Detection & Prevention

Throughout this module, we have mastered several different techniques that can be used from an `offensive perspective`. As penetration testers, we should also be concerned with the mitigations and detections that can be put in place to aid defenders in stopping these types of TTPs. This is crucial since we are expected to provide our customers with potential fixes or solutions to the issues we find and exploit during our assessments. Some may be:

- Physical hardware changes
- Changes to the network infrastructure
- Modifications to host baselines

This section will cover some of these fixes and what they mean for us and those in charge of defending the network.

Setting a Baseline

Understanding everything present and happening in a network environment is vital. As defenders, we should be able to quickly `identify` and `investigate` any new hosts that appear in our network, any new tools or applications that get installed on hosts outside of our application catalog, and any new or unique network traffic generated. An audit of everything listed below should be done annually, if not every few months, to ensure your records are up to date. Among some of the considerations we can start with are:

Things to Document and Track

- DNS records, network device backups, and DHCP configurations
- Full and current application inventory
- A list of all enterprise hosts and their location
- Users who have elevated permissions
- A list of any dual-homed hosts (more than one network interface)
- Keeping a visual network diagram of your environment

Along with tracking the items above, keeping a visual network diagram of your environment up-to-date can be highly effective when troubleshooting issues or responding to an incident. Netbrain is an excellent example of one tool that can provide this functionality and interactive access to all appliances in the diagram. If we want a way to document our network environment visually, we can use a free tool like diagrams.net. Lastly, for our baseline, understanding what assets are critical to the operation of your organization and monitoring those assets is a must.

People, Processes, and Technology

Network hardening can be organized into the categories *People*, *Process*, and *Technology*. These hardening measures will encompass the hardware, software, and human aspects of any network. Let's start with the `human (People)` aspect.

People

In even the most hardened environment, users are often considered the weakest link. Enforcing security best practices for standard users and administrators will prevent "easy wins" for pentesters and malicious attackers. We should also strive to keep ourselves and the users we serve educated and aware of threats. The measures below are a great way to begin the process of securing the human element of any enterprise environment.

BYOD and Other Concerns

Bring Your Own Device (BYOD) is becoming prevalent in today's workforce. With the increased acceptance of remote work and hybrid work arrangements, more people are using their personal devices to perform work-related tasks. This presents unique risks to organizations because their employees may be connecting to networks and shared resources owned by the organization. The organization has a limited ability to administer and secure a personally owned device such as a laptop or smartphone, leaving the responsibility of securing the device largely with the owner. If the device owner follows poor security practices, they not only put themselves at risk of compromise, but now they can also extend these same risks to their employers. Consider the practical example below to build perspective on this:

> Scenario: Nick is a hardworking and dedicated logistics manager for Inlanefreight. He has put in a lot of great work over the years, and the company trusts him enough to allow him to work from home three days out of the week. Like many Inlanefreight employees, Nick also takes advantage of Inlanefreight's willingness to allow employees to use their own devices for work-related tasks at home and in the office network environments. Nick also enjoys gaming and sometimes illegally torrents video games. One game he downloaded and installed also installed malware that gave an attacker remote access to his laptop. When Nick goes into the office, he connects to the WiFi network that extends access to the employee network. Anyone can reach the Domain Controllers, File Shares, printers, and other important network resources from this network. Because of malware on Nick's system, the attacker also has access to these network resources and can attempt to pivot across Inlanefreight's network due to Nick's bad security practices on his personal computer.

Using `multi-factor authentication` (Something you have, something you know, something you are, location, etc.) are all excellent factors to consider when implementing authentication mechanisms. Implementing two or more factors for authentication (especially for administrative accounts and access) is a great way to make it more difficult for an attacker to gain full access to an account should a user's password or hash get compromised.

Along with ensuring your users cannot cause harm, we should consider our policies and procedures for domain access and control. Larger organizations should also consider building a Security Operation Center (SOC) team or use a `SOC as a Service` to constantly monitor what is happening within the IT environment 24/7. Modern defensive technologies have come a long way and can help with many different defensive tactics, but we need human operators to ensure they function as they are supposed to. `Incident response` is something where we can't yet completely automate out the human element. So having a proper `incident response plan` ready is essential to be prepared for a breach.

Processes

Maintaining and enforcing policies and procedures can significantly impact an organization's overall security posture. It is near impossible to hold an organization's employees accountable without defined policies. It makes it challenging to respond to an incident without defined and practiced procedures such as a `disaster recovery plan`. The items below can help to start defining an organization's `processes`, `policies`, and `procedures` relating to securing their users & network environment.

- Proper policies and procedures for asset monitoring and management
  - Host audits, the use of asset tags, and periodic asset inventories can help ensure hosts are not lost
- Access control policies (user account provisioning/de-provisioning), multi-factor authentication mechanisms
- Processes for provisioning and decommissioning hosts (i.e., baseline security hardening guideline, gold images)
- Change management processes to formally document `who did what` and `when they did it`

Technology

Periodically check the network for legacy misconfigurations and new & emerging threats. As changes are made to an environment, ensure that common misconfigurations are not introduced while paying attention to any vulnerabilities introduced by tools or applications utilized in the environment. If possible, attempt to patch or mitigate those risks with the understanding that the CIA triad is a balancing act, and the acceptance of the risk a vulnerability presents may be the best option for your environment.

From the Outside Moving In

When working with an organization to help them assess the security posture of their environment, it can be helpful to start from the outside and move our way in. As penetration testers and security practitioners, we want our clients to take our findings and recommendations seriously enough to inform their decisions moving forward. We want them to understand that the issues we uncover can also be found by individuals or groups with less honorable intentions. Let's consider this through a mental exercise using the outline below. Feel free to use these burning questions and considerations to start a conversation with friends, team-members or if you are alone, take some notes and come up with the most secure design you can think of:

Perimeter First

- `What exactly are we protecting?`
- `What are the most valuable assets the organization owns that need securing?`
- `What can be considered the perimeter of our network?`
- `What devices & services can be accessed from the Internet? (Public-facing)`
- `How can we detect & prevent when an attacker is attempting an attack?`
- `How can we make sure the right person &/or team receives alerts as soon as something isn't right?`
- `Who on our team is responsible for monitoring alerts and any actions our technical controls flag as potentially malicious?`
- `Do we have any external trusts with outside partners?`
- `What types of authentication mechanisms are we using?`
- `Do we require Out-of-Band (OOB) management for our infrastructure. If so, who has access permissions?`
- `Do we have a Disaster Recovery plan?`

When considering these questions regarding the perimeter, we may face the reality that an organization has infrastructure that could be based on premises &/or in the cloud. Most organizations in the modern day operate hybrid-cloud infrastructures. This means some of the technologies used by organizations may be running on network & server infrastructure owned by the organization, and some may be hosted by a 3rd party cloud provider (AWS, Azure, GCP, etc.).

- External interface on a firewall
  - Next-Gen Firewall Capabilities
    - Blocking suspicious connections by IP
    - Ensuring only approved individuals are connecting to VPNs
    - Building the ability to quick disconnect suspicious connections without disrupting business functions

Internal Considerations

Many of the questions we ask for external considerations apply to our internal environment. There are a few differences; however, there are many different routes for ensuring the successful defense of our networks. Let's consider the following:

- `Are any hosts that require exposure to the internet properly hardened and placed in a DMZ network?`
- `Are we using Intrusion Detection and Prevention systems within our environment?`
- `How are our networks configured? Are different teams confined to their own network segments?`
- `Do we have separate networks for production and management networks?`
- `How are we tracking approved employees who have remote access to admin/management networks?`
- `How are we correlating the data we are receiving from our infrastructure defenses and end-points?`
- `Are we utilizing host-based IDS, IPS, and event logs?`

Our best chance of spotting, stopping, and potentially even preventing an attack often depends on our ability to maintain visibility within our environment. A proper SIEM implementation to correlate and analyze our host and infrastructure logs can go a long way. Combine that with adequate network segmentation, and it becomes infinitely more challenging for an attacker to gain a foothold and pivot to targets. Simple things like ensuring Steve from HR cannot view or access network infrastructure such as switches and routers or admin panels for internal websites can prevent the use of standard users for lateral movement.

MITRE Breakdown

As a different look at this, we have broken down the major actions we practice in this module and mapped controls based on the TTP and a MITRE tag. Each tag corresponds with a section of the Enterprise ATT&CK Matrix found here. Any tag marked as `TA` corresponds to an overarching tactic, while a tag marked as `TA###` is a technique found in the matrix under tactics.

TTP	MITRE Tag	Description
External Remote Services	T1133	We have options for prevention when dealing with the use of External Remote Services. `First`, having a proper firewall in place to segment our environment from the rest of the Internet and control the flow of traffic is a must. `Second`, disabling and blocking any internal traffic protocols from reaching out to the world is always a good practice. `Third`, using a VPN or some other mechanism that requires a host to be `Logically` located within the network before it gains access to those services is a great way to ensure you aren't leaking data you shouldn't.
Remote Services	T1021	Multi-factor authentication can go a long way when trying to mitigate the unauthorized use of remote services such as SSH and RDP. Even if a user's password was taken, the attacker would still need a way to acquire the string from their MFA of choice. Limiting user accounts with remote access permissions and separating duties as to who can remotely access what portions of a network can go a long way. Utilizing your networked firewall and the built-in firewall on your hosts to limit incoming/outgoing connections for remote services is an easy win for defenders. It will stop the connection attempt unless it is from an authorized internal or external network. When dealing with infrastructure devices such as routers and switches, only exposing remote management services and ports to an Out Of Band (OOB) network is a best practice that should always be followed. Doing this ensures that anyone who may have compromised the enterprise network cannot simply hop from a regular user's host into the infrastructure.
Use of Non-Standard Ports	T1571	This technique can be a tricky one to catch. Attackers will often use a common protocol such as `HTTP` or `HTTPS` to communicate with your environment. It is hard to see what is going on, especially with the use of HTTPS, but the pairings of protocols such as these with a non-standard port (`444` instead of `443`, for example) can tip us off to something suspicious happening. Attackers will often try to work in this manner, so having a solid `baseline` of what ports/protocols are commonly used in your environment can go a long way when trying to spot the bad. Using some form of a Network Intrusion Prevention or Detection system can also help spot and shut down the potentially malicious traffic.
Protocol Tunneling	T1572	This is an interesting problem to tackle. Many actors utilize protocol tunneling to hide their communications channels. Often we will see things much like we practiced in this module (tunneling other traffic through an SSH tunnel) and even the use of protocols like DNS to pass instructions from external sources to a host internal to the network. Taking the time to lock down what ports and protocols are allowed to talk in/out of your networks is a must. If you have a domain running and are hosting a DC & DNS server, your hosts should have no reason to reach externally for name resolution. Disallowing DNS resolution from the web (except to specific hosts like the DNS server) can help with an issue such as this. Having a good monitoring solution in place can also watch for traffic patterns and what is known as `Beaconing`. Even if the traffic is encrypted, we may possibly see requests happening in a pattern over time. This is a common trait of a C2 channel.
Proxy Use	T1090	The use of a Proxy point is commonplace among threat actors. Many will use a proxy point or distribute their traffic over multiple hosts so that they do not directly expose their infrastructure. By using a proxy, there is no direct connection from the victim's environment to the attacker's host at any given time. The detection and prevention of proxy use is a bit difficult as it takes an intimate knowledge of common net flow within your environment. The most effective route is maintaining a list of allowed/blocked domains and IP addresses. Anything not explicitly allowed will be blocked until you let the traffic through.
LOTL	N/A	It can be hard to spot an attacker while they are utilizing the resources on hand. This is where having a baseline of network traffic and user behavior comes in handy. If your defenders understand what the day-to-day normal for their network looks like, you have a chance to spot the abnormal. Watching for command shells and utilizing a properly configured EDR and AV solution will go a long way to providing you visibility. Having some form of networking monitoring and logging feeding into a common system like a SIEM which defenders check, will go a long way to seeing an attack in the initial stages instead of after the fact.