Assignment: Blue Team – 5 Minute Plan

Subject Name: BCYB 650 - Cyber Vulnerability Exploitation

Professor Name: Yusel Celik

University at Albany, SUNY

Submitted by: Mihir Katre

February 08, 2024

Contents

Introduction to blue team.

Blue team refers to a group of people or individuals who are responsible for defending an enterprise or organization's information system by maintaining its security posture against group of attackers (referred to as red team).

Typically, the Blue Team must defend against real or simulated attacks, detect and respond to security incidents and ensure overall security of the system.

What is a 5-minute plan?

A 5-minute plan for blue team is typically a set of initial most common steps or actions to be performed on a system for enhancing the cyber-defense of an organization. A 5-minute plan acts as a starter during a competition or defending a simulated attack where you try to harden your control over a device or a system by implementing strategies such as closing port, locking passwords, disabling services, etc.

5-minute plan

Change the desktop background of the system.

> This step does not contribute to the security, but this can make you look cool by adding a defensive background just to intimidate attackers and show that you are in control.

Change passwords for all users \ lock out fishy users.

> When a blue team is defending a system, a system might consist of users that you are not fully aware about or users whose credentials are already compromised to the attackers, this step helps to be in control of the system accounts.

Command to change password of the users (UNIX systems):

“sudo passwd username” – where username refers to the actual username of the user you want to change the password of.

Command to lock terminal access of the users (UNIX systems):

“sudo chsh -s /usr/sbin/nologin username”

If at the further point of time it is required to provide terminal access to the users:

“sudo usermod --shell /bin/sh username”

For Windows, follow the following steps:

Sign in using an account that has administrator rights.

In Windows, search for and open Control Panel, type User Accounts, and then click User Accounts from the list.

Click Manage another account, Select the local accounts for which password needs to be changed and provide the new password.

Conduct audits for all the user and group permissions.

Many systems have stale users or groups created for specific purposes and then left unattended with a lot of permissions.

Identify the roles and responsibilities of all the users and groups and provide access accordingly using the principle of least privilege.

Example:

In Linux systems:

Use commands such as “getent” or “ls” to view all the user and groups permissions on files and directories.

Give read only access to a specific directory:

“sudo chmod +r /abc /pqr”

Give read only access to a specific user and group on specific directory:

“sudo chown -R lionelmessi:lionelmessi /abc/pqr”

In Windows:

Audit the local user accounts and access provided to them. Disable all the inactive users, add them to appropriate group so that they can only access the directories they need access to.

Check the important file system folders by right clicking on them -> Properties -> Security.

Verify all the groups and users having access and administrative access to these folders and remove all the unnecessary and unidentified users.

Disable the unnecessary or unused services which are running on the system.

Many services run on various ports and applications which can turn out to be an entry point for an attacker to exploit the system.

In Linux, type the command:

“sudo systemctl --type=service --state=running” to view all the running services, and stop and disable the service which are not in use, for example:

“sudo systemctl stop apache.d.service”

“sudo systemctl disable apache.d.service”

Also, check for any automated services or tasks scheduled using cron.

Fire command “crontab -l” to view if any automated cron jobs are scheduled.

In Windows:

Open run and type: “services.msc”

A window opens showing all the running services. Manually navigate through all the services and right click on the service name and stop the service not in use.

Also, check for any automated tasks that might be scheduled or configured inside task scheduler which might be running in the background.

Ensure all the packages and applications on the system are up to date.

Systems usually run a lot of applications and services which are outdated and there are various security patches provided by the vendor which are not applied to the systems, these

outdated versions might have a vulnerability that red-team or any attacker can exploit to damage the system.

In Linux systems:

Fire command: “apt list --upgradable”. This command will show all the packages that need to be upgraded.

Fire command: "sudo apt update -y”.

In Windows systems:

In windows, we do not have a direct one stop shop for upgrading all packages, the updates are divided for application upgrades, windows updates and device driver updates.

This can be tackled by 2 ways:

1. Manually check and monitor all the Window updates which involve security, system and patches.
2. Identify all the installed software and programs that need to be updated.
3. Manually check all the device drivers and BIOS updates that need to be performed.

Or

Install an application such as DriverEasy, this application helps identify all the windows, security, application and driver updates that need to be performed and provides automated way to keep the system up to date.

Check for open ports on the system.

The open ports on the system are usually scanned by attackers to find loopholes and entry points into the system, these open ports are utilized by services running on the system.

Check the open ports on Linux systems:

Command 1: “sudo lsof -nP -iTCP -sTCP:LISTEN”

or

Command 2: "ss -tul”

These commands would provide a detailed summary of open ports, IP’s which they are open on and the services which are utilizing these ports.

Identify the ports or services like apache, ssh, samba, etc.

Disable the services by firing the command:

“sudo systemctl stop servicename.service”

“sudo systemctl disable servicename.service”

Please note: Some services would restart themselves after the system restarts, hence it is essential to disable them.

Check open ports on Windows systems:

Open command prompt from the start menu and fire the command:

“netstat -aon” – This command will provide detailed summary of open ports, IP’s which they are open on and the process IDs which are utilizing these ports.

Identify the unnecessary services, navigate to task manager, processes and filter out the PID which needs to be stopped and disable and disable them.

Check and implement strict firewall rules.

In the previous steps, we have already identified and closed all the unnecessary ports, but we also need to ensure that only authorized traffic comes in and goes out of our system, this can be achieved by implementing appropriate firewall rules.

This also can be achieved in two different ways:

Performing Network Segmentation and implementing firewall between the system and internet or outside network. The advantage of using router-based firewall is, all the traffic can be controlled and monitored through a single entity (router firewall) instead of manually editing Firewall rules into the host Windows and Linux systems.

Most common rule for centralized firewall is: DenyAll rule. Firewall treats all the rules based on the priority number, there should be a DenyAllTraffic rule at the end and other allow firewall rules must be added to prior to these rule.

Examples can be:

AllowHttpOutbound, AllowFTPInbound, AllowSSHOutbound, etc.

Network Segmentation is a complex setup, which in most cases cannot be performed within 5-minute plans or some given environment which is pre-configured on a network. Although, If the system can be pre-configured, the network should be segmented based on the use case.

The network should be divided into purpose specific subnets such as FTP servers, AD servers, Corporate Subnet, DMZ subnet, etc.

If there is no centralized router firewall, these rules must be implemented on the individual systems.

On Linux systems:

Install tools such as iptables or snort to implement strict firewall rules.

Check pre-configured firewall rules in iptables using command:

“sudo iptables -L -v -n”

Block SSH traffic or port 22 from a specific source:

“sudo iptables -A INPUT -s 212.12.4.2 -p tcp –dport 22 -j DROP”

Rules in `iptables` are volatile, meaning they’ll disappear upon reboot unless saved.

Save them using command: “sudo sh -c ‘iptables-save > /etc/iptables/iptables.rules’”

On Windows Systems:

Windows has an inbuilt windows defender firewall to manage and configure firewall rules.

Windows defender firewall is mostly used to configure home networks and there are not many changes to be done here, although you can configure some application to be default blocked by defender firewall.

Make sure to check the DNS servers’ settings for the network which you are connected to. The IP address provided there should be your default gateway address.

To check this, Open CMD and fire command “ipconfig/all”

Attackers most commonly change the DNS server address to a spoofed address, and this results in diverting your internet requests to a different DNS server.

Disable Port Forwarding.

Port forwarding, also known as port management, allows remote servers and devices on the internet to be able to access devices that are on a private network.

There might be several cases where port forwarding is required, for example, a mobile device trying to access CCTV or webcam setup at a home router from anywhere on the internet.

These rules should be monitored vigilantly as direct access from outside sources to the machines on private networks can do a lot of harm. If there is no such requirement, port forwarding should be always disabled.

Start a wireshark capture.

Even after implementation of all the security mechanisms, it becomes very important to monitor all the traffic that comes and goes out of the system.

Download and install Wireshark on the Windows and Linux systems and begin capturing the packets. This will allow you to monitor all the TCP and UDP traffic flowing, and capture packets and requests made.

Monitor and make copies of user and system logs.

Monitoring user and system logs provides insights into user activity, logins, operations they perform, or modifications done. It is very important to monitor these logs to detect malicious activity. It is also important to create a copy of these logs in an unidentified location as the attacker as part of covering their tracks, might delete the logs generated.

For Windows and Linux systems, making use of Splunk can be the best option as it monitors all the log files and provides a unified interface to view the activity.

Cron can be used with Splunk to copy logs from the designated location to a specific folder to create backup of all the logs.

Additionally, Windows Log monitoring can be done using Event Viewer and Windows Security Event logs. These logs provide detailed information about the user, action, timestamp and modification made.

Conclusion

This 5-minute plan just acts as a starting point for defending the systems, it is very important to keep in mind that the red-team or attackers are also aware about all the basics of defending strategies. Hence, it is very essential to try as much as possible to reduce attack surface, keep up to date with attacking strategies, think like an attacker, keep effective communication between the team and assign proper roles.

Make sure to not underestimate any weakness or findings, no matter how prepared you are, your presence of mind and critical thinking would take you miles.