***IMPORTANT:*** It is your responsibility to request permission and withstand consequences to use security tools to perform assessment of a public network system that is owned and administered by an organization.  DO NOT make attempts to scan or test against 140.146.x.x networks or IP's that belong to UW-Whitewater under ANY circumstances.  Therefore, it is much safer to start practicing network scanning on private networks, including 192.168.x.x, 172.16.x.x, or 10.0.x.x, etc.

**Q.0:** Agreement of Do No Harm

I agree.

**Q.1:**

**Graphical user interface

Description automatically generated**

**Q.2:Graphical user interface, text, application

Description automatically generated**

**Q.3:**

**Text, application

Description automatically generated**

I think that this alert is the biggest threat because it is placed as a medium risk factor, whereas the other two alerts were at a low risk. Also clickjacking is when the user thinks they are clicking on one thing but they are actually clicking on something else. This can be very powerful to steal different things like login information when the user thinks they are signing into the right portal but they are actually just giving away their info.

**Q.4:**

┌──(root💀kali)-[/home/kali]

└─# nc 192.168.56.101 21

220 Microsoft FTP Service

┌──(root💀kali)-[/home/kali]

└─# nc -zv 192.168.56.101 1-450

192.168.56.101: inverse host lookup failed: Unknown host

(UNKNOWN) [192.168.56.101] 445 (microsoft-ds) open

(UNKNOWN) [192.168.56.101] 139 (netbios-ssn) open

(UNKNOWN) [192.168.56.101] 135 (epmap) open

(UNKNOWN) [192.168.56.101] 80 (http) open

(UNKNOWN) [192.168.56.101] 21 (ftp) open

**Q.5:**

**-[ Lynis 3.0.8 Results ]-**

**Warnings (1):**

**----------------------------**

**! Couldn't find 2 responsive nameservers [NETW-2705]**

**https://cisofy.com/lynis/controls/NETW-2705/**

**Suggestions (45):**

**----------------------------**

**\* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]**

**https://cisofy.com/lynis/controls/LYNIS/**

**\* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]**

**https://cisofy.com/lynis/controls/BOOT-5122/**

**\* Consider hardening system services [BOOT-5264]**

**- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service**

**https://cisofy.com/lynis/controls/BOOT-5264/**

**\* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]**

**https://cisofy.com/lynis/controls/KRNL-5820/**

**\* Configure password hashing rounds in /etc/login.defs [AUTH-9230]**

**https://cisofy.com/lynis/controls/AUTH-9230/**

**\* Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc [AUTH-9262]**

**https://cisofy.com/lynis/controls/AUTH-9262/**

**\* When possible set expire dates for all password protected accounts [AUTH-9282]**

**https://cisofy.com/lynis/controls/AUTH-9282/**

**\* Configure minimum password age in /etc/login.defs [AUTH-9286]**

**https://cisofy.com/lynis/controls/AUTH-9286/**

**\* Configure maximum password age in /etc/login.defs [AUTH-9286]**

**https://cisofy.com/lynis/controls/AUTH-9286/**

**\* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]**

**https://cisofy.com/lynis/controls/AUTH-9328/**

**\* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]**

**https://cisofy.com/lynis/controls/FILE-6310/**

**\* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]**

**https://cisofy.com/lynis/controls/FILE-6310/**

**\* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]**

**https://cisofy.com/lynis/controls/FILE-6310/**

**\* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]**

**https://cisofy.com/lynis/controls/USB-1000/**

**\* Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]**

**https://cisofy.com/lynis/controls/STRG-1846/**

**\* Check DNS configuration for the dns domain name [NAME-4028]**

**https://cisofy.com/lynis/controls/NAME-4028/**

**\* Install debsums utility for the verification of packages with known good database. [PKGS-7370]**

**https://cisofy.com/lynis/controls/PKGS-7370/**

**\* Install package apt-show-versions for patch management purposes [PKGS-7394]**

**https://cisofy.com/lynis/controls/PKGS-7394/**

**\* Consider using a tool to automatically apply upgrades [PKGS-7420]**

**https://cisofy.com/lynis/controls/PKGS-7420/**

**\* Check your resolv.conf file and fill in a backup nameserver if possible [NETW-2705]**

**https://cisofy.com/lynis/controls/NETW-2705/**

**\* Determine if protocol 'dccp' is really needed on this system [NETW-3200]**

**https://cisofy.com/lynis/controls/NETW-3200/**

**\* Determine if protocol 'sctp' is really needed on this system [NETW-3200]**

**https://cisofy.com/lynis/controls/NETW-3200/**

**\* Determine if protocol 'rds' is really needed on this system [NETW-3200]**

**https://cisofy.com/lynis/controls/NETW-3200/**

**\* Determine if protocol 'tipc' is really needed on this system [NETW-3200]**

**https://cisofy.com/lynis/controls/NETW-3200/**

**\* Check iptables rules to see which rules are currently not used [FIRE-4513]**

**https://cisofy.com/lynis/controls/FIRE-4513/**

**\* Install Apache mod\_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]**

**https://cisofy.com/lynis/controls/HTTP-6640/**

**\* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]**

**https://cisofy.com/lynis/controls/HTTP-6643/**

**\* Add HTTPS to nginx virtual hosts for enhanced protection of sensitive data and privacy [HTTP-6710]**

**https://cisofy.com/lynis/controls/HTTP-6710/**

**\* Change the allow\_url\_fopen line to: allow\_url\_fopen = Off, to disable downloads via PHP [PHP-2376]**

**https://cisofy.com/lynis/controls/PHP-2376/**

**\* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]**

**https://cisofy.com/lynis/controls/LOGG-2154/**

**\* Check what deleted files are still in use and why. [LOGG-2190]**

**https://cisofy.com/lynis/controls/LOGG-2190/**

**\* It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-8318]**

**https://cisofy.com/lynis/controls/INSE-8318/**

**\* Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services [INSE-8320]**

**https://cisofy.com/lynis/controls/INSE-8320/**

**\* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]**

**https://cisofy.com/lynis/controls/BANN-7126/**

**\* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]**

**https://cisofy.com/lynis/controls/BANN-7130/**

**\* Enable process accounting [ACCT-9622]**

**https://cisofy.com/lynis/controls/ACCT-9622/**

**\* Enable sysstat to collect accounting (disabled) [ACCT-9626]**

**https://cisofy.com/lynis/controls/ACCT-9626/**

**\* Enable auditd to collect audit information [ACCT-9628]**

**https://cisofy.com/lynis/controls/ACCT-9628/**

**\* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]**

**https://cisofy.com/lynis/controls/FINT-4350/**

**\* Determine if automation tools are present for system management [TOOL-5002]**

**https://cisofy.com/lynis/controls/TOOL-5002/**

**\* Consider restricting file permissions [FILE-7524]**

**- Details : See screen output or log file**

**- Solution : Use chmod to change file permissions**

**https://cisofy.com/lynis/controls/FILE-7524/**

**\* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]**

**https://cisofy.com/lynis/controls/HOME-9304/**

**\* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]**

**- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)**

**https://cisofy.com/lynis/controls/KRNL-6000/**

**\* Harden compilers like restricting access to root user only [HRDN-7222]**

**https://cisofy.com/lynis/controls/HRDN-7222/**

**\* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]**

**- Solution : Install a tool like rkhunter, chkrootkit, OSSEC**

**https://cisofy.com/lynis/controls/HRDN-7230/**

**Follow-up:**

**----------------------------**

**- Show details of a test (lynis show details TEST-ID)**

**- Check the logfile for all details (less /var/log/lynis.log)**

**- Read security controls texts (https://cisofy.com)**

**- Use --upload to upload data to central system (Lynis Enterprise users)**

**================================================================================**

**Lynis security scan details:**

**Hardening index : 65 [############# ]**

**Tests performed : 274**

**Plugins enabled : 0**

**Components:**

**- Firewall [V]**

**- Malware scanner [X]**

**Scan mode:**

**Normal [ ] Forensics [ ] Integration [ ] Pentest [V] (running privileged)**

**Lynis modules:**

**- Compliance status [?]**

**- Security audit [V]**

**- Vulnerability scan [V]**

**Files:**

**- Test and debug information : /var/log/lynis.log**

**- Report data : /var/log/lynis-report.dat**

**================================================================================**

**Lynis 3.0.8**

**Auditing, system hardening, and compliance for UNIX-based systems**

**(Linux, macOS, BSD, and others)**

**2007-2021, CISOfy - https://cisofy.com/lynis/**

**Enterprise support available (compliance, plugins, interface and tools)**

**================================================================================**

**[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /home/kali/lynis/default.prf for all settings)**

There was only one warning provided by this pentest that it could not find 2 responsive nameservers NETW-2705, however there were 45 suggestions that came up such as adding a malware scanner to the system which was also flagged in the summary at the end.

**Q.6:**

My first key takeaway from this Practical Exercise is just how powerful Kali Linux is in terms of how many different commands there are and how many different tests can be done. They are very simply commands to run but have a powerful affect such as the last part which can provide a lot of information to improve the defense of the Kali Linux VM’s system. A lot of the suggestions are something that most likely would never cross a user’s mind when they are trying to improve the defense of their system so this command provides useful information. If you have the IP address of a system, this practical exercise demonstrated what kind of commands you can execute to gather information such as server checks, vulnerability checks, and additional port scanning. Lynis is a very powerful tool for security and compliance testing to highlight any vulnerabilities of a given system.