CYBER PATRIOT XIV
NATIONAL FINALS COMPETITION

CYBERSECURITY
COOKEVILLE HIGH SCHOOL

Linux KaliPatriot Security Checklist

Written By Parker Johnson, Nathan Papa, and Landon Byrge for the CyberPatriot XIV National Finals Competition

Team Information

Team Nickname	TNPatriot | KaliPatriot
Landon Byrge	Team Leader, Windows Server, Active Directory DC, IIS
Nathan Papa	Linux, SQL, HTTP, FTP
John Reagan	Windows Server, IIS, SQL, File Sharing
Parker Johnson	Linux, HTTP, SMTP, SMB
Daniel Fleisig	Windows 10
Yaran Hassan	Windows 10
Team Number	14-0105
Unique ID	**TCKL-36PT-KQA5**
Web Based Login	**Username: 14-0105** **Password: TCKL-36PT-KQA5**
Reserved Passwords	● **CyberPatriotRul3z!**

Table of Contents

Tmux For Two Images

- sudo apt-get install tmux -y
- tmux (Prefix = Ctrl-B)
    - Split window into two vertically
        - Prefix-%
    - SSH into second box
    - Set synchronize panes
        - Prefix-: set synchronize-panes
            - Rerun command to disable
    - Move to logging setup when complete

Setup

- Firewall Rules
    - Figure out IP
        - ip addr
    - Figure out scored services on your machine
    - Base Configuration
        - apt-get install ufw
        - ufw disable
        - ufw logging high
        - ufw default deny incoming
        - ufw default deny outgoing
        - ufw allow out 80,443/tcp
        - ufw allow out 53
        - ufw allow in from 172.21.0.0/24 to 172.21.0.101-107
        - ufw allow out from 172.21.0.101-107 to 172.21.0.0/24
        - Do Service Rules
        - ufw enable (after doing service rules)
    - HTTP
        - ufw allow in 80/tcp
    - HTTPS
        - ufw allow in 443/tcp
    - MAIL
        - ufw allow in 25,110,995/tcp
    - FTP
        - ufw allow in 20,21/tcp
        - ufw allow out 20,21/tcp
    - SMB
        - ufw allow in 445, 139/tcp (Only if scored)
    - MySQL
        - ufw allow in 3306/tcp (Only if scored)

  - SSH
    - ufw allow in 22/tcp (Only if scored)
- Check if services have basic RCE’s, like ssh, etc
  - Web shells
    - grep -iRIE “(eval|base64_decode|system|exec|phpinfo)” /var/www/html
    - find /var/www/html -type f -name "*shell*.php”
    - find /var/www/html -type f -name "*backdoor*.php”
    - find /var/www/html -type f -name ".*.php”
  - Check virtual hosts
    - Check in ‘/etc/apache2/sites-enabled’
  - FTP
    - Delete unnecessary shares
      - ‘/srv/ftp’
  - SMB
    - Delete unnecessary shares
      - Check ‘/etc/samba/smb.conf’ for shares to delete
- Check sudoers file for vulnerabilities
  - Open ‘/etc/sudoers’ by running sudo visudo
    - Make sure no line contains either “!authenticate” or “NOPASSWD”, if a line contains “NOPASSWD:”, then remove the “NOPASSWD:”. If a line contains “!authenticate”, then delete the line.
    - Check all files in ‘/etc/sudoers.d/’ as well
  - sudo passwd -l root
- Setup Snoopy and fail2ban
  - Snoopy
    - Update Sources
      - software-properties-gtk
    - wget -O install-snoopy.sh https://github.com/a2o/snoopy/raw/install/install/install-snoopy.sh
    - chmod 755 install-snoopy.sh
    - ./install-snoopy.sh stable
      - sudo snoopy-enable
        - Restart scored services
      - snoopy.ini
        - output = file:/home/*/Documents/start-stop-daemon
  - fail2ban
    - apt-get install fail2ban
- Roll Credits
  - read; for u in $(cat /etc/passwd | grep -E "/bin/.*sh" | cut -d":" -f1); do echo "$u:$REPLY" | sudo chpasswd ; done
  - Check /etc/group
    - sudo

        - adm
        - lpadmin
    - Remove SSH keys
        - sudo find / -name authorized_keys
    - Web Server Admin Passwords
        - Login into website and change admin password through GUI
- Make script for restarting all scored services
    - while true; do sudo systemctl unmask [service]; sudo systemctl enable [service]; sudo systemctl start [service]; sleep 5; done
    - Throw above command in a file if it does not work
- Make backups on service config files
    - cp to /home/*/Documents

Tmux For Rest of Competition

- sudo apt-get install tmux -y
- tmux (Prefix = Ctrl-B)
- Logging Setup
    - Split window into two horizontally
        - Prefix-”
    - Split bottom again horizontally
        - Prefix-”
        - Setup snoopy in middle
            - sudo tail -f /home/*/Documents/start-stop-daemon | grep -v "ss -antp"
        - Setup ss command in bottom
            - watch -n 1 “sudo ss -antp”

Operating System Updates

- Run the following command to open the Gnome Apt Manager
    - software-properties-gtk
    - if it doesn't exist, install it
    - Configure Main and Contrib files
    - Configure security and automatic updates
- When closing, do NOT update the package lists

User Auditing

- Check /etc/password for the following:
    - unauthorized users
        - Any user with a uid above 1000 and not in the readme and not a service user like mysql or ftp
    - root users

        - Any non-root user with UID or GID 0
    - system users with login shells or hidden users
        - Any user with uid below 1000 with any sort of login shell like the following
            - /bin/bash
            - /bin/sh
            - /bin/zsh
            - /bin/dash
        - if the user is a default system account, change the shell
        - if the user is not a default system account and is unauthorized, change the uid and delete the user
    - password hashes
        - every account should have an “x” between the first and second :
- Check /etc/group for the following:
    - unauthorized admins(sudo adm lpadmin)
        - Check any administrative group for non admin users
    - nopasswdlogin
        - No user should be in this group
    - users in root group
        - no user should be in the root group
- Change the main user password to CyberPatriotRul3z!
- Check /etc/shadow for the following:
    - System users with password hashes
    - Root not locked out (!)
    - change main user password policies to 10:30:7
    - Copy hash and policies from main user to all unauthorized users
- If you have any issues with managing users, check for immutable or append only files and folders

Password Policies

- Run `sudo apt-get install libpam-cracklib -y`
- Open up ‘/etc/login.defs’
    - Find the lines that have “PASS_MAX_DAYS”
    - Change to the following:
        - “PASS_MAX_DAYS 30”
        - “PASS_MIN_DAYS 10”
        - “PASS_WARN_DAYS 7”

    - Find the line with “ENCRYPT_METHOD”
        - Change to “ENCRYPT_METHOD SHA512”
- common-auth
    - Should contain all of the following lines

```
auth    [success=1 default=ignore]    pam_unix.so
auth    requisite                     pam_deny.so
auth    required                      pam_permit.so
auth    optional                      pam_tally.so deny=5 unlock_time=900  onerr=fail audit
even_deny_root_account silent
```

- common-password

```
password      [success=1 default=ignore]    pam_unix.so obscure use_authtok sha512 shadow
remember=5
password      requisite                     pam_cracklib.so gecoscheck retry=5 minlen=10
difok=3 reject_username minclass=3 maxrepeat=2 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1
pam_pwhistory.so use_authtok remember=24 enforce_for_root
password      required                      pam_permit.so
password      optional        pam_gnome_keyring.so
```

Local Policies

- LightDM
    - Open ‘/etc/lightdm/lightdm.conf’, add the following lines:
            - [SeatDefaults]
            - user-session=ubuntu
            - greeter-hide-users=true
            - greeter-show-manual-login=true
            - allow-guest=false
            - greeter-allow-guest=false
            - autologin-user=none
            - autologin-guest=false
            - AutomaticLoginEnable=false
            - xserver-allow-tcp=false
        - Check other directories in ‘/etc/lightdm’, delete anything you see that is looks malicious
- GDM3
    - Open ‘/etc/gdm3/custom.conf’
        - Add the following lines under “[daemon]”:
            - AutomaticLoginEnable=false
            - AutomaticLogin=
            - TimedLoginEnable=false
            - TimedLogin=

        - TimedLoginDelay=10
        - [greeter]
        - IncludeAll=false
        - Exclude=bin,root,daemon,adm,lp,sync,shutdown,halt,mail,news,uucp,operator,nobody,nobody4,noaccess,postgres,pvm,rpm,nfsnobody,pcap
        - [security]
        - DisallowTCP=true
        - AllowRoot=false
        - AllowRemoteRoot=false
        - VerboseAuth=false
        - [xdmcp]
        - Enable=false
        - [chooser]
        - Broadcast=false
        - [debug]
        - Enable=true
    - Check /etc/pam.d/gdm-password for any lines that look bad, such as allowing root to login
- Check which sysctl are running with `sysctl -p`
    - Comment out currently running sysctl’s
    - Add the following lines to the end of ‘/etc/sysctl.conf’:
        - net.ipv4.icmp_echo_ignore_all=1
        - net.ipv4.icmp_echo_ignore_broadcasts=1
        - net.ipv4.icmp_ignore_bogus_error_responses=1
        - net.ipv4.tcp_syncookies=1
        - net.ipv4.tcp_synack_retries = 2
        - net.ipv4.ip_forward=0
        - net.ipv4.conf.all.forwarding=0
        - net.ipv4.conf.default.forwarding=0
        - net.ipv4.conf.all.accept_redirects=0
        - net.ipv6.conf.all.accept_redirects=0
        - net.ipv4.conf.all.send_redirects=0
        - net.ipv4.conf.default.send_redirects=0
        - kernel.randomize_va_space=2
        - net.ipv4.tcp_rfc1337=1
        - net.ipv4.conf.default.rp_filter = 0
        - net.ipv4.conf.all.rp_filter = 1
        - kernel.dmesg_restrict=1
        - kernel.sysrq = 0

        - net.ipv4.conf.all.log_martians=1
        - net.ipv4.conf.default.log_martians=1
        - net.ipv4.conf.default.accept_source_route=0
        - net.ipv4.conf.all.accept_source_route=0
        - kernel.unprivileged_userns_clone=0
        - kptr_restrict=0
    - Run `sysctl -p` to apply them

Uncategorized Operating System Settings

- Set sticky bit on world writable directories
    - `df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d -perm -0002 2>/dev/null | xargs chmod a+t`
- Open ‘/etc/fstab’ and add the following line to the bottom of it:
    - none   /run/shm   tmpfs   noexec,nosuid,nodev   0   0
    - none /proc proc rw,nosuid,nodev,noexec,relatime,hidepid=2 0 0
    - /tmp   /var/tmp   none   rw,nodev,noexec,nosuid,bind   0 0
    - none   /dev/shm   tmpfs   rw,nodev,noexec,nosuid,size=5G 0 0
        - run `mount -a` to apply changes
- Grub Bootloader
    - Ensure the file ‘/etc/default/grub’ does not have the line “noexec=off”
    - Secure Grub Bootloader by following these steps:
        - Install/update grub by running `apt-get install grub-common -y`
        - Run `grub-mkpasswd-pbkdf2` and enter in any password (e.g. “CyberPatriotRul3z!”)
        - The password hash starting with grub.pbkdf will be used below
        - Add the following lines to ‘/etc/grub.d/40_custom’
            - “set superusers="root"”
            - “password_pbkdf2 root {password hash from above}”
        - Run `update-grub` to set these settings
    - Change /etc/grub/defaults
        - GRUB_CMDLINE_LINUX="audit=1 audit_backlog_limit=8192 apparmor=1 security=apparmor"
- Make sure ‘/etc/rc.local’ only contains “exit 0”, if it does not, it may lead to a backdoor
- Edit ‘/etc/host.conf’ to include the following:
    - nospoof on
    - order hosts,bind
- Ensure ‘/root/.profile/’ does not have any malicious commands in the file

Service Auditing

- Start the sudo rsyslog, systemd-journald, and apparmor services
  - sudo systemctl unmask {service}
  - sudo systemctl enable {service}
  - sudo systemctl start {service}
- Check for any unnecessary services
- purge the services

Application Updates

- Make sure that ALL programs or services mentioned in the readme are updated. DOUBLE AND TRIPLE CHECK

Prohibited Files

- Use the following commands to find every world readable and writable file:
  - find / -perm -o=r | grep "/etc"
  - find / -perm -o=w | grep "/etc"
- Download fsearch
  - sudo add-apt-repository ppa:christian-boxdoerfer/fsearch-stable
  - sudo apt-get update
  - sudo apt install fsearch
    - Go to preferences and then add '/' to the database
    - Then search for ".<extension>" in the search bar
- Search for files with a specific extension
  - find / -name "*.{extension}"

Prohibited Software

- Use the GUI to find basic program installed on the image
  - Use the command dpkg -l to find a list of every installed package
- Run the following command to check for software that was installed on the system
  - ps -ef --forest
- Go through '/var/logs/auth.log*' again to see what CyberPatriot installed
- Run the following command
  - (zcat $(ls -tr /var/log/apt/history.log*.gz); cat /var/log/apt/history.log) 2>/dev/null | egrep '^(Start-Date:|Commandline:)' | grep -v aptdaemon | egrep -B1 '^Commandline:'
- Remove any games directories
  - rm -rf /usr/lib/games

- rm -rf /usr/local/games
- rm -rf /usr/share/games
- rm -rf /var/games
- rm -rf /var/lib/games

Malware

- View all Running processes
  - `ps -eaf --forest`
- Run this command to find any python backdoors
  - `sudo ps -aux | grep python`
    - You can do the same thing for perl backdoors by replacing `python` with `perl`
- Use either `sudo netstat -tulpn` or `sudo lsof -i` to scan for listening ports
  - If you found a suspicious program, use the `whereis` command to find the directory of the program
- Find Web Shells
  - `cd /var/www/html`
  - `grep '((eval.*(base64_decode|gzinflate|\$_))|\$[0O]{4,}|FilesMan|JGF1dGhfc|IIIl|die\(PHP_OS|posix_getpwuid|Array\(base64_decode|document\.write\("\\u00|sh(3(ll|11)))' . -lroE --include=*.php*`
- Find all SUID files
  - `sudo find / -perm -4000 -type f 2>/dev/nullc`
    - Compare the output list to GTFOBins
      - https://gtfobins.github.io/
    - Run this command on certain files that was outputted
      - `chmod u-s /file/path`
- Delete red team binaries with:
  - sudo chattr +i “filename”; sudo killall “filename”; sudo rm “filename”; touch “filename”; sudo chattr -i “filename”
    - With “killall” command, use the filename only, not just the filepath.

Application Security Settings

FTP

- VSFTPD
  - VSFTPD configurations can be configured in '/etc/vsftpd.conf'
  - Change the following things:
    - "listen=NO"
    - "listen_ivp6=NO"
    - "anonymous_enable=NO"
    - "local_enable=YES"
    - "anon_upload_enable=NO"
    - "anon_mkdir_write_enable=NO"
    - "chroot_local_user=YES"
    - "chroot_list_enable=YES"
    - xferlog_enable=YES
    - xferlog_file=/var/log/vsftpd.log
    - xferlog_std_format=NO
  - Add the following:
    - anon_world_readable_only=YES
    - anon_world_readable_only=YES
    - passive-promiscuous=no
    - pasv-enable=yes
    - port-promiscuous=no
    - port-enable=yes
    - hide_ids = yes
    - log_ftp_protocol=YES
- PureFTPd
  - PureFTPd can be configured in '/etc/pure-ftpd/pure-ftpd.conf'
  - Add/change the following things:
    - "ChrootEveryone yes"
    - "NoAnonymous yes"
    - "AnonymousOnly no"
    - "TLS 2"
    - "MaxClientsNumber 50"
    - "MaxClientsPerIP 3"
    - "MaxIdleTime 10"
    - "LimitRecursion 500 8"
    - "Umask 133:022"
    - "MaxClientsPerIP 2"
    - "VerboseLog yes"

- ProFTPd
    - Pro FTPd can be configured in '/etc/proftpd/proftpd.conf'
    - Add/change the following things:
        - "TLSEngine on
        - "TLSLog /var/log/proftpd/tls.log
        - "TLSProtocol SSLv23
        - "TLSRequired on"
        - "TLSVerifyClient off"
        - "TLSOptions NoCertRequest EnableDiags NoSessionReuseRequired"
        - ServerIdent off

SSH

- OpenSSH
    - OpenSSH can be configured in '/etc/ssh/sshd_config'
    - Change the following things:
        - Protocol 2
        - PermitRootLogin no
        - StrictModes yes
        - PubkeyAuthentication yes
        - HostBasedAuthentication no
        - IgnoreRhosts yes
        - PasswordAuthentication no
        - PermitEmptyPasswords no
        - UsePAM yes
        - AllowTcpForwarding no
        - GatewayPorts no
        - X11Forwarding no
        - PermitTTY no
        - PrintMotd no
        - LoginGraceTime 30
        - PrintLastLog no
        - TCPKeepAlive no
        - PermitUserEnvironment no
        - ClientAliveInterval 300
        - ClientAliveCountMax 0
    - Add the following things:
        - UsePrivilegeSeparation yes

- AuthenticationMethods publickey
- MaxAuthTries 3

SMB

- Samba
  - Samba can be configured in ‘/etc/samba/smb.conf’
  - Change the following things:
    - obey pam restrictions = yes
    - usershare allow guests = no
  - Add the following:
    - ntlm auth = 0
    - smb encrypt = required
    - restrict anonymous = 2
    - min protocol = SMB2
    - server signing = mandatory
    - encrypt passwords = yes
    - null passwords = no
    - syslog = 10
    - encrypt passwords = yes
    - guest account = nobody
    - guest ok = no
    - Add/change the following depending on the readme
      - “browseable = no”
      - “read only = yes”
      - “writeable = no”
  - Check inside the share for bad files (DELETE THEM FROM THE SHARE LOCATION NOT THE NETWORK LOCATION)

HTTP

- Apache2
  - Apache2 can be configured in ‘/etc/apache2/apache2.conf’
  - Add/change the following:
    - “KeepAlive Off”
    - “ServerSignature Off”
    - “FileETag None”

    - “ServerTokens Prod”
    - “TraceEnable Off”
    - “Options -FollowSymLinks”
    - In <Directory /var/www/html>, Add/Change:
      - Options -Indexes
    - In <Directory />
      - “Order Deny,Allow”
      - “Deny from all”
      - “Options None”
      - “AllowOverride None”
- Nginx
  - Open nginx.conf
    - Add/edit the following lines in http{}
      - “server_tokens off”
      - Find the line with “ssl_protocols”
        - Remove any versions that are not “TLSv1.2” or “TLSv1.3”
    - Add/edit the following lines in server{}
      - add_header X-Frame-Options "SAMEORIGIN"
      - add_header Strict-Transport-Security max-age=31536000; includeSubdomains; preload";
      - add_header Content-Security-Policy "default-src 'self' http: https: data: blob: 'unsafe-inline'" always;
      - add_header X-XSS-Protection "1; mode=block";
      - ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA HIGH !RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS";
    - Disable TRACE and DELETE HTTP methods
      - Go to the line that has “if ($request_method !~” and remove TRACE and DELETE if there

SQL

- MySQL

  - MySQL can be configured in ‘/etc/mysql/my.cnf’
  - mysql_secure_installation
  - Ensure the line is “user =” is set to “mysql”
  - Add/change the following:
    - bind-address=localhost
    - local-infile=0
    - default_password_lifetime=30
    - symbolic-links = 0
- MariaDB
  - Same as MySQL
- PostgreSQL
  - PostgreSQL can be configured at ‘/etc/postgresql/*/main/postgresql.conf’
  - Add/change the following:
    - “max_connections = 100”
    - “authentication_timeout = 1min”
    - “password_encryption = scram-sha-256”
    - “db_user_namespace = off”
    - “ssl = on”
    - ssl_cert_file = 'server.crt'
    - ssl_key_file = 'server.key'
    - ssl_prefer_server_ciphers = on
    - logging_collector = on
    - log_directory = /var/log/postgres
    - log_hostname = on
    - log_connections = on
    - log_disconnections = on
    - log_error_verbosity = default
- pg_hba.conf
  - hostnossl all all 0.0.0.0/0 reject
  - If a line has trust in it, replace trust with krb5
- pg_user_mappings
  - Make sure there are no insecure user mappings. Delete the line or file if you don’t need any user mappings.
- MongoDB
  - MongoDB can be configured at ‘/etc/mongod.conf’
  - Add/change the following:
    - Under “systemLog:”, add
      - “verbosity: 5”
    - Under “security:”, add
      - authorization: “enabled”

SMTP

- Postfix
    - Postfix can be configured in "/etc/postfix/main.cf"
    - Add/change the following:
        - mail_owner = postfix
        - smtp_address_preference = ipv4
        - inet_protocols = ipv4
        - html_directory = no
        - disable_vrfy_command=yes
        - inet_interfaces=loopback-only
        - mynetworks = 0.0.0.0/0
        - myhostname = ubuntu.lan
        - mydestination = ubuntu.lan, localhost, localhost.lan
        - smtp_dns_support_level = disabled
        - smtpd_sasl_local_domain = $myhostname
        - smtpd_helo_required=yes
        - smtp_sasl_auth_enable = yes
        - smtp_sasl_security_options = noanonymous
        - smtp_use_tls = yes
        - smtp_tls_loglevel=1
        - broken_sasl_auth_clients = yes
        - smtpd_sasl_auth_enable = yes
        - smtpd_tls_received_header = yes
        - smtp_tls_security_level = may
        - smtpd_tls_security_level = may
        - smtp_tls_note_starttls_offer = yes
        - smtpd_data_restrictions = reject_unauth_pipelining
- Dovecot
    - Dovecot can be configured in "/etc/dovecot/dovecot.conf"
    - Add/change the following:
        - ssl = yes
        - ssl_verify_client_cert = no
        - ssl_ca =
        - ssl_protocols = TlSv1.2
        - ssl_cipher_list = EECDH+AESGCM:EDH+AESGCM
        - ssl_prefer_server_ciphers
- Roundcube
- Exim
    - Exim can be configured in " /etc/exim4/exim4.conf.template"

        - Add/change the following:
            - MAIN_TLS_ENABLE = true
            - dc_eximconfig_configtype=’satellite’
            - dc_other_hostnames=’localhost;domain.com’
            - dc_local_interfaces=’127.0.0.1′
            - dc_readhost=’domain.com’
            - dc_relay_domains=”
            - dc_minimaldns=’false’
            - dc_relay_nets=”
            - dc_smarthost=’smtp.gmail.com::587′
            - CFILEMODE=’644′
            - dc_use_split_config=’true’
            - dc_hide_mailname=’true’
            - dc_mailname_in_oh=’true’
            - dc_localdelivery=’mail_spool’

VPN

- OpenVPN
    - OpenVPN can be configured in “/etc/openvpn/server/server.conf”
    - Add/change the following:
        - ”proto udp”
        - “dev tun”
        - ”chroot jail”
        - ”cipher AES-256-CBC”
        - “auth SHA256”
        - “user nobody”
        - “group nogroup”
        - “verb 9”

PHP

- PHP
    - Find the php.ini file by using the command `php -i | grep “php.ini”`
    - Edit this file for the following:
        - Add all of the following:
            - expose_php = Off
            - display_errors = Off
            - log_errors = On
            - track_errors = Off

        - html_errors = Off
        - cgi.force_redirect=On
        - file_uploads = On
        - allow_url_fopen = Off
        - allow_url_include = Off
        - safe_mode=On
        - mail.add_x_header = Off
        - sql.safe_mode = On
        - session.use_strict_mode = 1
        - register_globals=off
    - Make sure the line with “disable_functions” includes the following functions:
        - Exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source
    - Make sure that “open_basedir= {}“ is **ONLY** equal to “/var/www/html”
        - If it is set to any other directory like /var/www, or /tmp or /etc, change it to “/var/www/html”
- Check all the files in the apache2 web directory for phpinfo() functions

Firefox

- Inside of ‘/usr/lib/firefox/defaults/pref/local-settings.js’, put the following:
    - “// local-settings.js” MAKE SURE THE FIRST LINE IS A COMMENT
    - “pref("general.config.filename", "mozilla.cfg");”
    - “pref("general.config.obscure_value", 0);”
- Add all of the following lines to ‘/usr/lib/firefox/mozilla.cfg’:

```
"lockPref("browser.safebrowsing.downloads.enabled", true);"
"lockPref("dom.disable_open_during_load", true);"
"lockPref("xpinstall.whitelist.required", true);"
"lockPref("app.update.enabled", true);"
"lockPref("app.update.auto", true);"
"lockPref("privacy.donottrackheader.enabled", true);"
"lockPref("browser.safebrowsing.downloads.remote.block_potentially_unwanted", true);"
"lockPref("browser.safebrowsing.downloads.remote.block_uncommon", true);"
"lockPref("browser.safebrowsing.malware.enabled", true);"
"lockPref("browser.safebrowsing.phishing.enabled", true);"
```

Prohibited Software List

- 4g8
- abc
- acccheck
- ace-voip
- acquisition
- airbase-ng
- aircrack
- aircrack-ng
- amap
- android-sdk
- apache-users
- apktool
- aquisition
- arachni
- arduino
- aria2
- armagetron
- armitage
- arp-scan
- asleap
- automater
- backdoor-factory
- bbqsql
- bed
- beef
- bestat
- bind9
- bing-ip2hosts
- binwalk
- bitcomet
- bitlet
- bitspirit
- bittorrent
- blindelephant
- bluelog
- bluemaho
- bluepot
- blueranger
- bluesnarfer
- braa
- bulk-extractor
- bully
- burpsuite
- capstone
- casefile
- cdpsnarf
- cewl
- chntpw
- cisco-auditing-tool
- cisco-global-exploiter
- cisco-ocs
- cisco-router-config
- cisco-torch
- cl-irc
- cmospwd
- commix
- cookie-cadger
- copy-router-config
- cowpatty
- crack
- crackle
- creddump
- crunch
- cryptcat
- ctorrent
- cuckoo
- cupp3
- cutycapt
- cymothoa
- cyphesis
- davtest
- dbd
- dbpwaudit
- dc3dd
- ddrescue
- deblaze
- deluge
- dex2jar

- dff
- dhclient
- dhcpig
- dictstat
- dirb
- dirbuster
- distorm3
- dmitry
- dnmap
- dns2tcp
- dnschef
- dnsenum
- dnsmap
- dnsrecon
- dnstracer
- dnswalk
- doona
- dos2unix
- dotdotpwn
- dradis
- dsniff
- dumpzilla
- eapmd5pass
- edb-debugger
- ember
- endless-sky
- enum4linux
- enumiax
- ettercap
- exploitdb
- extundelete
- fern-wifi-cracker
- fierce
- fiked
- fimap
- findmyhash
- firewalk
- foremost
- fragroute
- freeciv
- freeciv-client-extras
- freeciv-client-gtk
- freeciv-data
- freeciv-server
- frostwise
- funkload
- galleta
- gameconqueror
- ghost-fisher
- giskismet
- go-lismero
- goofile
- gpp-decrypt
- gqrx
- gr-scan
- grabber
- gsad
- gsd
- guymager
- hamster-sidejack
- hash-identifier
- heartbleeder
- hexinject
- hexorbase
- hping3
- http-tunnel
- httptunnel
- hunt
- hydra
- hydra-gtk
- iaxflood
- icmp
- inguma
- inspircd
- intersect
- intrace
- inundator
- inviteflood
- iphone-backup-analyzer
- ipscan

- ipv6-toolkit
- irc
- irssi
- ismtp
- isr-evilgrade
- jad
- javasnoop
- jboss-autopwn
- jd-gui
- john
- johnny
- joomscan
- jsql
- kalibrate-rtl
- keepnote
- keimpx
- killerbee
- kismet
- knocker
- ktorrent
- lcrack
- ldb
- linux-exploit-suggester
- linuxdcpp
- lpd
- lynis
- magictree
- maltego-teeth
- manaplus
- maskgen
- maskprocessor
- masscan
- mdk3
- medusa
- metagoofil
- metasploit
- mfcuk
- mfoc
- mfterm
- minetest
- minetest-server
- miranda
- mitmproxy
- multiforcer
- multimon-ng
- nbtscan
- nc
- ncrack
- netcat
- netcat-minimal
- netcat-openbsd
- netcat-traditional
- netcat-ubuntu
- netdiag
- netris
- nfs
- nfs-common
- nfs-kernel-server
- nikto
- nipper-ng
- nishang
- nmap
- nmdb
- ntop
- oclgausscrack
- ohwurm
- ollydpg
- openarena
- openra
- openvas-administrator
- openvas-cli
- openvas-manager
- openvas-scanner
- ophcrack
- oscanner
- p0f
- padbuster
- paros
- parsero
- patator

- pdf-parser
- pdfid
- pdgmail
- peepdf
- phrasendrescher
- pipal
- pixiewps
- plecost
- polenum
- policygen
- pop3
- portmap
- postfix
- postgres
- postgresql
- powerfuzzer
- powersploit
- protos-sip
- proxystrike
- pryit
- pwnat
- python-scapy
- qbittorrent
- rcrack
- rcrack-mt
- reaver
- rebind
- recon-ng
- redfang
- regripper
- remmina
- responder
- rfdump
- ridenum
- rsmangler
- rsync
- rtlsdr-scanner
- rtorrent
- rtpbreak
- rtpflood
- rtpinsertsound
- rtpmixsound
- sakis3g
- sbd
- sctpscan
- setoolkit
- sfuzz
- shellnoob
- sidguesser
- siparmyknife
- sipp
- sipvicious
- skipfish
- slowhttptest
- smali
- smtp-user-enum
- sniffjoke
- snmp
- snmpcheck
- snmpd
- snort
- spooftootph
- sqldict
- sqlmap
- sqlninja
- sqlsus
- squid
- sslcaudit
- sslsplit
- sslstrip
- sslyze
- statprocessor
- t50
- tcpdump
- tcpspray
- telnet
- telnet-server
- telnetd
- termineter
- thc-hydra

- thc-ipv6
- thc-pptp-bruter
- thc-ssl-dos
- theharverster
- tightvnc
- tightvnc-common
- tightvncserver
- tixati
- tlssled
- tnscmd10g
- tomcat
- tomcat6
- torrent
- transmission-bittorrent-client
- transmission-common
- transmission-gtk
- truecrack
- twofi
- u3-pwn
- uatester
- uniscan
- unix-privesc-check
- up.time
- uptimeagent
- urlcrazy
- utorrent
- valgrind
- vega
- vino
- vnc4server
- vncserver
- voiphopper
- volatility
- vuse
- w3af
- webscarab
- webshag
- webshells
- webslayer
- websploit
- weevely
- weplab
- wesnoth
- wfuzz
- wifi-honey
- wifitap
- wifite
- winexe
- wireshark
- wol-e
- wordlists
- wpscan
- xplico
- xprobe
- xspy
- xsser
- yara
- yersinia
- zaproxy
- zenmap

Injects

SSH

- What is asked:
    - Add a user to the system, ensure SSH is running and externally accessible, and allow the user to SSH into the system with a public key.
- How to solve:
    - Check/Change “PubkeyAuthentication yes” (sshd_config)
    - Check/Change “UsePAM no” (sshd_config)
    - Check/Change “PasswordAuthentication no” (sshd_config)
    - Check/Change “AllowUsers user_name” (sshd_config)
    - Create new user
    - New user must own their .ssh directory with the keys in them.
        - chown user:user /home/{user}/.ssh/
        - chown user:user /home/{user}/.ssh/authorized_keys
    - Put keys in the right places
        - pubkey - /.ssh/authorized_keys
            - Change file perms (600)
    - Make sure the key files are linked in sshd_config (~/.ssh/authorized_keys)
    - sudo systemctl restart sshd

HTTP

- What is asked:
    - Set up HTTP service, set up file share, enable anonymous read
- How to solve:
    - cd to correct directory
    - python3 -m http.server 80

FTP

- What is asked:
    - Enable anonymous FTP, setup FTP service shared directory
- How to solve:
    - sudo apt-get install vsftpd -y
    - Add vsftpd to the service start/unmask/enable one liner
    - ‘/etc/vsftpd.conf’
        - anonymous_enable = yes
        - local_root = “shared_directory”
        - “anon_world_readable_only=YES”
        - “anon_world_readable_only=YES”
        - “anon_upload_enable=NO”

        - "anon_mkdir_write_enable=NO"

SSL

- What is asked:
    - Enable HTTPS using a self-signed SSL/TLS certificate for the e-commerce site.
- How to solve:
    - Nginx
        - sudo apt install ssl-cert -y
            - ssl-cert will install the public key at /etc/ssl/certs/ssl-cert-snakeoil.pem
            - and the private key at /etc/ssl/private/ssl-cert-snakeoil.key
            - ssl-cert will install configuration at /etc/nginx/snippets/snakeoil.conf
        - sudo nano /etc/nginx/sites-enabled/SITE
            - "server {
                - listen 443 ssl;
                - listen [::]:443 ssl;
                - include snippets/snakeoil.conf;
        - sudo systemctl nginx restart
    - Apache2
        - sudo a2enmod ssl
        - sudo a2ensite default-ssl
        - sudo systemctl restart apache2