CyberPatriot Semifinals Round Checklist

#cyberpatriot

Take a screenshot of the scoring report after every category.

Image Backups

1. Create a folder on the Windows desktop named `golden`
2. Create a folder on the Windows desktop named `copies`
3. Copy **all images** to **both** the `golden` folder and the `copies` folder
4. Open the image in the `C:\Temp` folder
5. If the image bricks, **delete** the image from `C:\Temp`, **move** an image from `copies` to `C:\Temp`, and immediately open it in VMWare
6. Re-copy the image from `golden` to `copies`

Windows

New for Semis: For all baseline tasks, append `new` to the end of the command to show only items that are new to that image (highlighted red), or append `diff` to the end of the command to show items that are new or different in some way (highlighted red or yellow).

1. README
   - **Remember necessary software!**
2. Forensics
   - Maximum 20 minutes per question, on a timer (return at end)
3. Complete all vulns in README
4. Start CyberBot
5. User Auditing
   - #CyberBot `modules run pr`
   - #CyberBot `modules run ua` (not on AD)
   - #CyberBot `modules load ua`, `enum_users`
     - Check for suspicious group membership, logon scripts, etc
   - New user password: `CyberP@triot23`
   - Active Directory:
     - Enable View -> Advanced Features
     - Prevent user from accidental deletion

        - Store certain users with reversible encryption
        - Account cannot be delegated
        - Kerberos preauth
        - Group managed by other group
        - Group membership on each account
6. Account Policies/Local Policies
    - #CyberBot `modules run gp`
        - (Exports GPO to `C:\CyberBot-backups`, copies backup `PolicyRules` file)
        - Open `C:\CyberBot-backups\PolicyAnalyzer\PolicyAnalyzer.exe`
        - Change `Policy Rule sets` location to `C:\CyberBot-backups\Rules`
        - Click `Add`, then `File` > `Add files from GPO(s)...`
        - Browse to `C:\CyberBot-backups` and select the folder with the long ID string
        - Click `Import...`
        - Type `image`, and press Enter
        - Click `View / Compare`
        - Click `View` > `Show only Differences`
        - Check for new policies set, and especially security settings that are different from default (highlighted yellow)
        - Active Directory:
            - Export all linked GPOs from `gpmc.msc` and open in PolicyAnalyzer
    - #CyberBot `modules load gp`, `reset`
    - #CyberBot `windows_autogp`
        - This wraps running all of the Windows checklist files:
            - `windows/gp_audit`
            - `windows/exploit_protection`
            - `windows/gp_firewall`
            - `windows/gp_network`
            - `windows/gp_plugins`
            - `windows/gp_security`
            - `windows/gp_system`
            - `windows/gp_user`
            - `windows/gp_wincomp_av`
            - `windows/gp_wincomp_eventlog`
            - `windows/gp_wincomp_misc`
            - `windows/gp_wincomp_rds`
            - `windows/gp_wincomp_update`
7. Defensive Countermeasures

- #CyberBot `modules load baselines`, `firewall`
  - Will show firewall rules that are non-standard
- Check Control Panel action center
- Check Microsoft Defender dialogs
  - Click through settings and check for file exclusions (should already be set by group policy, but doesn't hurt to check)
- Run a malware full scan, can sometimes detect archives that contain malware

8. Prohibited Files
   - #CyberBot `launch everything`
     - Make the following searches:
       - `C:\Users` (shows user files)
       - `audio:` (all audio files)
       - `zip:` (all compressed files)
       - `doc:` (all "document" files)
       - `exe:` (all executable files)
       - `pic:` (all pictures)
       - `video:` (all videos)
   - #CyberBot `modules run files`
   - Check paths relating to services (for SMB, the folder being shared; for IIS, the web server root (`C:\inetpub\wwwroot`))
   - Use SysInternals `Streams` to find NTFS alternate data streams
9. Unwanted Software
   - Download Bulk Crap Uninstaller (not bundled b/c very large)
   - #CyberBot `launch autoruns`
     - Find programs running on startup that shouldn't (also falls under Malware)
10. Malware
    - #CyberBot `modules load baselines`, `tasks`
      - Check for suspicious tasks
      - For all baseline tasks, append `new` to the end of the command to show only items that are new to that image (highlighted red), or append `diff` to the end of the command to show items that are new or different in some way (highlighted red or yellow).
    - #CyberBot `launch procexp`
      - Check Process Explorer for malicious tasks
11. Service Auditing
    - #CyberBot `modules load baselines`, `services`
    - #CyberBot `checklist run windows/services`

12. Uncategorized
    - `compmgmt.msc`, check shares
    - Remote assistance/remote desktop
    - Active Directory:
        - NTDS.dit file, SYSVOL, etc
13. Updates
    - Update all applications in README, set automatic update
    - Check Windows Update for any group policy settings
14. Application Security
    - Refresh Firefox to default settings (Hamburger menu > Help > More troubleshooting information > Refresh Firefox)
        - #CyberBot `checklist run all/firefox`
            - **This is untested and might not work**
    - Go to written checklist related to service
        - If RDP, appsec is already done through Group Policy
    - Check permissions on directories and files related to the critical service (for SMB, the folder being shared; for SSH, the SSH configuration file)
    - Active Directory
        - V-8555 dsHeuristics
        - V-15372 AD Schema
        - Enable rolling of expiring NTLM secrets during sign on, for users who are required to use Microsoft Passport or smart card for interactive sign on (AD Domain Center)
    - V-220717 directory permissions
    - V-220907 registry permissions
    - V-220782, V-220783, V-220784 event log file permissions

Ubuntu

New for Semis: For all baseline tasks, append `new` to the end of the command to show only items that are new to that image (highlighted red), or append `diff` to the end of the command to show items that are new or different in some way (highlighted red or yellow).

1. README
    - Remember necessary software!
2. Forensics
    - Maximum 20 minutes per question, on a timer (return at end)
3. **Complete all vulns in README**

4. Create root shell
5. Start CyberBot
    - #CyberBot `modules run baselines` (ignore the output for now, this just caches the baseline data in the background so that changes you make don't affect it)
    - `cp -r /etc /root/etc`
        - For baselining later
6. User Auditing
    - #CyberBot `modules run pr`
    - #CyberBot `modules run ua`
    - #CyberBot `modules load ua`, `enum_users`, check for the following:
        - Extra users with UID below 1000 ("hidden" users)
        - Built-in user with a valid logon shell
        - System users with passwords
        - Incorrect home directories
    - New user password: `CyberP@triot23`
    - `pwck`, `grpck`
    - #CyberBot `modules load baselines`
        - Check `passwd` for any differences in system users or shadowed passwords (there should not be a shadowed password in the `passwd` file)
        - Check `passwd` for users that have unlocked accounts
        - Check for group membership changes that are not specified in README
        - Check `group` for extra groups that should not be on system
        - Check `shadow` for users with blank passwords (automatic logon)
        - Check `gshadow` to find group admins
        - Check `gshadow` for passwords set that make a user part of a group
7. Account Policies
    - #CyberBot `modules load baselines`, `pam`
        - Check for differences between old and new PAM configuration
    - #CyberBot `checklist run linux/pam`
        - Sets correct PAM settings
    - #CyberBot `checklist run linux/passwords`
    - #CyberBot `checklist auditreport linux/accounts`
        - Will give a short audit of user accounts and policies
8. Local Policies
    - For each item, check `.d` directories for any additional configuration files
    - Meld
        - `apt install meld`

    - Set `support/baselines/deb-11/etc` as one directory, and `/etc` as the other, click Compare
    - Shows a diff of everything in etc
- #CyberBot `modules load baselines`, `sysctl diff`
- #CyberBot `modules load baselines`, `sudo`
- #CyberBot `modules load baselines`, `cron`
    - Check `/var/spool/cron/crontabs`, no files there
    - Check `/etc/crontab`
    - Check `/etc/cron.d` and `.<time>`
- #CyberBot `modules load baselines`, `debsums`
- #CyberBot `modules load baselines`, `kernelmods`
- #CyberBot `checklist run linux/general/sysctl`
- #CyberBot `checklist run linux/general/sudo`
    - `cat /etc/sudoers.d/*`
    - `rm /etc/sudoers.d/*`
- #CyberBot `checklist run linux/general/audit`
- #CyberBot `checklist run linux/general/gdm3` **needs testing**
- #CyberBot `checklist run linux/general/grub`
    - **Username**: `cyberhounds`
    - **Passsword**: `CyberP@triot23`
- #CyberBot `checklist run linux/general/modprobe`
- #CyberBot `checklist run linux/general/permissions`
- #CyberBot `checklist run linux/general/systemd`
- #CyberBot `checklist run linux/general/apt`
- #CyberBot `checklist run linux/debian/pam`
- #CyberBot `modules load baselines`, `etc <file>` to diff files in etc
- #CyberBot `modules load baselines`, `etcr <file>` to recursively diff folders in etc

9. Defensive Countermeasures
    - #CyberBot `modules load baselines`, `ufw`
        - Check for any additional firewall rules
    - `ufw --force reset`
    - #CyberBot `checklist run linux/general/ufw`
10. Prohibited Files
    - #CyberBot `modules run files`
        - If nothing shows up, run `updatedb`

- `cd support/linux/programs`, `apt install ./fsearch_0.2.3-1+3.1_amd64.deb`, `fsearch`
  - Do not forget the `./` on the `fsearch` binary
  - Change database to include `/`, wait for it to index
  - Click on `All` to change file types

11. Unwanted Software
    - #CyberBot `checklist run linux/prohibited_software`
    - #CyberBot `modules load baselines`, `aptmark`
    - #CyberBot `modules load baselines`, `dpkg diff`
      - Look through new programs installed
12. Malware
    - `ps -aef --forest`
      - Default `ps` output in baselines folder
    - List cron jobs of all users
      - `for user in $(cut -f1 -d: /etc/passwd); do echo $user; crontab -u $user -l; done`
    - Check init scripts
    - List systemd timers
      - `systemctl list-timers --all`
    - List running processes
      - `ps -aef --forest`
      - Default ps output in baselines folder
    - List capabilities of binaries
      - `/usr/bin/getcap -r /usr/bin`
      - `=ep` means all capabilities
      - Remove with `/usr/bin/setcap -r FILEPATH`
    - Check SUID, SGID, and sticky bit
      - `find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \;`
      - `find / -uid 0 -perm -4000 -type f 2>/dev/null`
      - `2000` (SGID), `1000` -> (sticky bit)
    - `rk-hunter`
    - `clamav`
13. Service Auditing
    - #CyberBot `modules load baselines`, `basicservices`
    - #CyberBot `modules load baselines`, `services`
14. Updates
    - #CyberBot `modules load baselines`, `etc apt.d/sources.list`

        - Check all of the files in `/etc/sources.list.d` too
    - #CyberBot `checklist run linux/debian/apt`
        - Resets sources
    - Go to Ubuntu update center and enable automatic updates
    - `add-apt-repository ppa:apt-fast/stable`
    - `apt update`
    - `apt install apt-fast`
        - Select `apt-get`, `10`, then select Yes (not the default option)
    - `apt-fast update && apt-fast dist-upgrade`
15. Reboot to apply kernel updates
16. Application Security
    - Firefox
        - Refresh Firefox to default settings (Hamburger menu > Help > More troubleshooting information > Refresh Firefox)
        - #CyberBot `checklist run all/firefox`
            - **This is untested and might not work**
    - For SSH:
        - #CyberBot `checklist view linux/general/ssh`, make sure that there are vulns and not just "SSH is not installed"
            - #CyberBot `options set SERVICES=SSH` if not
        - #CyberBot `checklist run linux/general/ssh`
    - Go to written checklist related to service
    - Check permissions on directories and files related to the critical service (for SMB, the folder being shared; for SSH, the SSH configuration file)
    - Check for insecure served files (sensitive files, backdoors PHP files, etc)