics Question 2 Correct - 8
Forensics Question 3 Correct - 8
Removed unauthorized user hzolomon - 1
Bin user no longer has a shell login - 1
User savitar is not an administrator - 1
User jgarrick has a secure password - 1
Root password is no longer blank - 1
Application Security Check Passed - 2
Application Security Check Passed - 2
Application Security Check Passed - 2
Application Security Check Passed - 2
Application Security Check Passed - 2
Local Policy Check Passed - 2
Local Policy Check Passed - 2
Local Policy Check Passed - 2
Local Policy Check Passed - 2
Synack Retries set to secure values - 2
Uncomplicated Firewall has been enabled - 1
Uncategorized Operating System Setting Check Passed - 2
Bind9 Service has been stopped and disabled - 2
Nginx Service has been stopped and disabled - 2
MySQL Service has been stopped and disabled - 2
Apt Sources list has been updated and set - 2
Linux Kernel has been updated - 2
PHP5 has been updated - 2
Apache has been updated - 2
OpenSSH Server has been updated - 2
Prohibited software OPHCrack removed - 2
Prohibited software Ettercap removed - 2
Prohibited software Wireshark removed - 2
Prohibited software Chntpw removed - 2
Index.php malware removed - 5
Plain Text file “users” in root directory removed - 2
Firefox warns for malicious downloads - 2
PHP expose_php has been disabled - 3
PHP strict mode has been enabled - 3
Apache Server Signature has been disabled - 3
SSH Port has been changed to 222 - 3
SSH Root Login has been disabled - 3

2019-2020 Semifinals Round (Ubuntu 16)

Vulns listed - 36/36 - 100/100
Forensics Question 1 Correct - 8
Forensics Question 2 Correct - 8
Forensics Question 3 Correct - 8
Removed hidden user kpaulis - 1
Unauthorized user ace removed - 1
User espence is not an administrator - 1
User pdiole has a secure password - 1
User fdumas has a maximum password age - 2
Account Policy Check Passed - 2
Account Policy Check Passed - 2
Account Policy Check Passed - 2
Account Policy Check Passed - 2
Local Policy Check Passed - 2
Local Policy Check Passed - 2
Local Policy Check Passed - 2
Local Policy Check Passed - 2
Defaults !Authenticate removed from the /etc/sudoers file - 2
Uncomplicated Firewall has been enabled - 2
Uncategorized Operating System Setting Check Passed - 2
QTorrent Service has been stopped and disabled - 2
Samba service has been stopped and disabled - 2
Updates are automatically checked for daily - 2
Important Security Downloads have been conducted - 2
MySQL has been updated - 2
Bash has been updated - 2
Proftpd has been updated - 2
Linux Kernel has been updated - 2
Removed prohibited mp3 media files - 2
Prohibited software Ettercap removed - 2
Prohibited software hunt removed - 2
Netcat backdoor removed - 4
Proftpd anonymous configuration removed - 5
Firefox dangerous downloads are blocked - 3
MySQL SSL Certificates are valid and enabled - 4
MySQL bind address has been set to local ip (127.0.0.1) - 5
Proftpd ServerIdent has been disabled - 5

2020-2021 Exhibition Round 1 (Ubuntu16)

Vulns listed - 19/19 - 100/100
Forensics Question 1 Correct - 8
Forensics Question 2 Correct - 8
Forensics Question 3 Correct - 8
Removed unauthorized user brainiac - 4
Removed unauthorized user alchemy - 4
User wwest is not an administrator - 4
User jwest is not an administrator - 4
Changed insecure password for user jwells- 4
A default maximum password age is set - 5
Uncomplicated Firewall (UFW) protection has been enabled - 6
OpenSSH server has been installed and is running - 5
Samba service has been disabled or removed - 5
Updates are automatically checked for automatically daily - 4
Linux Kernel has been updated - 4
Removed plain text file containing passwords - 6
Removed prohibited mp3 media files - 6
OPHCrack software removed - 5
Minetest software removed - 5
SSH Root Login has been disabled- 5

2020-2021 Exhibition Round 2 (Ubuntu 14)

Vulns listed - 22/22 - 100/100
Forensics Question 1 Correct - 8
Forensics Question 2 Correct - 8
Forensics Question 3 Correct - 8
Removed unauthorized user gward - 2
Removed unauthorized user aida - 2
User deke is not an administrator - 2
User hunter is not an administrator - 2
Changed insecure password for user mack - 2
Created user group shield - 3
Added users to group shield - 3
A default maximum password age is set - 5
A default minimum password age is set - 5
Uncomplicated Firewall (UFW) protection has been enabled - 5
Apache service has been disabled or removed - 5
Samba service has been disabled or removed - 5
Updates are automatically checked for automatically daily - 5
Linux Kernel has been updated - 5
Sudo has been updated - 5
Firefox has been updated - 5
Removed prohibited mp3 media files - 5
OPHCrack software removed - 5
Minetest software removed - 5

2020-2021 AFA Advanced Cybercamp Image

Vulns listed - 30/30 - 100/100
Forensics Question 1 Correct - 6
Forensics Question 2 Correct - 6
Forensics Question 3 Correct - 6
Forensics Question 4 Correct - 6
Removed unauthorized user darla - 2
Removed unauthorized user mrray - 2
Removed hidden user dentist - 2
User chum is not an administrator - 2
User bruce is not an administrator - 2
Changed insecure password for user gill - 2
Created user group fisharefriends - 2
Added users to group fisharefriends - 2
A minimum password length is required - 4
Previous passwords are remembered - 4
An account lockout policy is configured - 4
IPv4 TCP SYN Cookies have been enabled - 4
Address Space Layout Randomization enabled - 4
IPv4 Forwarding has been disabled - 4
Uncomplicated Firewall (UFW) protection has been enabled - 3
Apache service has been disabled or removed - 3
MySQL service has been disabled or removed - 3
NFS service has been disabled or removed - 3
Linux Kernel has been updated - 3
Samba has been updated - 3
OpenSSH has been updated - 3
Removed prohibited mp3 media files - 3
Prohibited software Wireshark removed - 3
Prohibited software John removed - 3
Removed netcat backdoor - 3
Removed python backdoor - 3

2020-2021 Training Round (Ubuntu 16)

Vulns listed - 14/14 - 100/100
Forensics Question 1 Correct - 10
Forensics Question 2 Correct - 10
Forensics Question 3 Correct - 10
Removed unauthorized user rsharpe - 5
Removed unauthorized user kdanvers - 5
User csnow is not an administrator - 10
Changed insecure password for user jwells - 5
Firewall protection has been enabled - 10
FTP service has been disabled or removed - 10
The system automatically checks for updates daily - 5
Install updates from important security updates - 5
Prohibited mp3 files have been removed - 5
Prohibited software Zenmap and Nmap removed - 5
Firefox pop-up blocker enabled - 5

2020-2021 Practice Round (Ubuntu 16)

Vulns Listed - 13/13 - 100/100
Forensics Question 1 Correct - 9
Forensics Question 2 Correct - 9
Removed unauthorized user reno - 7
Removed unauthorized user elena - 7
User ykisaragi is not an administrator - 7
Changed insecure password for user bwallace - 7
Uncomplicated Firewall (UFW) protection has been enabled - 10
FTP service has been disabled or removed - 9
The system automatically checks for updates daily - 7
Install updates from important security updates - 7
Prohibited mp3 files are removed - 7
Prohibited software Kismet removed - 7
Firefox warns when sites try to install add-ons - 7

2020-2021 Practice Round (Debian 9)

Vulns Listed - 16/16 - 100/100
Forensics Question 1 Correct - 9
Forensics Question 2 Correct - 9
Removed unauthorized user rude - 6
Removed unauthorized user tseng - 6
User dyne is not an administrator - 6
Created user account ykisaragi - 5
Created user group gold - 5
Added users to group gold - 5
Uncomplicated Firewall (UFW) protection has been enabled - 8
POP3 service has been disabled or removed - 7
The system automatically checks for updates daily - 5
Install updates from important security updates - 5
OpenSSH has been updated - 6
Prohibited software Nmap removed - 6
Prohibited software Ettercap removed - 6
Firefox blocks dangerous downloads - 6

2020-2021 Round 1 (Ubuntu 18)

Vulns Listed - 20/20 - 100/100
Forensics Question 1 Correct - 10
Forensics Question 2 Correct - 10
Removed unauthorized user ballen - 5
Removed unauthorized user sheogorath - 5
User ulfric is not an administrator - 4
Changed insecure password for user esber - 4
Guest account is disabled - 4
Created user account belethor - 5
Uncomplicated Firewall (UFW) protection has been enabled - 6
FTP service has been disabled or removed - 6
The system automatically checks for updates daily - 4
Install updates from important security updates - 4
Linux Kernel has been updated - 4
OpenSSH has been updated - 4
LibreOffice has been updated - 4
Firefox has been updated - 4
Prohibited mp3 files have been removed - 4
Prohibited software ManaPlus removed - 4
Prohibited software Game Conqueror removed - 4
SSH Root Login has been disabled - 5

2020-2021 Round 2 (Ubuntu 16)

Vulns Listed - 31/31 - 100/100
Forensics Question 1 Correct - 7
Forensics Question 2 Correct - 7
Forensics Question 3 Correct - 7
Removed unauthorized user sephiroth - 3
Removed terminated employee's user accoutn 'dyne' - 4
User zfair is not an administrator - 2
Changed insecure password for user againsborough - 2
Changed insecure password for user bwallace - 2
A default maximum password age is set - 3
A minimum password length is required - 4
Stack and heap address space layout randomization enabled - 3
IPV4 Forwarding has been disabled - 3
Sudo requires authentication - 3
Group Shinra does not have sudo privileges - 3
Uncomplicated Firewall (UFW) has been enabled - 3
Inline scripts are not allowed by nginx content security policy - 3
Nginx set to block XSS attacks for legacy browsers - 3
Nginx server tokens disabled - 3
SNMP service has been disabled or removed - 3
The system automatically checks for updates daily - 2
Install updates from important security updates - 2
Nginx has been updated - 2
OpenSSH has been updated - 2
Prohibited plaintext credit card information was removed - 3
Prohibited software Hydra removed - 3
Prohibited software yersinia removed - 3
Prohibited software deluge removed - 3
Removed perl bindshell backdoor - 4
Firefox warns when sites try to install add-ons - 2
SSH does not permit empty passwords - 3
SSH Protocol 1 has been disabled - 3

2020-2021 Round 2 (Ubuntu 18)

Vulns Listed - 37/37 - 100/100
Forensics Question 1 Correct - 6
Forensics Question 2 Correct - 6
Forensics Question 3 Correct - 6
Removed hidden user akatosh - 3
Removed unauthorized user alduin - 2
User belethor is not an administrator - 2
Disabled password login for user bin - 3
Disabled shell login for user irc - 3
Previous passwords are remembered - 3
A default minimum password age is set - 2
An account lockout policy is configured - 3
Null passwords do not authenticate - 3
X Server does not allow TCP connections - 3
IPv$ TCP SYN cookies have been enabled - 2
Ignore broadcast ICMP echo requests enabled - 2
Insecure sudo configuration fixed - 3
Uncomplicated Firewall (UFW) protection has been enabled - 2
Insecure permissions on shadow file fixed - 3
IRC Daemon has been disabled or removed - 2
AppArmor service is enabled and running - 3
Install updates from important security updates - 1
Linux Kernel has been updated - 2
APT has been updated - 1
Firefox has been updated - 1
Samba has been updated - 2
Prohibited MP3 files are removed - 3
Prohibited software dsniff removed - 2
Prohibited software linuxdcpp removed - 2
Prohibited software rfdump removed - 2
Prohibited software heartbleeder removed - 2
Removed perl owl-shell backdoor - 4
Fixed insecure permissions on find - 4
Firefox checks the current validity of certificates - 2
Samba SMB1 protocol is disabled - 3
Unauthorized Samba share is disabled - 2
Insecure permissions on Samba share fixed - 2
Samba encryption is required - 3

2020-2021 Round 3 (Debian 9)

Vulns Listed - 37/37 - 100/100
Forensics Question 1 Correct - 5
Forensics Question 2 Correct - 5
Forensics Question 3 Correct - 5
Forensics Question 4 Correct - 5
Removed unauthorized user bahamut - 2
Removed hidden user sephiroth - 3
User jessie is not an administrator - 2
Disabled shell login for user games - 2
User rtuesi has a maximum password age - 2
Password for zfair hashed with a secure algorithm - 3
A minimum password length is required - 2
Extra dictionary password checks enabled - 3
A secure password hashing algorithm is used - 2
A default maximum password age is set - 2
IPv4 TIME-WAIT assassination protection enabled - 3
Logging of martian packets enabled - 2
Restrict unprivileged access to kernel syslog enabled - 3
Uncomplicated firewall (UFW) protection has been enabled - 2
Insecure permissions on PostgreSQL configuration files fixed - 3
GRUB configuration is not world readable - 2
Apache service has been disabled or removed - 2
Samba service has been disabled or removed - 2
DNS service has been disabled or removed - 2
Install updates from important security updates - 1
PostgreSQL has been updated - 3
Firefox has been updated - 2
Prohibited MP3 files removed - 3
Prohibited software cupp3 removed - 2
Prohibited software cmospwd removed - 2
Prohibited software fcrackzip removed - 2
Removed netcat backdoor - 3
Removed python backdoor - 3
PostgreSQL rejects all non-local connection requests without SSL - 3
PostgreSQL required authentication for all connections - 4
PostgreSQL has ssl enabled (ssl = true) - 4
PostgreSQL configured to log connections - 2
PostgreSQL does not map any user to the postgres account - 2

2020 Hivestorm Round (Debian 9)

Vulns Listed - 49/56

Forensics Question 1 correct
Forensics Question 2 correct
Forensics Question 3 correct
Removed unauthorized user minaros
Removed unauthorized user jpmao
Removed hidden user serrinwright
Removed hidden user amurty
User jmiller is not an administrator
User fjohnson is not an administrator
Root password no longer blank
Password for jholden is hashed with a secure algorithm
Previous passwords are remembered
A minimum password length is required
Extra dictionary based password strength checks enabled
Null passwords do not authenticate
IPv4 TCP SYN cookies have been enabled
Ignore bogus ICMP errors enabled
IPv4 accept source routing disabled
IPv4 TCP SYN,ACK retries reduced
Logging of martian packets enabled
Restrict unprivileged access to kernel syslog enabled
Insecure permissions on shadow file fixed
Process information hidden from other users
Firewall protection has been enabled
NFS has been stopped and disabled
Rsync service has been disabled or removed
IRC daemon has been disabled or removed
Minetest service has been disabled or removed
Install updates from important security updates
OpenSSL shared libraries have been updated
Apache has been updated
PHP has been updated
Bluefish has been updated
FileZilla has been updated
Prohibited software Nmap removed
Prohibited software xprobe removed
Prohibited software Ettercap removed
Prohibited software yersinia removed
Prohibited software john the ripper removed
Prohibited software OpenRA removed
Removed netcat backdoor
Firefox warns when sites try to install add-ons
SSH root login has been disabled
SSH does not permit empty passwords

PHP does not display errors
Apache server signature disabled
Apache server tokens set to least
Apache etags disabled
Apache trace requests disabled

2020 Hivestorm Round (Ubuntu 16)

Vulns Listed - 44/51

Forensics Question 1 correct
Forensics Question 2 correct
Forensics Question 3 correct
Guest account is disabled
Removed unauthorized user mkoh
Removed unauthorized user leelee
Removed unauthorized user emartin
Removed hidden user pcortazar
User jmiller is not an administrator
User avolovodov is not an administrator
Disabled password login for user bin
User nnagata has a minimum password age
A default maximum password age is set
Extra GECOS password strength checks enabled
Null passwords do not authenticate on insecure consoles
An account lockout policy is configured
Greeter does not enumerate user accounts
Ignore broadcast ICMP echo request enabled
IPv4 source route verification enabled
IPv4 accept ICMP redirects disabled
Address space layout randomization enabled
Kernel pointers hidden from unprivileged users
GRUB uses encrypted password protection
GRUB configuration is not world readable
DNS service is disabled or removed
FTP service has been disabled or removed
Squid proxy service has been disabled or removed
POP3 service has been disabled or removed
SMTP service has been disabled or removed
Sudo has been updated
Bash has been updated
Nginx has been updated
PHP has been updated
LibreOffice has been updated
Thunderbird has been updated
Removed php backdoor
Prohibited software Angry IP Scanner removed
Prohibited software scapy removed
Prohibited software arp-scan removed
Prohibited software ophcrack removed
Prohibited software Endless Sky removed
Firefox pop-up blocker enabled
Firefox warns when sites try to install add-ons
PHP does not display errors

PWest Round 1 Simulation Image (Ubuntu 16)

Vulns listed - 20/20 - 100/100

Forensics 1 Correct - 8
Forensics 2 Correct - 8
Unauthorized user gjohnson removed - 4
Unauthorized user chudson removed - 4
User drake is not an administrator - 4
Added new user aandthechipmunks - 5
User cdamelio has a secure password - 5
Guest user has been disabled - 5
A secure maximum password age has been set - 5
Firewall is enabled - 5
FTP Service has been stopped or disabled - 5
Updates are checked for daily - 4
A majority of important security updates have been installed - 4
OpenSSH Service has been updated - 4
Firefox has been updated - 5
Bash has been updated - 4
Prohibited mp3 media file removed - 5
Prohibited software John The Ripper removed - 5
Prohibited software Freeciv removed - 5
SSH Root Login has been disabled - 5

2020-2021 PWest Tryout Image (Ubuntu 16)

Vulns listed - 50/50 - 100/100

Forensics 1 Correct - 4
Forensics 2 Correct - 4
Forensics 3 Correct - 4
Forensics 4 Correct - 4
Forensics 5 Correct - 4
Removed hidden user oatsthementor- 2
Removed hidden user mviswanadha - 2
Removed hidden user richtheindian - 2
Unauthorized user ahadji removed- 1
Unauthorzied user kjongun removed - 1
User sjaladi is not an administrator - 1
User kviswanadha is not an administrator - 1
User jrooks has a secure password - 1
User swinfrey has a secure password - 1
Created new user emusk- 1
User musk is an administrator - 1
Created New Group ogs - 1
Users have been added to Group ogs - 2
Disabled shell login for user man - 2
Disabled shell login for user bin - 2
Guest user has been disabled - 1
Previous passwords are remembered - 1
A secure minimum password length has been set - 1
A secure maximum password age has been set - 1
IPv4 Forwarding has been disabled - 2
Address Space Layout Randomization has been enabled- 2
Insecure sudo configuration fixed - 2
User kviswanadha can no longer use the sudo command without a password - 2
Firewall is enabled - 1
Shadow file has secure file permissions - 3
Apache Service has been stopped or disabled - 2
Postgresql Service has been stopped or disabled - 2
Samba Service has been stopped or disabled - 2
Updates are automatically checked for daily - 1
APT Sources list has valid and secure sources - 2
Prohibited mp3 media files have been removed - 1
Removed plain-text password file - 2
Removed bad shadow file copy containing password hashes - 3
Removed netcat backdoor - 2

/bin/nano suid bit removed - 3
/sbin/sforce suid bit creator file removed - 3
Prohibited software John the Ripper removed - 2
Prohibited software Nmap removed - 1
Prohibited software Wireshark removed - 1
Prohibited software Freeciv removed - 1
Firefox blocks pop ups - 3
Firefox displays warnings on dangerous downloads - 3
SSH no longer allows root login - 3
SSH port has been changed to 222 - 3
SSH Protocol has been changed to Protocol 2 - 3

Troy Practice Image Scoring Engine 1 (Debian 8)

Vulns listed - 45/45 - 100/100

```
vulns.append(newCommandObject('cat /home/tanjiro/Desktop/forensics1.txt', 'zenitsu', True, 4, 'Forensics Question 1 correct'))
vulns.append(newCommandObject('cat /home/tanjiro/Desktop/forensics2.txt', '1234', True, 4, 'Forensics Question 2 correct'))
vulns.append(newCommandObject('cat /home/tanjiro/Desktop/forensics3.txt', 'IMACTUALLYMICHAELJACKSON', True, 4, 'Forensics Question 3 correct'))
vulns.append(newCommandObject('a', 'a', True, 1, 'Removed unauthorized user'))
vulns.append(newCommandObject('cat /etc/passwd', 'rui', False, 1, 'Removed unauthorized user'))
vulns.append(newCommandObject('cat /etc/passwd', 'muzan', False, 1, 'Removed unauthorized user'))
vulns.append(newCommandObject('cat /etc/passwd', 'debiansys', False, 1, 'Removed unauthorized user'))
vulns.append(newCommandObject('cat /etc/passwd', 'critlampuser', False, 1, 'Removed unauthorized user'))
vulns.append(newCommandObject('cat /etc/shadow | grep zenitsu', '18273', False, 1, 'Changed zenitsu\'s password'))
vulns.append(newCommandObject('cat /etc/shadow | grep nezuko', '18273', False, 1, 'Changed nezuko\'s password'))
vulns.append(newCommandObject('cat /etc/group | grep 27', 'crow', True, 1, 'Added crow as admin'))
vulns.append(newCommandObject("cat /etc/group | grep 27 | grep -Eo \'(urokodaki|tamayo|tomioka|shinobu)\' | wc -l", '4', True, 2, 'urokodaki, tamayo, tomioka, and shinobu are all admins'))
vulns.append(newCommandObject("ufw status | grep -E \'(21|22|80|3306)\' | grep ALLOW | wc -l", '4', True, 2, 'Firewall allows FTP, SSH, and LAMP stack'))
vulns.append(newCommandObject("stat -c '%a' /etc/passwd", '644', True, 2, 'System hardening check passed'))
vulns.append(newCommandObject('cat /etc/pam.d/common-password | grep pam_cracklib.so', 'gecoscheck', True, 1, 'System hardening check passed'))
vulns.append(newCommandObject('cat /etc/pam.d/common-password | grep pam_unix.so', 'sha512', True, 1, 'System hardening check passed'))
vulns.append(newCommandObject('stat -c %a /etc/grub.d ', '777', False, 3, 'System hardening check passed'))
vulns.append(newCommandObject('cat /etc/host.conf | grep nospoof', 'on', True, 2, 'System hardening check passed'))
vulns.append(newCommandObject('ls -la /etc/skel', '.sysclean', False, 4, 'Removed backdoor'))
vulns.append(newCommandObject('cat /etc/login.defs' | grep -E \'(PASS_MAX_DAYS|PASS_MIN_DAYS)\' | grep -v "#" | grep -E \'(99999|0)\' | wc -l', '0', True, 2, 'A default min/max password age set'))
```

```
vulns.append(newCommandObject('cat /etc/gdm3/greeter.dconf-defaults | grep disable-user-list', 'true', True, 3, 'System hardening check passed'))
vulns.append(newCommandObject('cat /etc/sysctl.conf | grep net.ipv4.tcp_syncookies', '1', True, 2, 'Sysctl hardening check passed'))
vulns.append(newCommandObject('cat /etc/sysctl.conf | grep net.ipv4.ip_forward', '0', True, 2, 'Sysctl hardening check passed'))
vulns.append(newCommandObject('cat /etc/sysctl.conf | grep net.ipv6.conf.all.disable_ipv6', '0', True, 2, 'Sysctl hardening check passed'))
vulns.append(newCommandObject('apt list --installed p0f', 'installed', False, 1, 'Unauthorized software removed'))
vulns.append(newCommandObject('apt list --installed openarena', 'installed', False, 1, 'Unauthorized software removed'))
vulns.append(newCommandObject('apt list --installed kismet', 'installed', False, 1, 'Unauthorized software removed'))
vulns.append(newCommandObject('apt list --installed tightvncserver', 'installed', False, 1, 'Unauthorized software removed'))
vulns.append(newCommandObject('apt list --installed medusa', 'installed', False, 1, 'Unauthorized software removed'))
vulns.append(newCommandObject('apt list --installed john', 'installed', False, 1, 'Unauthorized software removed'))
vulns.append(newCommandObject('cat /etc/fstab', 'noexec', True, 3, 'Stricter defaults have been enabled for shared memory'))
vulns.append(newCommandObject('ls -l /bin/nano', 'rwsrwxrwx', False, 5, 'nano is no longer SUID'))
vulns.append(newCommandObject('apt list --installed apache2 vsftpd mysql-server openssh-server php7.0 | wc -l', '6', True, 1, 'FTP, SSH, and LAMP are installed'))
vulns.append(newCommandObject('cat /etc/vsftpd.conf | grep anonymous_enable', 'NO', True, 2, 'Application security check'))
vulns.append(newCommandObject('cat /etc/vsftpd.conf | grep secure_chroot_dir', '/srv/ftp', True, 2, 'Application security check passed'))
vulns.append(newCommandObject('cat /etc/apache2/apache2.conf | grep ServerSignature', 'Off', True, 2, 'Software security check passed'))
vulns.append(newCommandObject('cat /etc/apache2/apache2.conf | grep ServerTokens', 'Prod', True, 2, 'Software security check passed'))
vulns.append(newCommandObject('cat /etc/mysql/my.cnf | grep bind-address', '127.0.0.1', True, 2, 'Software security check passed'))
vulns.append(newCommandObject('cat /etc/php/7.0/apache2/php.ini | grep expose_php', 'Off', True, 2, 'Software security check passed'))
vulns.append(newCommandObject('cat /etc/ssh/sshd_config | grep PermitRootLogin', 'no', True, 2, 'Software security check passed'))
vulns.append(newCommandObject('3', '3', True, 3, 'Corrected incorrect system setting'))
vulns.append(newCommandObject('ls /bin', 'nologin', False, 4, 'Removed /bin/nologin'))
```

```
vulns.append(newCommandObject('cat /etc/adduser.conf | grep DSHELL', '/bin/bash', True, 3, 'Default shell changed to /bin/bash'))
vulns.append(newCommandObject('cat /etc/passwd | grep -E \'^(daemon|games|man)\' | grep nologin', 'nologin', False, 3, 'Changed shell for daemon, games, man from /bin/nologin'))
vulns.append(newCommandObject('ls -R /home | grep "rf"', 'rf', False, 4, 'Removed tricky directory ahahaahaa'))
```

Troy Practice Image Scoring Engine 2 (Ubuntu 14)

Vulns listed - 31/31 - 100/100

```
vulns.append( newConfigObject( "/etc/lightdm/lightdm.conf", "allow-guest", "false", "=", 2, "Guest account is disabled" ) )
vulns.append( newUserObject( "vector", False, None, None, 2, "Removed unauthorized user vector" ) )
vulns.append( newUserObject( "short", False, None, None, 2, "Removed unauthorized user short" ) )
vulns.append( newUserObject( "telnet", False, None, None, 3, "Removed hidden user telnet" ) )
vulns.append( newMemberObject( "sudo", "aaron", False, 2, "User aaron is not an administrator" ) )
vulns.append( newMemberObject( "sudo", "nicole", False, 2, "User nicole is not an administrator" ) )
vulns.append( newUserObject( "root", True, True, "", 2, "Changed insecure root password" ) )
vulns.append( newConfigObject( "/etc/pam.d/common-password", "password", "remember=10", " ", 4, "Previous passwords are remembered" ) )
vulns.append( newConfigObject( "/etc/pam.d/common-password", "password", "sha512", " ", 4, "A secure password hashing algorithm is used" ) )
vulns.append( newConfigObject( "/etc/login.defs", "PASS_MAX_DAYS", "15", '\t', 4, "A default maxiumum password age is set" ) )
vulns.append( newConfigObject( "/etc/pam.d/common-auth", "auth", "deny=10", " ", 4, "An account lockout policy is configured" ) )
vulns.append( newConfigObject( "/etc/sysctl.conf", "net.ipv4.conf.all.rp_filter", "1", "=", 4, "IPv4 source route verification enabled" ) )
vulns.append( newConfigObject( "/etc/sysctl.conf", "net.ipv4.conf.all.send_redirects", "0", "=", 4, "IPv4 sending ICMP redirects disabled" ) )
vulns.append( newConfigObject( "/etc/sysctl.conf", "net.ipv4.tcp_synack_retries", "2", "=", 4, "IPv4 TCP SYNACK retries reduced" ) )
vulns.append( newCommandObject( "ufw status", "Status: active", True, 4, "Firewall protection has been enabled" ) )
vulns.append( newCommandObject( "service ssh status", "ssh start/running", True, 4, "sshd service has been installed and started" ) )
vulns.append( newCommandObject( "service apache2 status", "* apache2 is running", False, 4, "Apache2 service has been stopped and disabled" ) )
vulns.append( newCommandObject( "service inspircd status", "* inspircd is running", False, 4, "IRC daemon has been stopped and disabled" ) )
vulns.append( newCommandObject( "service mysql status", "Uptime:", False, 4, "MariaDB service has been stopped and disabled" ) )
vulns.append( newCommandObject( "find /home | grep [.]favorites", ".favorites", False, 3, "Prohibited MP3 files are removed" ) )
vulns.append( newCommandObject( "apt list --installed | grep firefox/", "upgradable", False, 3, "Firefox has been updated" ) )
```

```
vulns.append( newCommandObject( "apt list --installed | grep openssl", "upgradable", False, 3, "OpenSSL has been updated" ) )
vulns.append( newCommandObject( "apt list --installed | grep ophcrack/", "installed", False, 3, "Prohibited software ophcrack removed" ) )
vulns.append( newCommandObject( "apt list --installed | grep ettercap-common/", "installed", False, 3, "Prohibited software Ettercap removed" ) )
vulns.append( newCommandObject( "find /var | grep oxygen.html", "oxygen", False, 3, "Removed html file with credit card numbers in it" ) )
vulns.append( newCommandObject( "crontab -u root -l", "nc -e /bin/sh -nvlp 1337", False, 3, "Removed netcat backdoor" ) )
vulns.append( newCommandObject( "cat /etc/samba/smb.conf", "[share]", False, 3, "Public Samba Share is disabled" ) )
vulns.append( newCommandObject( "cat /etc/sudoers", "!authenticate", False, 4, "Insecure sudo configuration fixed" ) )
vulns.append( newCommandObject( "stat /var/opt/AFAGenesis/", "(0600/", True, 4, "Fixed insecure permissions for AFAGenesis" ) )
vulns.append( newConfigObject( "/etc/apt/apt.conf.d/10periodic", "APT::Periodic::Update-Package-Lists", "\"1\";", " ", 3, "The system automatically checks for updates daily" ) )
vulns.append( newConfigObject( "/etc/ssh/sshd_config", "PermitRootLogin", "no", " ", 2, "SSH root login has been disabled" ) )
```

Troy Practice Image Scoring Engine 3 (Ubuntu 16)

Vulns listed - 46/46 - 100/100

```
vulns.append(newCommandObject('cat "/home/sackboy/Desktop/Forensics Question 1"', 'Play! Create! Share! Huzzah!', True, 8, 'Forensics question 1 solved'))
vulns.append(newCommandObject('cat "/home/sackboy/Desktop/Forensics Question 2"', '/etc/passwd', True, 8, 'Forensics question 2 solved'))
vulns.append(newCommandObject('cat "/home/sackboy/Desktop/Forensics Question 3"', '192.168.0.15', True, 8, 'Forensics question 3 solved'))
vulns.append(newUserObject('newton', False, None, None, 2, 'Removed hidden root newton'))
vulns.append(newUserObject('sackbot', False, None, None, 1, 'Removed unauthorized user sackbot'))
vulns.append(newUserObject('sackgirl', True, True, '!', 1, 'Set a password for sackgirl'))
vulns.append(newUserObject('negativatron', False, None, None, 2, 'Removed unauthorized hidden user negativatron'))
vulns.append(newCommandObject('sudo -l -U larrydavinci | grep "not allowed"', 'not allowed', True, 2, 'Larry Davinci is not an admin'))
vulns.append(newCommandObject('cat /etc/group | grep sudo | grep narrator', 'narrator', True, 1,  'Narrator is an admin'))
vulns.append(newCommandObject('cat /etc/sudoers | grep -c auth', '1', True, 1, 'Removed authentication bypass'))
vulns.append(newCommandObject('cat /etc/sudoers | grep -c auth', '0', True, 1, 'Removed authentication bypass'))
vulns.append(newCommandObject('cat /etc/sudoers.d/README | grep auth', "authenticate", False, 1, 'Removed authentication bypass'))
vulns.append(newCommandObject('ls /media/album | grep [.]mp3', 'mp3', False, 1, 'Removed unauthorized MP3 files'))
vulns.append(newCommandObject('ls /mnt/moon | grep passwords', 'passwords', False, 2, 'Removed plaintext passsword file'))
vulns.append(newCommandObject('cat /etc/samba/smb.conf | grep -i printers', 'printers', False, 2, 'Removed printers share'))
vulns.append(newCommandObject('cat /etc/samba/smb.conf | grep -i negativatron', 'negativatron', False, 1, 'Removed negativatron share'))
vulns.append(newCommandObject('cat /etc/crontab | grep "nc "', 'nc', False, 1, 'Removed backdoor in /etc/crontab'))
vulns.append(newCommandObject('cat /var/spool/cron/crontabs/root | grep "nc "', 'nc', False, 2, 'Removed backdoor in roots crontab'))
vulns.append(newCommandObject('ls -l /mnt | grep moon | grep drw-r-----', "drw-r-----", True, 2, 'Secure file permissions set for /mnt/moon'))
vulns.append(newCommandObject('ufw status', 'Status: active', True, 1, 'Firewall is enabled'))
vulns.append(newUserObject('root', True, True, '!', 1, 'Changed insecure root password'))
vulns.append(newConfigObject('/etc/login.defs', 'PASS_MAX_DAYS', '15', '\t', 2, 'A default maxiumum password age is set'))
```

```
vulns.append(newConfigObject('/etc/login.defs', 'PASS_MIN_DAYS', '7', '\t', 2, 'A default minimum password age is set'))
vulns.append(newCommandObject('ls /bin', 'ex1t', False, 5, 'Removed bad executable ex1t'))
vulns.append(newCommandObject('cat /etc/pam.d/common-password','minlen=', True, 2, 'A minimum length has been set for passwords'))
vulns.append(newCommandObject('cat /etc/rc.local', 'ex1t', False, 2, 'Removed startup backdoor'))
vulns.append(newCommandObject('ufw show added', 'deny 21', False, 4, 'Firewall allows port 21'))
vulns.append(newCommandObject('cat /etc/ssh/sshd_config | grep X11Forwarding', 'no', True, 2, 'Disabled X11 Forwarding'))
vulns.append(newCommandObject('cat /etc/ssh/sshd_config | grep PermitRootLogin', 'no', True, 2, 'Disabled root login via ssh'))
vulns.append(newCommandObject('cat /etc/ssh/sshd_config | grep Protocol', '2', True, 2, 'SSH Protocol set to 2'))
vulns.append(newCommandObject('ls /etc/cron.d', 'runcheck', False, 2, 'Removed backdoor in crontab'))
vulns.append(newCommandObject('ls -l /etc | grep -v gshadow | grep -v shadow- | grep shadow', '-rw-r-----', True, 2, 'Secure file permissions set for shadow file'))
vulns.append(newCommandObject('ls /var', 'timemachine', False, 3, 'Removed the timemachine'))
vulns.append(newCommandObject('cat /etc/samba/smb.conf | grep -A 8 "\[moon\]" | grep "guest ok"', 'no', True, 2, 'moon share does not allow guests'))
vulns.append(newCommandObject('cat /etc/samba/smb.conf | grep -A 8 "\[moon\]" | grep "create mask"', '0640', True, 2, 'moon share create mask hardened'))
vulns.append(newCommandObject('cat /etc/vsftpd.conf | grep -v "#"', 'anonymous_enable=NO', True, 1, 'VSFTPD no longer allows anonymous access'))
vulns.append(newCommandObject('cat /etc/vsftpd.conf | grep -v "#"', 'secure_chroot_dir=/var/chroot', True, 1, 'VSFTPD chroot is properly configured'))
vulns.append(newCommandObject('cat /etc/sysctl.conf | grep -v "#"', 'net.ipv4.icmp_echo_ignore_broadcasts = 1', True, 2, 'Ignore IPv4 ICMP echo broadcasts'))
vulns.append(newCommandObject('cat /etc/apt/apt.conf.d/20auto-upgrades | grep Update-Package-Lists', '"1"', True, 2, 'Automatically checks for updates'))
vulns.append(newCommandObject('apt list --installed | grep ophcrack/', 'installed', False, 2, 'Prohibited software ophcrack removed'))
vulns.append(newCommandObject('apt list --installed | grep wireshark/', 'installed', False, 2, 'Prohibited software wireshark removed'))
vulns.append(newCommandObject('apt list --installed | grep postgresql/', 'installed', False, 2, 'Prohibited software postgresql removed'))
vulns.append(newCommandObject('apt list --installed | grep apache2/', 'installed', False, 2, 'Prohibited software apache2 removed'))
vulns.append(newCommandObject('apt list --installed | grep armagetronad/', 'installed', False, 2, 'Prohibited software armagetronad removed'))
```

```
vulns.append(newCommandObject('apt list --installed | grep netris/', 'installed', False, 2,
'Prohibited software netris removed'))
vulns.append(newCommandObject('apt list --installed | grep nmap/', 'installed', False, 1,
'Prohibited software nmap removed'))
```