
# *CyberPatriot IV*

## Open Division Round 1

**04-05 November 2011**

# Open Division Round 1

The Open Division Round 1 target is a Windows XP workstation. Your goal is to find and remediate as many vulnerabilities as possible while maintaining the critical services outlined in this document. While you may find the targets have much more than the what's stated on your status page, very specific sets have been selected to score you on.

Please read over this document as it outlines things to consider, and things to avoid.

### ***Do's & Don'ts:***

1. **DO Work within the Virtual Machine Target ONLY!**
   Only the changes you make within the virtual machine will be recognized by the scoring server.

2. **DO register your Target!**
   Even if you have registered a Target in past rounds, when it comes time for competition day you **MUST** register that Target at the beginning of each new round or you won't be scored and are **NOT** part of the game.

3. **DO NOT delete the Target once the exercise is started and you have registered**
   It contains your unique registration ID and identifies you to the scoring system located at SAIC. If your unique ID is removed, you will have to re-register and your score will return to zero.

4. **DO NOT Disconnect VMWare Devices →Network Adapter**
   While you are working, your virtual machine is constantly communicating to the scoring system located at SAIC. If you are disconnected from the network, your system will be seen as "down" and your score will be inversely affected.

5. **DO NOT Change Devices → Network Adapter → NAT**
   This setting will work for the majority of participants. Changing to "Bridged" or "Host-Only" can affect your network connectivity and you will lose connection to the scoring system. A small percentage of participant networks may not accept traffic from the virtual machine in this configuration. Only if you cannot access the Internet, and have already verified you have a valid IP, should you change this setting to "Bridged.

6. **DO NOT RELOAD another copy of the Target without contacting the help desk**
   Each Target needs to be individually registered, if you damage your Target to the point that you feel that the only solution is to start over, you should contact the help desk for instructions on how to proceed.

7. **DO NOT Run any targets that are not part of this round during the exercise. Any targets from previous rounds should have been deleted before this round was started.**

8. **DO NOT Attempt to register your Target by any non-standard means.**
   When a new Windows Target image is started up for the first time, the guest operating system will load several startup programs, including the registration program. It may take several seconds, but you will eventually see a registration window that takes up the entire screen. This is the only way you should register your team. Attempting to register by any other means may prevent your Target from being properly registered and as a result you may not be scored.

9. **DO check the "Get My Status" page to ensure your client can still communicate to Scorebot!**
If "Your last health update was" time is more than 30 minutes past the current "Scorebot time" in the Get My Status, then you may have disabled/broken the connectivity between the CyberNEXSClient in the Target and the ScoreBot server.

## Users:

1. **The Administrator account is NOT set to auto-login.**
The initial passwords are listed below. If you change the password, write it down to ensure you don't forget it.

**Windows**
**Username: Administrator**
**Password: letmein**

2. **DO NOT modify, disable, delete, or change the password of the CyberNEXS users**
This user enables the CyberNEXSClient service to connect to the scoring system. Tampering with this user may cause your system to stop reporting updates. This includes changing permissions, changing the group, disabling the user, expiring its password, etc. Any users referring to CyberNEXS in the name or description should not be modified.

## *Services:*

1. **DO maintain the *critical* services**
Each Target will have a set of "Critical Services" associated with it. These services are representative of real life critical services you may find in production servers. For example, a web server must always run an HTTP or HTTPS service to serve web content to users. A mail server must run an SMTP service to deliver mail. And so on.

**Windows**
**SNMP udp/161**

2. **DO NOT disable, stop, or modify the CyberNEXSClient service parameters**
This is the main service that communicates with the scoring system at SAIC. If this service is not running, you will not receive a score.

3. **DO NOT disable or stop these services:**
- **TCP/IP NetBIOS Helper (LmHosts)**
- **Terminal Services (TermService)**
- **DNS Client (Dnscache)**

These services have been identified as critical to network connectivity for your Windows target.

## *Files:*

1. **DO NOT uninstall CyberNEXSClient or delete or modify any files in C:\SAIC**
The CngClient program runs as a service that constantly evaluates your system health and configuration.

2. **DO NOT delete the C:\Get_My_Status.html file**
This file appears after successful registration and contains a link personalized to your registered Target. This link redirects you to your team's status page.

## *Environment:*

1. **DO NOT Delete or modify the CNGCLIENT_CONFIG_HOME environment variable**
   This variable is used within the CyberNEXSClient program.

## Please make sure…

1. You are running from the ***same network*** and using the ***same computer(s)*** that you used during the practice round. In addition to familiarizing you with the game environment, practice rounds are used to ensure your network and computers are compatible with the CyberNEXS™ platform.

2. You have already *verified* the MD5 checksum of the downloaded target matches the one listed in this document. If it does not, the 7zip file that you have downloaded is corrupted or truncated and you must download the file again.

3. BEFORE you unlock the 7zip file and extract the Target, that you delete any remaining Target files and directories.

4. You read this ENTIRE document, including the *Do's and Don'ts*. The extra minutes you spend here will prove valuable.

5. You MUST ensure that you are using the target for this round and NOT using any other previous images.

6. If you have successfully registered the image you are working on and you are no longer seeing updates to your "Get My Status" page, try rebooting your virtual machine to force the client to attempt a connection to the server.

MD5 Checksum: 93e77eb5eeb2df3601441818119ed7f3
Password: pupH2Traprac