2017-18 Round 1

Vulns - 21/21 - 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

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
FTP anonymous write commands are disabled - 3pts
FTP PASV security checks enabled - 3 pts
FTP anonymous user is not root - 3pts
Insecure permissions on FTP root directory fixed - 3pts

2017-18 State Round (Shared With Gold)

Vulns - 44/44 - 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
LOCAL POLICY CHECK - 2 pts
Ignore broadcast ICMP echo requests enabled - 2 pts
IPv4 TCP SYN,ACK 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
Unauthorized Samba share is disabled - 2 pts
Samba blank passwords are disabled - 2 pts
Samba SMB1 protocol is disabled - 2 pts

2017-18 Semifinals

Vulns - 40/52 - 76 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 Round 1

Vuln - 22/22 - 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

Vulns - 30/30 - 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 Platinum
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
- SMB share is not world writeable
- Encrypt smb traffic is enabled
- ntlm authentication is disabled
- SSH does not permit empty passwords

2018-19 Semifinals Ubuntu

Vulns - 30/30 - 100

Application security:
- SSH - PermitUserEnvironment No sshd_config
- SSH - Not Protocol 1 in sshd_config
- Firefox - Block dangerous and deceptive content

User Management:
- Remove user raven
- Remove user dusk
- Wildcat should not be admin
- Calamity must login with a password

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

Malware:
- /usr/lib/gvfs/gvfs-trash removed

Software:
- Minetest removed
- NBTscan removed

Prohibited files:
- Prohibited mp3 files

Application update:
- Sshd
- Firefox

Operating system update:
- bash
- Kernel
- Daily updates

Services:
- Postfix - removed
- Minetest - removed

Uncategorized operating system updates:
- /etc/shadow not world readable

Local Policies:
- Dmesg restrict set to 1
- Ipv4_forward contains 0(disable ipv4 forwarding)
- Sysrq is set to 0(disable sysrq)
- Xserver-allow-tcp disabled

Forensics:
- 1- 22,631,17071,17072,1707,30000

2- Frosty Flights

3- 38f3b03e-4415-43d2-bc22-1e1b12941c27

2018-19 Semifinals Debian

Vulns - 40/40 - 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
root- has a password
iwest- pass encrypted with a secure hash (MAYBE)
hwells- pass expires i think?
mrory- take out of sudo
debian user is removed

ACCOUNT POLICY:
password complexity - added gecoscheck to cracklib line
Secure hashing algerithm - 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 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 or 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 and /usr/share/wordpress/wp-login.php is removed

UNWANTED SOFTWARE:
Tcpspray
dsniff

MALWARE:
Perl and LPD are removed - /usr/bin/perl & /usr/bin/lpd &
/etc/systemd/system/multi-user.target.wants/lpd.service,
^ExecStart=/usr/bin/nohup\s+/usr/bin/lpd are removed

php backdoor /usr/share/wordpress/wp-admin/webroot.php is removed
/sbin/sforce SUID backdoor removed

APPLICATION SECURITY:

SQL bind address to localhost & skipnetworking
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 Round 1
Vulns - 17/17 - 100

Forensics 1 - Forensics
Unauthorized User 1 - User auditing
Unauthorized User 2 - User auditing
Unauthorized User 3 - User auditing
Changed user away from admin - User auditing
Changed insecure password - User auditing
Created new user - User Auditing
Default maximum password age is set - Account Policies
UFW Firewall is enabled - Defensive countermeasures
Apache2 Service has been removed - Service auditing
System auto checks for updates - Operating system updates
Important security updates downloaded - Operating system updates
OpenSSH has been updated - Application Updates
Removed plain text file containing passwords - Prohibited files
Removed Wireshark - Unwanted Software
Removed Zenmap and nmap - Unwanted Software
SSH Root Login disabled - Application Security Settings

2019-20 Round 2

Vulns - 30/30 - 100
Forensics 1 - Forensics
Forensics 2 - Forensics
Removed unauthorized user MrFreeze - User auditing
Removed unauthorized user joker - User auditing
Removed unauthorized user rghul - User auditing
User Harold is not an administrator - User auditing
User skyle is not an administrator - User auditing
Changed insecure password for user bgordon - User auditing
Created user ace - User auditing
A default maximum password age is set - Account Policies
A default minimum password age is set - Account Policies
IPv4 TCP SYN Cookies have been enabled - Local Policies
Ignore broadcast ICMP echo requests enabled - Local Policies
Sudo requires authentication - Local Policies
UFW protection enabled - Defensive Countermeasures
Insecure permissions on shadow file fixed - Uncategorized Operating System Settings
Apache2 service has been disabled or removed - Service Auditing
Postgresql has been disabled or removed - Service Auditing
The system automatically checks for updates daily - Operating System Updates
Install updates from important security updates - Operating System Updates
OpenSSH has been updated - Application Updates
7zip has been updated - Application Updates
Removed plain text file containing passwords - Policy Violation: Prohibited Files
Prohibited software Wireshark removed - Policy Violation: Unwanted Software
Prohibited Software Zenmap and Nmap removed - Policy Violation: Unwanted Software
Stellarium has been installed - Policy Violation: Unwanted Software
Prohibited software Freeciv removed - Policy Violation: Unwanted Software
Removed Netcat backdoor - Policy Violation: Malware
SSH Root Login has been disabled - Application Security Settings
Firefox displays warning on known malware sites - Application Security Settings

2019-2020 State Round

Vulns listed - 41/42 - 98/100

Forensics 1 - 5
Forensics 2 - 5
Forensics 3 - 5
Forensics 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
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

MISSING: 1
Uncategorized Operating System Settings - 1

2019-2020 Semifinals Round

DEBIAN 8

Forensic 1: f2e186fa-862a-423b-8faa-a4a840ac5602
Forensic 2: Catch me if you can!
Forensic 3: index.php
User Auditing Check Passed - change /bin/sh to /bin/false
User Auditing Check passes - script
User Auditing Check passes - script
User Auditing Check passes - script
User Auditing Check passes - script
Account Policy Check Passed - script
Account Policy Check Passed - script
Account Policy Check Passed - script
Account Policy Check Passed - script
Account Policy Check Passed - script
Local Policy Check Passed - script
Local Policy Check Passed - script
Local Policy Check Passed - script
Local Policy Check Passed - script
Local Policy Check Passed - Synack Retries 1-4 (script)
Service Auditing - script (Bind9)
Service Auditing - script (Nginx)
Service Auditing - script (MySQL)
Defensive countermeasure - script
Uncategorized Operating System Setting - script
Operating System Update Check Passed - uncommenting /etc/apt/sources.list
Operating System Update Check Passed - script
Operating System Update Check Passed - script
Application Update check passed - script
Application Update check passed - script
Malware check passed - remove index.php - REMOVE BACK END /bin/ls
Unwanted Software - Remove ophcrack (script)
Unwanted Software - Remove ettercap (script)
Unwanted Software - script (Wireshark)
Unwanted Software - script (chntpw)
Prohibited File - UNKNOWN
Application Security Check Passed - php modifications (expose_php set to off)
Application Security Check Passed - php modifications
Application Security Check Passed - Apache modifications
Application Security Check Passed - SSH Port change
Application Security Check Passed - script (SSH root maybe?)
Application Security Check Passed - script

2019-2020 Semifinals Round

UBUNTU 16

LIST VULNS AND HOW TO HERE:

Forensics 1 - espence, agabr, ggentile
Forensics 2 - Atlantis is Real!
Forensics 3 - Cosmo
User auditing check passed - Script
User auditing check passed - Script
User auditing check passed - Script
User auditing check passed - Script
User auditing check passed - REMOVE KPAULIS IN /ETC/PASSWD
Account Policy check passed - Script
Account Policy check passed - Script
Account Policy check passed - Script
Account Policy check passed - Script
Local Policy check passed - Script
Local Policy check passed - Script
Local Policy check passed - Script
Local Policy check passed - Script
Defensive Countermeasure - Script
Uncategorized Operating System Setting Check Passed - Script
Service Auditing - Script
Service Auditing - Script
Application Update check passed - Updates
Operating System Updates Check passed - Modify Updates requirements
Operating System update check passed - Updates
Operating System update check passed - Updates
Operating System update check passed - Updates
Application Update check passed - Updates
Prohibited file check passed - Script
Unwanted software check passed - Script
Unwanted software check passed - Script
Unwanted software check passed - Ettercap (Script)
Malware check passed - Netcat backdoor at /usr/local/games/nc
Application Security check passed - Remove Anonymous config in proftpd
Application Security check passed - Disable ServerIdent
Application Security check passed - Script (Firefox)
Application Security check passed - Uncomment ssl certificates for mysql
Application Security check passed - Set mysql bind-address to 127.0.0.1

Troy prac image scoring engin

```
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'))
```

```
vulns = []
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 SYN,ACK 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" ) )
```

```
vulns = []
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'))
```