# Windows 2008R2 Server Hardening Checklist

Riders Notes:

1. Install Windows
2. Install Updates via windowsupdate website
3. Run SCW
4. Set up networking using information in table below
5. Create Domain
6. Setup primary DNS
7. Set up secondary called DMZ\_DNS @ 192.168.5.24
8. Set up secondary DNS called SECONDARY\_LAN\_DNS @ 192.168.4.16
9. Create accounts necessary for other users on the domain – see below for details
10. Set up GPO policy – see table below for details
11. Set up Firewall policy – see table below for details

# Server Information

|  |  |
| --- | --- |
| IP Address | 192.168.4.18 |
| Default Gateway | 192.168.4.10 |
| DNS Server | 8.8.8.8, 8.8.4.4 |
| Administrator Name | PeeWee2000 |
| 2k12 User Name (Nick) | 2K12SP\_Admin |
| 2k3 Username (Ian) | Criwl1998  \\ |
|  |  |
| Windows 7 Client Acct | Win7\_Client\\ |

# Domain Information

|  |  |
| --- | --- |
| Domain Name | T2.Local |
| Domain Controller | T2-DC |
| DNS Server | 192.168.4.18, 8.8.8.8 |
| SharePoint Server |  |
| FTP Server |  |
| Windows 7 Client |  |

# GPO Settings

|  |  |
| --- | --- |
| Policy | Setting |
| Computer Config\Windows\Security\Account\Password\Min Length | 10 |
| Computer Config\Windows\Security\Account\Password\Complexity | Enabled |
| Computer Config\Windows\Security\Account\Account Lockout\Duration | 90 |
| Computer Config\Windows\Security\Account\Account Lockout\Threshold | 5 |
| Computer Config\Windows\Security\Account\Account Lockout\Reset | 90 |
| Computer Config\Windows\Security\Local Policies\Security\Admin Account | Disabled |
| Computer Config\Windows\Security\Local Policies\Security\Guest Account | Disabled |
| Computer Config\Windows\Security\Local Policies\Security\Rename Admin | Badmin |
| Computer Config\Windows\Security\Local Policies\Security\AllowUnlock | Disabled |
| Computer Config\Windows\Security\Local Policies\Security\AllowSchedTasks | Disabled |
| Computer Config\Windows\Security\Local Policies\Security\RefusePassChanges | Enabled |
| Computer Config\Windows\Security\Local Policies\Security\RequireStrongSession | Enabled |
| Computer Config\Windows\Security\Local Policies\Security\Display user info | Do not display |
| Computer Config\Windows\Security\Local Policies\Security\DO not display last user | Enabled |
| Computer Config\Windows\Security\Local Policies\Security\Require Domain Authentication | Enabled |
| Computer Config\Windows\Security\Local Policies\Security\Send unencrypted passwords  Computer Config\Windows\Security\Local Policies\Security\ | Disabled |
| Computer Config\Windows\Security\Local Policies\Security\Amount of idle time | 5 minutes |
| Computer Config\Windows\Security\Local Policies\Security\RemotelyAccessibleRegistry | None |
| Computer Config\Windows\Security\Local Policies\Security\RemotelyAccesibleRegistryAndSub | None |
| Computer Config\Windows\Security\Local Policies\Security\RestrictAnonymousAccessToNamed | Enabled |
| Computer Config\Windows\Security\Local Policies\Security\RecoveryConsole:Allowautomatic | Disabled |
| Computer Config\Windows\Security\Local Policies\Security\AllowShutdown w/o logon | Disabled |
| Computer Config\Windows\Security\Local Policies\Security\UAC: admin approval | Enabled |
| Computer Config\Windows\Security\Local Policies\Security\UAC Behavior of elevation | Prompt for C |
| Computer Config\Windows\Security\Local Policies\Security\UAC Behavior for standard | Deny |
| Computer Config\Windows\Security\Local Policies\Security\UAC Detect installs | Enabled |
| Computer Config\Windows\Security\Local Policies\Security\UAC Only elevate execs | Disabled |
| Computer Config\Windows\Security\Local Policies\Security\Switch to secure | Enabled |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Firewall Settings

|  |  |
| --- | --- |
| Domain Name | T2.Local |
| Domain Controller | T2-DC |
| DNS Server | 192.168.4.18, 8.8.8.8 |
| SharePoint Server |  |
| FTP Server |  |
| Windows 7 Client |  |

**Checklist**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Step | **√** | Instruction | Cat I | Cat II/III |
|  |  | Preparation and Installation |  |  |
| 1 |  | If new install, protect it from hostile network traffic until the OS is installed and hardened | ! |  |
| 2 |  | Consider using the Security Configuration Wizard to assist in hardening the | ! |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | host. |  |  |
|  |  | Service Packs and Hotfixes |  |  |
| 3 |  | Install the latest service packs and hotfixes from Microsoft. | ! |  |
| 4 |  | Enable automatic notification of patch availability. | ! |  |
|  |  | Auditing and Account Policies |  |  |
| 5 |  | Configure Audit policy as described. | ! |  |
| 6 |  | Set minimum password length. | ! |  |
| 7 |  | Enable Password Complexity. |  |  |
| 8 |  | Configure Event Log Settings. |  |  |
|  |  | Security Settings |  |  |
| 9 |  | Disable anonymous SID/Name translation. (default) | ! |  |
| 10 |  | Do not allow Anonymous Enumeration of SAM accounts (Default) | ! |  |
| 11 |  | Do not allow Anonymous Enumeration of SAM accounts and shares. |  |  |
| 12 |  | Disable the guest account. (Default) |  |  |
| 13 |  | Digitally Encrypt or Sign Secure Channel Data (Always). (Default) |  |  |
| 14 |  | Digitally Encrypt Secure Channel Data (When Possible). (Default) | ! |  |
| 15 |  | Digitally Sign Secure Channel Data (When Possible). (Default) | ! |  |
| 16 |  | Place the University warning banner in the Message Text for Users Attempting to log on. | ! |  |
| 17 |  | Disable the sending of unencrypted password to connect to Third-Party SMB Servers. (Default) |  |  |
| 18 |  | Do not allow Everyone permissions to apply to anonymous users. (Default) |  |  |
| 19 |  | Do not allow any named pipes to be accessed anonymously. | ! |  |
| 20 |  | Restrict anonymous access to Named Pipes and Shares. | ! |  |
| 21 |  | Ensure that no shares can be accessed anonymously. | ! |  |
| 22 |  | Choose "Classic" as the sharing and security model for local accounts. (Default) | ! |  |
| 23 |  | Do not store LAN Manager hash values | ! |  |
| 24 |  | Set LAN Manager Authentication level to NTLMv2 only | ! |  |
|  |  | Additional Security Protection |  |  |
| 25 |  | Disable or uninstall unused services. | ! |  |
| 26 |  | Disable or delete unused users. |  |  |
| 27 |  | Configure User Rights to be as secure as possible. |  |  |
| 28 |  | Ensure all volumes are using the NTFS file system. |  |  |
| 29 |  | Use the Internet Connection Firewall or other methods to limit connections to the server. |  |  |
| 30 |  | Configure file system permissions. |  |  |
| 31 |  | Configure registry permissions. |  |  |
|  |  | Additional Steps |  |  |
| 32 |  | Set the system date/time and configure it to synchronize against campus time servers. |  |  |
| 33 |  | Install and enable antivirus software. |  |  |
| 34 |  | Install and enable anti-spyware software. |  |  |
| 35 |  | Configure antivirus software to update daily |  |  |
| 36 |  | Configure anti-spyware software to update daily. |  |  |
| 37 |  | Configure a screensaver to lock the console screen automatically if the |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | host is left unattended. |  |  |
| 38 |  | If the machine is not physically secured against unauthorized tampering, set a BIOS/firmware password to prevent alterations in system startup settings. |  |  |
| 39 |  | Configure the device boot order to prevent unauthorized booting from alternate media. |  |  |
| 40 |  | Systems will provide secure storage for Category-I data as required by confidentiality, integrity, and availability needs. Security can be provided by means such as, but not limited to, encryption, access controls, file system audits, physically securing the storage media or any combination thereof as deemed appropriate. |  |  |
| 41 |  | Install software to check the integrity of critical operating system files. |  |  |
| 42 |  | If Remote Desktop Protocol (RDP) is utilized, set RDP connection encryption level to high. |  |  |
| 43 |  | Ensure server has been added to the domain. |  |  |
| 44 |  | Ensure server resides in the correct Organizational Unit (OU). |  |  |

**Addendum**

|  |  |
| --- | --- |
| 1 | If other alternatives are unavailable, this can be accomplished by installing a SOHO router/firewall between the network and the host to be protected. IMPORTANT NOTE: The use of a SOHO router/firewall is only allowed during an initial setup only. It is not to be used for a server in Production. |
| 2 | The Security Configuration Wizard (SCW) can greatly simplify the hardening of the server. Once the role for the host is defined, the SCW can help create a system configuration based specifically on that role. It does not completely get rid of the need to make other configuration changes, though. For more information, please see Security Configuration Wizard for Windows Server 2008 . |
| 3 | There are several methods available to assist you in applying patches in a timely fashion: **Microsoft Update Service**   * Microsoft Update checks your machine to identify missing patches and allows you to download and install them. * This is different than the "Windows Update" that is the default on Windows 2008. Microsoft Update includes updates for many more Microsoft products, such as Office and Forefront Client Security. * This service is compatible with Internet Explorer only.   **Windows AutoUpdate**  OIT offers a Windows Server Update Services Server (WSUS) for campus use using Microsoft's own update servers. It includes updates for additional Microsoft products, just like Microsoft Update, and provides additional administrative control for software deployment.  **Microsoft Baseline Security Analyzer** This is a free host-based application that is available to download from Microsoft . In addition to detailing missing patches, this tool also performs checks on basic security settings and provides information on remediating any issues found. |

|  |  |
| --- | --- |
|  |  |
| 4 | Configure Automatic Updates from the Automatic Updates control panel   * On most servers, you should choose either "Download updates for me, but let me choose when to install them," or "Notify me but don't automatically download or install them." * The campus Windows Server Update Services server can be used as the source of automatic updates. |
| 5 | No further explanation. |
| 6 | Configuring the minimum password length settings is important only if another method of ensuring compliance with the Standard for Password s and Passphrases is not in place. |
| 7 | Configuring the password complexity setting is important only if another method of ensuring compliance with Standard for Passwords and Passphrases is not in place. |
| 8 | The university requires the following event log settings instead of those recommended by the CIS Benchmark:   * Maximum application log size---**50000 KB** * Maximum security log size---**100000 KB** * Maximum system log size---**50000 KB** * Prevent local guests group from accessing application log---**enabled** * Prevent local guests group from accessing security log---**enabled** * Prevent local guests group from accessing system log---**enabled** * Retention method for application log---**Overwrite events older than 14 days** * Retention method for security log---**Overwrite events older than 14 days** * Retention method for system log---**Overwrite events older than 14 days**   These are minimum requirements. The most important log here is the security log - 100 MB is a suggested minimum, but if you have a high-volume service, make the file as large as necessary to make sure at least 14 days of security logs are available. You may increase the number of days that the logs are kept, or you may set the log files to not overwrite events. Note that if the event log reaches its maximum size and no events older than the number of days you specified exist to be deleted or if you have disabled overwriting of events, no new events will be logged. This may happen deliberately as an attempt by an attacker to cover his tracks. For critical services working with Cat 1 or other sensitive data, you may wish to consider log shipping using syslog, Splunk, Intrust, or a similar service. Another option is to configure Windows to rotate event log files automatically when an event log reaches its maximum size as described in the article <http://support.microsoft.com/kb/312571> using the the AutoBackupLogFiles registry entry. |
| 9  – 15 | No further explanation. |
| 16 | The text of the university's official warning banner can be found in the Standard for Server Hardening. You may add localized information to the banner as long as the university banner is included. |
| 17  - 26 | No further explanation. |
| 27 | Configure user rights to be as secure as possible. Every attempt should be made to remove Guest, |

|  |  |
| --- | --- |
|  | Everyone, and ANONYMOUS LOGON from the user rights lists. |
| 28 | Volumes formatted as FAT or FAT32 can be converted to NTFS, by using the convert.exe utility provided by Microsoft. Microsoft has provided instructions on how to perform the conversion **This conversion cannot be reversed.** |
| 29 | IPSec is one method that can limit connections to the server, and it is another standard method by which communication between servers can be encrypted.  IPSec configuration can be managed using the IP Security Policies Snap-In. More information can be found on the Microsoft site. |
| 30 | **Be extremely careful, as setting incorrect permissions on system files and folders can render a system unusable.** |
| 31 | **Be extremely careful, as setting incorrect permissions on registry entries can render a system unusable.** |
| 32 | By default, domain members synchronize their time with domain controllers using Microsoft's Windows Time Service . The domain controller should be configured to synchronize its time with an external time source, such as the university's network time servers.  OIT operates <insert service here> for network time synchronization services for university network administrators. |
| 33 | Download and install Microsoft Forefront Client Security. Microsoft Forefront can be configured directly or through the use of Group Policy Objects (GPOs) . GPOs can simplify the management of multiple servers. |
| 34 | Anti-spyware software is only required to be installed if the server is used to browse websites not specifically related to the administration of the server. At a minimum, SpyBot Search and Destroy should be installed. We also recommend the installation of a secondary anti-spyware application, such as SpyWare Blaster, EMS Free Surfer, or AdAware.  An additional measure that can be taken is to install Firefox with the NoScript and Adblock Plus add-ons  **Spyware Blaster** — Enabling auto-update functionality requires the purchase of an additional subscription.  **SpyBot Search and Destroy**--Automatic update tasks can be created inside the program itself and are scheduled using the Windows Task Scheduler.   1. In the Spybot Application, click on Mode-->Advanced View. 2. Click Settings on the left hand side of the window. 3. You should now see an option labeled "Scheduler." Select that option. 4. Adding the task to update automatically is relatively straightforward.    * Click **Add** to create a task.    * Click **Edit** to edit the task schedule.    * In the Scheduled Task window that pops up, enter the following In the **Run** field:   "C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe" /AUTOUPDATE |

|  |  |
| --- | --- |
|  | /TASKBARHIDE /AUTOCLOSE   * Click the **Schedule** tab and choose a time for it to update. The duration of the update is very brief, but it is processor intensive, so consider scheduling it to occur during periods of low usage. The task should be scheduled daily. |
| 35  – 36 | No further explanation. |
| 37 | 1. Open the Display Properties control panel. 2. Select the Screen Saver tab. 3. Select a screensaver from the list. Although there are several available, consider using a simple one such as "Blank." 4. The value for **Wait** should be no more than 30 minutes. 5. Select the **On resume, password protect** option. |
| 38  – 39 | No further explanation. |
| 40 | Windows provides the Encrypting File System as a built-in mechanism to allow the encryption of individual users' files and folders. Be aware of the caveats involved in the use of EFS before implementing it for general use, though. Other options such as PGP , GNUPG , and [TrueCrypt ] also exist.  Another encryption option to consider is whole-disk encryption, which encrypts the entire contents of the drive instead of just specific files and folders. Windows Vista and Windows 2008 come with BitLocker for this. TrueCrypt can also do whole-disk encryption in addition to file-based encryption. ITS provides WinMagic SecureDoc which is recommended for encrypting laptops.  We strongly recommend that, if encryption is being used in conjunction with Category I data, one of the solutions listed in the Standard for Data Encryption be implemented. |
| 41 | Windows Server 2008 has a feature called Windows Resource Protection which automatically checks certain key files and replaces them if they become corrupted. It is enabled by default. You can audit much more in depth using Tripwire. Modern versions of Tripwire require the purchase of a license. The Tripwire management console can be very helpful for managing more complex installations. |
| 42 | This setting is configured using the Terminal Services Configuration tool. On the General tab of the properties of the RDP connection, select **High** from the list next to encryption level. |

**References**

* UT Austin ISO Windows 2008R2 Server Hardening Checklist

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 4**

**SUBJECT: Security Assessment**

**VERIFICATION TIME: 90 minutes**

**Scenario:**

As part of the sales agreement between our company and our newest major customer, we are required to submit security assessment services that identify the current state of our enterprise network. The Board of Directors is looking forward to reviewing your findings.

**Management Instructions:**

1. Provide Management a discussion ready document reviewing the top three (3) potential risks associated with the following areas:

* Top 3 Risks to each operating system in our local area network. Identify the risk for each operating system.
* Top 3 Risks to each application within our local area network.
* Top 3 Risks pertaining to overall network security of our local area network.

2. You are to perform a security assessment of your local area network and submit your   
 findings with the information in step 1 above. Identify any and all vulnerabilities, and if   
 possible, identify the known CVE # associated with it.

Please write the report so that IT Management can forward it to the Board Members for review in 90 minutes. Please forward this as a professional looking document via established communication channels. Submit as one document!

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | [CVE-2011-0661](https://www.cvedetails.com/cve/CVE-2011-0661/) | [20](https://www.cvedetails.com/cwe-details/20/cwe.html) |  | Exec Code | 2011-04-13 | 2017-09-18 | **10.0** | None | Remote | Low | Not required | Complete | Complete | Complete |
| The SMB Server service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate fields in SMB requests, which allows remote attackers to execute arbitrary code via a malformed request in a (1) SMBv1 or (2) SMBv2 packet, aka "SMB Transaction Parsing Vulnerability." | | | | | | | | | | | | | | | | | | | |
| 2 | [CVE-2011-1268](https://www.cvedetails.com/cve/CVE-2011-1268/) | [20](https://www.cvedetails.com/cwe-details/20/cwe.html) |  | Exec Code | 2011-06-16 | 2017-09-18 | **10.0** | None | Remote | Low | Not required | Complete | Complete | Complete |  |  |  |  |  |
| The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka "SMB Response Parsing Vulnerability." | | | | | | | | | | | | | | | | | | | |
| 3 | [CVE-2011-2013](https://www.cvedetails.com/cve/CVE-2011-2013/) | [189](https://www.cvedetails.com/cwe-details/189/cwe.html) |  | Exec Code Overflow | 2011-11-08 | 2017-09-18 | **10.0** | None | Remote | Low | Not required | Complete | Complete | Complete |  |  |  |  |  |
| Integer overflow in the TCP/IP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code by sending a sequence of crafted UDP packets to a closed port, aka "Reference Counter Overflow Vulnerability." | | | | | | | | | | | | | | | | | | | |

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 15B**

**SUBJECT: DNS Functionality**

**VERIFICATION TIME: 30 MINUTES**

**Scenario:**

Being able to resolve Domain Names is a core function of any network.

Confirm that all Servers can resolve public DNS lookups.

**Description** - Prove this inject was completed by submitting the results of a DNS lookup for "www.google.com" from each server. (The IP Address of results is just fine; screenshots not required.)

**Setup all boxes on network to use 192.168.4.18 as DNS on the LAN and 5.24 as the DNS on the DMZ**

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO #16**

**SUBJECT: Set up and Verify DNS**

**VERIFICATION TIME: 60 minutes**

**Scenario:**

Make sure your DNS server is configured to function appropriately. Take a screen shot of your servers DNS configuration and verify it is able to:

1 Answer queries for addresses within their subnet.

2. Forward to the Internet for outside addresses.

**Setup 2K8R2 box as described in doomsday above and use 8.8.8.8 as primary DNS and 8.8.4.4 as backup**

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 18**

**SUBJECT: Create User Accounts and Group**

**VERIFICATION TIME: 90 MINUTES**

**Scenario**  New users and groups

You are to demonstrate administrative control of your server, users and groups.

1. Create a group on the 2008 R2 server and name it Newgroup.
2. Create two users, PeeWee and Herman
3. Create a screenshot of the new group and users and submit via normal channels

**Follow the instructions. If this takes more than 5 minutes its probably time to raise the white flag.**

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 20**

**SUBJECT: Set Up / Verify Active Directory**

**VERIFICATION TIME: 90 minutes**

**Scenario:** Active Directory Should Be Functional on your Network

As part of the corporate IT policy, Active Directory is required to be functional at all times on the local network. New users, groups, policies, services and devices all play a role in the cohesiveness of network functionality. You are to perform an assessment of your A/D services and report on the status of all services in the following manner:

1. Create a chart of services provided by A/D. Have a column that indicates running services and if that service is running / not running, secured / not secured, monitored / not monitored.
2. Take a screen shot verifying these services as enabled and running and submit with your response.

|  |  |  |  |
| --- | --- | --- | --- |
| Service | Status | Secured? | Monitored? |
| AD DS | Running | Yes | Yes |
| AD LDS |  |  |  |
| AD CS |  |  |  |
| AD FS |  |  |  |
| AD RMS |  |  |  |

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 34**

**SUBJECT: Remote Desktop Capability**

**VERIFICATION TIME: 90 minutes**

**Scenario: Remote Access**

Your organization's employees need remote access to the internal Microsoft Server to access Files and Server Applications. Provide connection instructions and a proper username/password credentials for the remote user to access your system. Submit this information along with a screen shot of it as implemented.

**Setup a user account with limited access and allow RDS connections (GP will need to be changed)**

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 38**

**SUBJECT: Consistent Remote Access**

**VERIFICATION TIME: 90 minutes**

**Scenario:**

Our management has experimented with several administrative remote access methods, for example XDMCP and VNC, but these may not be best. It should also be noted that some staff have implemented unauthorized programs such as GoToMyPC, Webex and Microsoft remote desktop with Dynamic DNS to gain access to our systems.

We need an improved methodology for remote access that provides security and consistency for all employees, while preventing unauthorized use.

**Management Instructions:**

Generate a summary report of all current administrative remote access methods for all of your internal systems, including any unauthorized methods.

Plan and implement a consistent methodology for administrative remote access to our internal systems that also blocks unauthorized access.

Once you have determined the best approach to prevent unauthorized use of these services the admin team will need a quick summary report outlining what solution your team has chosen, why you chose it, and how you’ve implemented it within your environment.

Once you have completed the above, send to the admin team revised administrative remote access instructions. This is needed by the admin team in order to verify proper implementation. You are to determine the appropriate level of access to the admin team, however, understand too little access will not result in too high a score.

You are to identify how you completed this task and what tools or techniques you utilized.

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 41**

**SUBJECT: Room Clean Up**

**VERIFICATION TIME: 15 MINUTES**

**Scenario:**

It’s the end of the qualifier and assessment. All scoring has ceased, and further work on injects will not be judged, except for room cleanup.

To complete this inject your team needs to perform the following tasks:

1. Erase startup configs on the router and switch; erase any vlan.dat file on the team switch. Make sure the router/switch is set for password recovery enable if applicable.
2. Dispose of any trash
3. Erase the white board
4. Place any equipment, CDs, pens, sharpies, License key sheet, dry erase markers, pads of paper, printer paper, etc. on the front table in the room
5. Erase anything on your flash drives that you copied from this event.

**THE TEAM CAPTAIN MUST REMAIN IN THE ROOM UNTIL THE ROOM IS CLEARED BY THE OPERATIONS TEAM.**

**Follow the instructions**

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 24**

**SUBJECT: Set up and install Snort**

**VERIFICATION TIME: 120 minutes**

**Scenario:**

Your CIO wants to show shareholders that he takes security very seriously. The news has been swarming with details of other companies getting hacked recently. To help detect breaches within the company, your CIO would like you to install and configure Snort.

Configure snort, verify traffic monitoring, take a screen shot and submit with your response to the admin team. Someone will come around to verify onsite.

**https://www.snort.org/**

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 27**

**SUBJECT: SSH Account Connectivity**

**VERIFICATION TIME: 90 MINUTES**

**Scenario:**

Recently our company has brought on three new developers to work on commercial portions of our mapping software. As the current economic situation is requiring more cost efficient solutions to be developed, we have decided not to offer a relocation package to the new hires. Access needs to be provided electronically for each employee via SSH to the source code repository allowing for check-in and check-out of different mapping components.

You are to provide three SSH accounts for the following individual users with the following passwords:

User #1: mbuchanan Password: n3tw0rx!

User #2: bschneier Password: (rYpt0guru

User #3: kmitnick Password: s0c!4lENG

These users will need to connect directly to the server serving up the Source Code Repository and need to be accessible 24/7 for committing new code to the current branch as there is a code freeze coming up. Confirm functionality of this service and submit a screen shot with your response. An admin / support team member will be by to verify.

**https://winscp.net/eng/docs/guide\_windows\_openssh\_server**

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 29**

**SUBJECT: Implement\_Secure\_Webmail\_Capability**

**VERIFICATION TIME: 60 minutes**

Please configure secure self signed web-based email capability on one of your unused external IP addresses, X.Y.Z.K, called. Make sure users can get to it from anywhere inside or outside the company. As part of this request you are also asked to create specific instructions regarding the use of this system. Please be prepared to submit two copies of your instructions along with a test user account for verification by corporate personnel. Do not use the same internal email solution you implemented in a previous inject.

This task must be ready for verification within 90 minutes.

Windows Mail Server program – Backup only will need a firewall rule

https://www.hmailserver.com/download\_getfile/?performdownload=1&downloadid=256

**Needs to be set up on DMZ**

**Linux Mail Server Program**

**https://www.tecmint.com/setup-postfix-mail-server-in-ubuntu-debian/**

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 36**

**SUBJECT: Bring On-line and Protect the Database Server**

**VERIFICATION TIME: 60 minutes**

**Scenario:**

We have just had a fire in the secure server room. We believe this fire was the result of arson to cover up a physical intrusion. We believe the target of the intrusion was the secure database server. Your job is to protect this server at all costs. You are to create a database / repository server of your choosing and bring this server on-line and notify the admin team when complete. Submit the internal address of the database server along with a screen shot of it fully implemented. The scoring engine must see this server so access to it through the gateway must be maintained.

**Install MySQL and lock it down**

[**https://dev.mysql.com/downloads/file/?id=474495**](https://dev.mysql.com/downloads/file/?id=474495)

**CYBER DEFENSE QUALIFIER AND ASSESSMENT  
INJECT SCENARIO # 40**

**SUBJECT: Enough is Enough – Hack Back!**

**VERIFICATION TIME: Immediate**

Your CIO has had enough of the bad guys and all of their port scans and excursions into your network. He has decided to take matters into his own hands and has directed you to immediately begin offensive measures against them. He has learned that the ‘bad guys’ are your company’s competitor and he wants you to do anything you can to ‘take them down’. The network address of the bad guys is \_\_x.x.x.x\_\_\_\_\_\_\_\_\_. You may NOT perform any offensive activities against any other network, if you do you will be terminated from employment from the company and may face prosecution from legal authorities.

You are to document each type of offensive action taken against the bad guys and any successes.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP Address Attacked** | **Action Taken (Tools, technique)** | **Team Member Who Took Action** | **Indications of Success (Services disabled, etc)** |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Submit a screen shot of any successful attacks against the target network.