Where Technology Means More®

A Pen Tester's Advice for Minimizing Your Attack Surface

By: **Mike D'Arezzo**,
Director of Security Services

Penetration testing, or pen testing, which is a simulated cyberattack, is a great way to increase the security maturity for your organizational infrastructure. But you don't have to wait for a penetration test to improve your defenses. Some attack-surface vulnerabilities are common and easily remediated without waiting for an ethical hacker's after-action report.

Follow my 6 pen tester-tested suggestions, and you will be on your way to taking your security strategy to the next level.

1. Understand what is in your environment

Why do I need to do this? "Know Thyself."

The first rule of protecting an environment or operation is knowing what is within that operation – you simply cannot protect that which you do not know exists. This is the single most important task here and is constantly in motion. Adding visibility to your network provides the information you need to identify vulnerabilities. Proper visibility allows you to monitor endpoints, for example, and determine if network policies are being enforced. It also allows you to monitor databases to understand what data is being stored.

How do I fix this issue? An asset manager or other process monitor allows you to collect data on your network and environment to include data, processes, and users. If someone plugs in an unrecognized endpoint or is trying to circumvent your security controls, it should raise an alarm! An asset manager can serve as an early warning system for your network by tracking assets from initial onboarding to end-of-life. Ideally, it gives you visibility into data silos, privileges, and user configurations and allows you to set baseline security protocols and policies.

What if I do nothing? Hackers can exploit what you don't know, compromise endpoints, take over resources, install dangerous applications, and move laterally from environment to environment. These vulnerabilities increase your attack surface.

2. Remove unnecessary ports and services

Why do I need to do this? Any port or service that faces the public internet is scanned by cybercriminals and state-sponsored hacking rings. Most of these vulnerabilities are scanned twice within the first 15 minutes of going live on your public facing network.

Hackers scan networks because they want to know if their ports are open, closed, or filtered. By mapping ports, they can look for weak spots in your security.

How do I fix this issue? A port scanner can identify active hosts, scan for open ports, and create a database of known ports. With this information, you can close ports that are not in use to lessen the chance of intrusion. Since ports are often opened for legitimate purposes, it is worthwhile to routinely rescan your network to see if any connections have been accidentally left open.

Make sure all open ports are active for a valid business reason. There is always a concern that closing a port will have unintended business consequences, but you cannot let this concern put infrastructure at-risk.

Implement a change management program to track the open ports and services (among other things) to apply those business reasons to the open port. You should be able to see a configuration on your network and think “Oh, that is there because of program X.”

e+

Where Technology Means More®

2. Remove unnecessary ports and services

What if I do nothing? When hackers scan ports, they are first conducting reconnaissance on your network. They are mapping open ports, identifying servers, and determining which services are vulnerable to attack. They are using other software to determine if your patches are up-to-date or ripe for exploit.

Under the right circumstances, they can use this information to access your network and begin their attack strategy. Bottom line: – open ports that have no legitimate purpose increase your attack surface risk!

e+
Where Technology Means More®

3. Enforce network access control

Why do I need to do this? More workers are on-the-go, even within the office. Often, they are relying on wireless access points to provide network connectivity but wireless networks aren't only limited to the four walls of your office.

Why is it a problem? Wireless network access points are convenient, but they can bypass your physical security perimeter and allow hackers to gain access to your network – even from the parking lot! Even a secure wireless network can be spoofed by Hackers use powerful radio devices, such as Wi-Fi Pineapple, to spoof wireless connections, create fake log-in web pages, and intercept end-user traffic. This sort of indirect attack allows hackers to impersonate legitimate devices and de-authenticate users (using deception to steal credentials) and other types of attacks.

How do I fix this issue? Network access control provides processes and tools for monitoring and authorizing network and network connected devices. They can help to ensure that only legitimate users and devices are able to connect with your resources and that all over-the-air traffic is compliant with the Advanced Encryption Standard or similar criteria.

4. Limit opportunities for in-person social engineering

Why do I need to do this? Hackers use this strategy if the potential rewards are large enough. To gain access to a facility, they probably have to bypass security barriers such an automatic door or a guard station.

Social engineering hackers are masters of human behavior. They may insinuate themselves into a group by joining a conversation at a smoking station or outdoor break area, for example. They know how to overcome reservations and piggyback on group trust to breach physical perimeters.

Once inside a building, these hackers look for open workstations, unlocked computers, or labeled network port in empty conference rooms. They sometimes pretend to be part of IT and parley that position of trust to co-op the login credentials of non-technical staff.

Why is it a problem? Innately, most of us want to help people who look like they're in need – especially when they look like they're carrying heavy boxes, look upset, or seem worried. Some bad people intentionally take advantage of this human trait to enter buildings or areas where sensitive information or systems are kept. Ever see someone carrying heavy boxes and try to open a door while balancing a laptop bag? Most people won't even think twice about helping that person and holding the door open for them but this may actually be an attempt to gain access to the building or room.

e+ Where Technology Means More®

4. Limit opportunities for in-person social engineering

How do I fix this issue? Helping people should not stop you from being secure! Ask the person who they are and ask who they work for in the building. Escort them to the person or walk them over to the reception/ visitor's desk. Asking simple questions can sometimes be the best deterrent to someone who may only know the name of the CEO or Vice President of Information Technology. Escorting them directly to that person eliminates opportunities.

The best way to achieve defending against these types of attacks is through frequent and ongoing worker training. Social engineering uses trust as a weapon. To protect valuable assets, you have to help workers develop a healthy mistrust of unannounced visitors, friendly strangers, and seemingly helpful technicians.

e+ Where Technology Means More®

5. Segment network to improve inside-the-perimeter security

Why do I need to do this? Many attacks focus on traversing the publicly accessible network and entering a secured perimeter and then moving laterally through the network to steal and/or encrypt data.

Why is it a problem? Without proper segmentation an attacker can quickly go from the external , public network to your data center. Movement around the network can provide the attacker with information about where valuable data is stored.

Without access control and segmentation the attack may remain undetected until compromised traffic crosses the network firewall.

How do I fix this issue? Creation of virtual local area networks (VLANs) and access control between nodes used to be difficult, but new tools allow you to create network segments and even micro segmentation to block unauthorized activity before attacks can spread or data is removed, deleted, changed, or encrypted.

Control on network segments help prevent unauthorized devices and users from accessing sensitive or valuable resources, such as shared folders and domain or database servers. It also provides an early warning system that your defenses are being tested and that heighten vigilance is needed to discourage further attempts.

6. Require strong passwords and multi-factor authentication

Why do I need to do this? Login credentials are stolen all the time. And workers often use similar if not identical logins across multiple sites and accounts. Hackers take advantage of both these vulnerabilities to launch credential stuffing attacks.

Credential stuffing occurs when hackers combine stolen credentials with brute force algorithms to try to "guess" their way past security. When a match occurs, the hackers are able to begin infiltrating the compromised network.

Why is it a problem? Hackers are focused on earning a payday. And credential stuffing allows them to be more efficient while using fewer resources. Hackers are unlikely to abandon this strategy as long as it continues to be an effective way of gaining access to secure resources.

How do I fix this issue? Multi-factor authentication can put a stop to credential stuffing. Even if hackers have all your credentials, they won't be able to access any resources without the multi-factor code. With this approach, you are introducing an additional layer of defense for frustrating attackers.

While it is possible for hackers to intercept the text messages or mobile phone that transmits temporary authentication credentials, this theft requires much more effort. Most hackers will probably shift to less protected networks. End users may grumble about having to enter a temporary code along with their username and password, but organizations can implement Identity Access programs that can minimize the necessity to enter MFA every time a login is required.

Where Technology
Means More®

eplus-security@eplus.com

www.eplus.com/security

ePlus Technology | 13595 Dulles Technology Drive | Herndon, VA 20171