Troy CheckList 2018

Key

- Anything in text like `this` is a command to be typed in terminal
- Anything in single quotes is a file or directory path
  - ‘/etc/shadow’
- Anything in double quotes is a line to be added to a file

Operating System Updates

- Start out by going into the settings and enabling automatic updates, and security updates.
- Check if ‘/etc/apt.d/sources.list’ has valid repositories.
- Run `sudo apt-get update -y` and `sudo apt-get update -y`

User Auditing

- Run the following:
  - `chattr -i /etc/passwd`
  - `chattr -i /etc/shadow`
  - `chattr -i /etc/group`
- Start out by doing user auditing in the GUI.
  - Go to Settings and user accounts.
  - Unlock the gui
  - Delete all unauthorized users
  - Make all unauthorized admins standard users
  - add any users you need to
- Next check ‘/etc/passwd’ for the following things:
  - Users with a uid of 0
    - eg: paul:x:0:1012
  - Any unauth users with uids 1000-60000
  - If any accounts with a uid from 1-1000 and have a login shell (i.e. ‘/bin/sh’ ‘/bin/bash’ ‘/bin/rbash’ ‘/bin/dash’ /usr/bin/tmux’ ‘/usr/bin/screen’) Then follow the steps below:
    - Research the user, is it supposed to exist?
    - If yes, change the login shell to ‘/bin/false’
    - if no, then delete the user by removing the line in the file.

- run sudo -l root
- Next open '/etc/shadow' to check for the following:
    - any authorized users(uid 1000-60000) for incorrect password expiring. No users should have :99999: in their line.
- DO PASSWORD POLICIES BEFORE CONTINUING HERE
- Now, set every users password using the following commands:

```
for user in $(sudo sed 's/:.*//' /etc/passwd);
do
    if [[ $(sudo id -u $user) -ge 999 && "$user" != "nobody" && "$users" != "$SUDO_USER" ]]
    then
        (echo "CyberPatriot1!"; echo "CyberPatriot1!") | sudo passwd "$user"
    fi
done
```

- This will change your password as well to CyberPatriot1!
- Look in '/etc/group' for the following
    - Check that all of the following groups only contain admins if they exists
        - sudo
        - admins
        - adm
        - any other groups that have something to do with administration
    - Delete the line that starts with "nopasswdlogin"
- Check in '/etc/shadow' again for the following:
    - Users that still don't have a password
    - root having "root::" instead of "root:!:"
    - Users having "$1" in front of their password hash instead of "$6"
- The Readme may specify creating users/groups, here are the commands for each:
    - To create a user: sudo useradd -p CyberPatriotRul3z! {username}
    - To create a group: sudo groupadd {groupname}
    - To add a user to a group: sudo usermod -a -G {groupname} {username}

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 it to “ENCRYPT_METHOD SHA512”
- Open up ‘/etc/pam.d/common-auth’
    - If you see nullok anywhere in this file, delete it
    - Add the following line to the end of the file:

“auth optional pam_tally.so deny=5 onerr=fail unlock_time=900 audit even_deny_root_account silent”

- Open up ‘/etc/pam.d/common-password’
    - Add the following 2 lines to the file:

“password requisite pam_cracklib.so retry=3 minlen=10 difok=3 ucredit=1 lcredit=1 dcredit=1 ocredit=1”
“password requisite pam_pwhistory.so use_authtok remember=24 enforce_for_root”

    - If nullok is anywhere in the file, then delete it
    - if md5 is anywhere in the file, replace it with sha512
    - Add “remember=5”, “sha512”, and “obscure” to the end of the line with unix.so in it

Local Policies

- Open ‘/etc/lightdm/lightdm.conf’
    - Add the Following lines
        - “allow-guest=false”
        - “greeter-hide-users=true”
        - “greeter-show-manual-login=true”
        - “autologin-user=none”
        - “xserver-allow-tcp=false”
- Next we will configure sysctl
- Edit ‘/etc/sysctl.conf’ with the following lines:
    - Common Scored Values:
        - "net.ipv4.conf.all.send_redirects=0"
        - "net.ipv4.conf.default.send_redirects=0"
        - "kernel.dmesg_restrict=1"
        - "net.ipv4.tcp_synack_retries = 2"
        - "net.ipv4.tcp_rfc1337=1"
        - "kernel.unprivileged_userns_clone=0"
        - "net.ipv4.ip_forward=0"
        - "kernel.sysrq = 0"
        - "net.ipv4.tcp_syncookies=1"
        - "kernel.randomize_va_space=2"
        - "fs.suid_dumpable=0"

        - "net.ipv6.conf.all.disable_ipv6=1"
        - "net.ipv4.icmp_echo_ignore_all=1"
        - "net.ipv4.icmp_echo_ignore_broadcasts=1"
        - "net.ipv4.icmp_ignore_bogus_error_responses=1"
    - Other Value That Might Be Scores:
        - fs.file-max=65535
        - fs.protected_hardlinks=1
        - fs.protected_symlinks=1
        - kernel.core_uses_pid=1
        - kernel.ctrl-alt-del=0
        - kernel.kptr_restrict=2
        - kernel.maps_protect=1
        - kernel.msgmax=65535
        - kernel.msgmnb=65535
        - kernel.pid_max=65535
        - kernel.shmall=268435456
        - kernel.shmmax=268435456
        - net.core.default_qdisc=fq
        - net.core.dev_weight=64
        - net.core.netdev_max_backlog=16384
        - net.core.optmem_max=65535
        - net.core.rmem_default=262144
        - net.core.rmem_max=16777216
        - net.core.somaxconn=32768
        - net.core.wmem_default=262144
        - net.core.wmem_max=16777216
        - net.ipv4.conf.all.accept_redirects=0
        - net.ipv4.conf.all.accept_source_route=0
        - net.ipv4.conf.all.bootp_relay=0
        - net.ipv4.conf.all.forwarding=0
        - net.ipv4.conf.all.log_martians=1
        - net.ipv4.conf.all.proxy_arp=0
        - net.ipv4.conf.all.rp_filter=1
        - net.ipv4.conf.all.secure_redirects=0
        - net.ipv4.conf.default.accept_redirects=0
        - net.ipv4.conf.default.accept_source_route=0
        - net.ipv4.conf.default.forwarding=0
        - net.ipv4.conf.default.log_martians=1
        - net.ipv4.conf.default.rp_filter=1
        - net.ipv4.conf.default.secure_redirects=0
        - net.ipv4.conf.lo.accept_redirects=0

- net.ipv4.conf.lo.accept_source_route=0
- net.ipv4.conf.lo.log_martians=0
- net.ipv4.conf.lo.rp_filter=1
- net.ipv4.ip_local_port_range=2000 65000
- net.ipv4.ipfrag_high_thresh=262144
- net.ipv4.ipfrag_low_thresh=196608
- net.ipv4.neigh.default.gc_interval=30
- net.ipv4.neigh.default.gc_thresh1=32
- net.ipv4.neigh.default.gc_thresh2=1024
- net.ipv4.neigh.default.gc_thresh3=2048
- net.ipv4.neigh.default.proxy_qlen=96
- net.ipv4.neigh.default.unres_qlen=6
- net.ipv4.route.flush=1
- net.ipv4.tcp_congestion_control=htcp
- net.ipv4.tcp_ecn=1
- net.ipv4.tcp_fastopen=3
- net.ipv4.tcp_fin_timeout=15
- net.ipv4.tcp_keepalive_intvl=15
- net.ipv4.tcp_keepalive_probes=5
- net.ipv4.tcp_keepalive_time=1800
- net.ipv4.tcp_max_orphans=16384
- net.ipv4.tcp_max_syn_backlog=2048
- net.ipv4.tcp_max_tw_buckets=1440000
- net.ipv4.tcp_moderate_rcvbuf=1
- net.ipv4.tcp_no_metrics_save=1
- net.ipv4.tcp_orphan_retries=0
- net.ipv4.tcp_reordering=3
- net.ipv4.tcp_retries1=3
- net.ipv4.tcp_retries2=15
- net.ipv4.tcp_rmem=8192 87380 16777216
- net.ipv4.tcp_sack=0
- net.ipv4.tcp_slow_start_after_idle=0
- net.ipv4.tcp_syn_retries=5
- net.ipv4.tcp_timestamps=1
- net.ipv4.tcp_tw_recycle=0
- net.ipv4.tcp_tw_reuse=1
- net.ipv4.tcp_window_scaling=0
- net.ipv4.tcp_wmem=8192 65536 16777216
- net.ipv4.udp_rmem_min=16384
- net.ipv4.udp_wmem_min=16384
- net.ipv6.conf.all.accept_ra=0

        - net.ipv6.conf.all.accept_redirects=0
        - net.ipv6.conf.all.accept_source_route=0
        - net.ipv6.conf.all.autoconf=0
        - net.ipv6.conf.all.forwarding=0
        - net.ipv6.conf.default.accept_ra=0
        - net.ipv6.conf.default.accept_ra_defrtr=0
        - net.ipv6.conf.default.accept_ra_pinfo=0
        - net.ipv6.conf.default.accept_ra_rtr_pref=0
        - net.ipv6.conf.default.accept_redirects=0
        - net.ipv6.conf.default.accept_source_route=0
        - net.ipv6.conf.default.autoconf=0
        - net.ipv6.conf.default.dad_transmits=0
        - net.ipv6.conf.default.disable_ipv6=1
        - net.ipv6.conf.default.forwarding=0
        - net.ipv6.conf.default.max_addresses=1
        - net.ipv6.conf.default.router_solicitations=0
        - net.ipv6.conf.lo.disable_ipv6=1
        - net.ipv6.ip6frag_high_thresh=262144
        - net.ipv6.ip6frag_low_thresh=196608
        - net.ipv6.route.flush=1
        - net.unix.max_dgram_qlen=50
        - vm.dirty_background_ratio=5
        - vm.dirty_ratio=30
        - vm.min_free_kbytes=65535
        - vm.mmap_min_addr=4096
        - vm.overcommit_memory=0
        - vm.overcommit_ratio=50
        - vm.swappiness=30

Uncategorized Operating System Settings

- 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.
- Delete all files in the directory ‘/etc/sudoers.d/’ using the command: `sudo rm -rf /etc/sudoers.d/`
- Set the secure permissions on the following files using the commands listed:
    - `chown root:root /etc/fstab`
    - `chmod 644 /etc/fstab`
    - `chown root:root /etc/group`
    - `chmod 644 /etc/group`

  - chown root:root /etc/shadow
  - chmod 400 /etc/shadow
  - chown root:root /etc/apache2
  - chmod 755 /etc/apache2
  - chmod 0600 /etc/securetty
  - chmod 644 /etc/crontab
  - chmod 640 /etc/ftpusers
  - chmod 440 /etc/inetd.conf
  - chmod 440 /etc/xinetd.conf
  - chmod 400 /etc/inetd.d
  - chmod 644 /etc/hosts.allow
  - chmod 440 /etc/sudoers
  - chmod 640 /etc/shadow
  - chmod 600 /boot/grub/grub.cfg
  - chmod 600 /etc/ssh/sshd_config
  - chmod 600 /etc/gshadow-
  - chmod 600 /etc/group-
  - chmod 600 /etc/passwd-
  - chown root:root /etc/ssh/sshd_config
  - chown root:root /etc/passwd-
  - chown root:root /etc/group-
  - chown root:root /etc/shadow
  - chown root:root /etc/securetty
  - chown root:root /boot/grub/grub.cfg
- Open '/etc/fstab' and add the following line to the bottom of it:
  - "none   /run/shm   tmpfs   rw,noexec,nosuid,nodev   0   0"
- 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
  - On any restart, you may have to login with the username root and whatever password you input above
- Edit '/etc/host.conf' to include the following:
  - "nospoof on"
  - "order bind,hosts"
- Make sure '/etc/rc.local' only contains "exit 0", if it does not, it may lead to a backdoor

Defensive Countermeasures

- Install ufw using `sudo apt-get install ufw`
- Enable ufw by using `sudo ufw enable`
- Enable ufw logging with `sudo ufw logging`

Service Auditing

- Check the output of `sudo service --status-all` to check if any services that are not needed are installed/running. Some Examples are below:
  - Minetest service
  - OpenArena service
  - DNS service
  - IRC daemon
  - Postgresql
  - Apache2 service
  - FTP service
  - SNMP service
  - Samba service
  - Rsync service
  - Bind9 service
  - Nfs services

Application Updates

- Make sure that ALL programs or services mentioned in the readme are updated. DOUBLE AND TRIPLE CHECK
- Google how to install things it asks you to install

Prohibited Files

- There are a few types of prohibited files you might want to look for: mp3, csv, sh, zip, and txt files.
- Use the following command along with the files above inside the '/home/' directory to find any of those files:
  - `find -name “*.{extension}” –type f`
- Use this command with the password in the readme to find any files containing passwords in the '/home/', '/etc/', and '/usr/' directories
  - `grep -iRl “<Password in Readme>”`

Prohibited Software

- Remove any of the following programs using this command: `sudo apt remove {program}* -y`
    - airbase-ng
    - aircrack-ng
    - armitage
    - bind9
    - crack
    - crunch
    - cryptcat
    - cups
    - cupsd
    - dovecot
    - dsniff
    - ettercap
    - exim4
    - freeciv
    - freeciv-server
    - hydra
    - hydra-gtk
    - icmp
    - john
    - lcrack
    - medusa
    - minetest
    - minetest-server
    - nbtscan
    - netcat
    - netcat-traditional
    - netdiag
    - nfs-common
    - nfs-kernel-server
    - nikto
    - nmap
    - ophcrack
    - p0f
    - pop3
    - portmap
    - postfix
    - pryit

  - snmp
  - snort
  - tcpdumb
  - tcpspray
  - telnet
  - telnetd
  - weplab
  - wesnoth
  - wireshark
  - zenmap
- Delete the following folders using `sudo rm -rf {directory below}`
  - ‘/usr/lib/games’
  - ‘/usr/local/games’
  - ‘/usr/share/games’
  - ‘/var/games’
  - ‘/var/lib/games’

Malware

- 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`
- Next, look through and try to find any backdoors in the web directory if LAMP is a critical service to see if there are any backdoors
- Find any SUID Files using this command:
  - `find / -perm -4000 -type f 2>/dev/null`
    - If you find anything other than the following, investigate further on what the files is:
      - '/bin/fusermount'
      - '/bin/mount'
      - '/bin/ping'
      - '/bin/su'
      - '/bin/umount'
- Find any SGID files using this command:
  - `find / -perm -2000 -type f 2>/dev/null`
    - Check any of the files, there should be nothing listed
- If LAMP or any other web server is a critical service, you need to check for php backdoors. First find the base directory for the webserver. cd into it, then run the following command(c&p suggested)

```
grep
'((eval.*(base64_decode|gzinflate|\$_))|\$[0O]{4,}|FilesMan|JGF1dGhfc|IIIl|die\(PHP_OS|posix_getpwuid|Array\(base
64_decode|document\.write\("\\u00|sh(3(ll|11)))' . -lroE --include=*.php*
```

Application Security Settings

- 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");”
    - 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);"
```

- SSH (OpenSSH Server)
    - Run `sudo apt-get install openssh-server -y` to make sure ssh is installed
    - Open ‘/etc/ssh/sshd_config’ to secure it by adding/changing the following:
        - Change the line “UsePAM no” to “UsePAM yes”
        - Change “AllowTcpForwarding yes” to “AllowTcpForwarding no”
        - Change “X11Forwarding yes” to “X11Forwarding no”
        - Change “LoginGraceTime 120” to “LoginGraceTime 30”
        - Add the line “ClientAliveInterval 300”
        - Add the line “ClientAliveCountMax 0”
        - The line “Protocol” should be “Protocol 2”
        - Change “HostBasedAuthentication yes” to “HostBasedAuthentication no”
        - Change “PermitEmptyPasswords yes” to “PermitEmptyPasswords no”
        - Change “StrictModes no” to “StrictModes yes”
        - Change “UsePrivilegeSeparation no” to “UsePrivilegeSeparation yes”
        - Change “PermitRootLogin yes” to “PermitRootLogin no”
        - Change “PrintLastLog yes” to “PrintLastLog no”
        - Change “PermitUserEnvironment yes” to “PermitUserEnvironment no”
- Samba (smbd)
    - All of the security is done in ‘/etc/samba/smb.conf’
        - Ensure the only SAMBA share is the required share
        - Make sure that the global section contains the lines:
            - “ntlm auth = 0”
            - “smb encrypt = required”

-
    -
        -
            - “guest ok = no”
            - “restrict anonymous = 2”
            - “min protocol = SMB2”
            - “server signing = mandatory”
            - “read only = yes”
            - “encrypt password = true”
            - “obey pam restrictions = yes”
            - “max log size = 24”
        - Make sure that the opposite of those lines(e.g. “ntlm auth = 1”) is not anywhere in the file
        - Check the share location for secure permissions, good permissions would be 640, eg:
            - chmod 640 /var/supercoolshare
        - Check inside the share for bad files (DELETE THEM FROM THE SHARE LOCATION NOT THE NETWORK LOCATION)
- FTP (VSFTPD)
    - VSFTPD configurations is done inside of ‘/etc/vsftpd.conf’
    - Add/change the following things:
        - Change “anonymous_enable yes” to “anonymous_enable no”
        - Uncomment line starting with “chroot_local_user”
            - (Possible) Change line from no to yes
        - Change “chroot_list_enable no” to “chroot_list_enable yes”
        - Change “write_enable yes” to “write_enable no”
- FTP (PureFTP)
    - PureFTPd can be configured in ‘/etc/pure-ftpd/pure-ftpd.conf’, make sure it contains the following lines:
        - "ChrootEveryone yes"
        - "NoAnonymous yes"
        - "TLS 2"
        - "MaxClientsNumber 50"
        - "MaxClientsPerIP 3"
        - "MaxIdleTime 10"
        - "LimitRecursion 500 8"
        - "Umask 133:022"

LAMP Stack (Linux, Apache2, MySQL, PHP) - Might be mixed with wordpress:

- Apache2
    - Check the root of the web server for malicious/phpinfo files: ‘/var/www/html’ or ‘/var/www’
    - Edit ‘/etc/apache2/apache2.conf’ for the following:
        - Change “ServerSignature On” to “ServerSignature Off”
        - Change the line with “FileETag” to “FileETag None”
        - Change the line with “ServerTokens” to “ServerTokens Prod”
        - Change “TraceEnable On” to “TraceEnable Off”
- MySQL

  - Run `sudo mysql_secure_installation`
  - Configure MySQL inside of ‘/etc/mysql/my.cnf’ under “[mysqld]”
    - Ensure MySQL is being ran by mysql user by changing the line that has “user = root” to “user = mysql”
    - Change/add the line “bind-address=localhost”
    - Add the line “skip-networking”
    - Add the line “local-infile=0”
    - Add the line “default_password_lifetime=30”
- PHP
  - Find the php.ini file by using the command `php -i | grep “php.ini”`
  - Edit this file for the following:
    - Change “safe_mode=Off” to “safe_mode=On”
    - Add “register_globals=off”
    - Change “track_errors = On” to “track_errors = Off”
    - Change “html_errors = On” to “html_errors = Off”
    - Change “display_errors = On” to “display_errors = Off”
    - Change “allow_url_fopen = On” to “allow_url_fopen = Off”
    - Change “allow_url_include = On” to “allow_url_include = Off”
    - Change “file_uploads = On” to “file_uploads = Off”
    - Change “session.use_strict_mode = Off” to “session.use_strict_mode = On”
    - Add all of the following:
      - "expose_php = Off"
      - "allow_url_fopen = Off"
      - "allow_url_include = Off"
      - "upload_max_filesize = 2M"
      - "max_execution_time = 30"
      - "max_input_time = 30 "
      - "open_basedir = "
      - "display_errors = Off"
      - "memory_limit = 40M"
      - "mail.add_x_header = Off"
      - "fle_uploads = Off"
      - "max_input_time = 60"
    - Make sure the line with “disable_functions” includes the following functions:
      - exec
      - system
  - Check all the files in the apache2 web directory for phpinfo() functions

Possible Vulnerability List

1. Forensic Question
2. Removed unauthorized user [user]
3. Removed hidden user
4. User [user] is not an administrator
5. Changed insecure password for [user]
6. Created user group [group]
7. Created user account [user]
8. Users added to group [group]
9. Guest account is disabled
10. User cannot login without a password
11. [User] password expires
12. Root password is no longer blank / Changed insecure Root password
13. Password for user is hashed with a secure algorithm
14. man - Does not have a login shell
15. A default maximum password age is set
16. Previous passwords are remembered
17. A minimum password length is required
18. Extra dictionary based password strength checks
19. A secure password hashing algorithm is used
20. PASS_MAX_DAYS corrected in login.defs
21. Null passwords do not authenticate
22. An account lockout policy is configured
23. Greeter does not enumerate user accounts
24. Ignore broadcast ICMP echo requests enabled
25. IPv4 TCP SYN cookies have been enabled
26. IPv4 TCP SYN,ACK retries reduced
27. IPv4 forwarding has been disabled
28. IPv4 sending ICMP redirects disabled
29. ASLR is enabled
30. /proc/sys/net/ipv4/tcp_rfc1337 - contains 1
31. /proc/sys/kernel/unprivileged_userns_clone - contains 0
32. Resolver checks for IP spoofing
33. Dmesg restrict set to 1
34. Sysrq is set to 0(disable sysrq)
35. Xserver-allow-tcp disabled
36. Sudo requires authentication
37. Insecure permissions on shadow file fixed
38. GRUB configuration is not world readable
39. boot/grub/grub.cfg - contains set superusers= and password_pbkdf2 grub

40. Stricter defaults have been enabled for shared memory
41. Firewall protection has been enabled
42. Minetest service has been disabled or removed
43. OpenArena service has been disabled or removed
44. DNS service is disabled or removed
45. IRC daemon has been stopped and disabled
46. Postgresql has been disabled or removed
47. Apache2 service has been disabled or removed
48. FTP service has been disabled or removed
49. SNMP service has been disabled/removed
50. Samba service has been disabled/removed
51. Rsync service has been disabled/removed
52. bind9 service is stopped and removed
53. nfs services is stopped and removed
54. The system automatically checks for updates daily
55. Install updates from important security updates
56. The Linux Kernel has been updated
57. Bash has been updated
58. OpenSSL shared libraries have been updated
59. Glibc has been updated
60. sources.list has valid lists
61. Firefox has been updated
62. Samba has been updated
63. Apache2 has been updated
64. PHP5 has been updated
65. WordPress has been updated
66. OpenSSH has been updated
67. 7zip has been updated
68. LibreOffice has been updated
69. Pure FTP has been updated
70. Prohibited MP3 files are removed
71. Removed plaintext file containing passwords
72. Stellarium has been installed
73. Removed *{Prohibited software below}*
    a. Minetest
    b. NBTScan
    c. Nmap and Zenmap
    d. TCPSpray
    e. Dsniff
    f. p0f
    g. freeciv

   h. Wireshark
   i. ophcrack
   j. knocker
   k. kismet

74. Removed python backdoor
75. Removed perl backdoor
76. Removed netcat backdoor
77. php backdoor is removed
78. SUID backdoor removed
79. SSH root login has been disabled
80. SSH protocol 1 has been disabled
81. SSH only listens on port 222(situational)
82. SSH allows only public key authentication
83. SSH does not permit empty passwords
84. SSH user environment processing is disabled
85. Anonymous Samba access is disabled
86. Unauthorized Samba share is disabled
87. Samba blank passwords are disabled
88. Samba SMB1 protocol is disabled
89. SMB share is not world writeable
90. Encrypt smb traffic is enabled
91. ntlm authentication is disabled
92. FTP local users must log in as anonymous
93. FTP anonymous write commands are disabled
94. FTP PASV security checks enabled
95. FTP anonymous user is not root
96. FTP anonymous access is disabled
97. Insecure permissions on FTP root directory fixed
98. FTP plain-text authentication disabled
99. MySQL remote access is disabled
100. SQL is not ran as root
101. Removed phpinfo() php file
102. PHP expose is Off
103. PHP system function is disabled
104. php allow url fopen is off
105. php session.use strict mode is on
106. Apache server signature is disabled
107. Apache trace requests disabled
108. Apache fileEtags none
109. Firefox displays warning on known malware sites
110. Firefox warns when sites try to install add-ons

111. Firefox - Block dangerous and deceptive content