10.2 Conducting an Initial Assessment

Disaster recovery, access rights, and appropriate policies are topics that are often overlooked by those new to security. To keep it simple and easy to remember, the stages of assessing a system's security can be separated into the "Six Ps":

- Patch
- Ports
- Protect
- Policies
- Probe
- Physical

You should note that these Six Ps are not yet standards in the security industry. They are provided here as a framework for approaching system security.

10.2.1 Patches

Patching a system is perhaps the most fundamental part of security. Therefore, when assessing any system's security, you should check to see whether a procedure is in place to govern the routine updating all patches. You should also, of course, check to see that the machines have current patches and updates. A written policy is essential, but when performing a security audit, you need to ensure that those policies are actually being followed.

As you are aware, operating system and application vendors occasionally discover security flaws in their products and release patches to correct these flaws. Unfortunately, it is quite common in organizations to find patches that have not been applied as late as 30 days or more after their release.

10.2.2 Ports

All communication takes place via certain ports (TCP/UDP). This is also the case for many virus attacks. Virus attacks will frequently utilize an uncommon port to gain access to your system. Recall that ports 1 through 1024 are assigned and used for well-known protocols. We have examined viruses, Trojan horses, and other dangers that operate

on specific port numbers. If those ports are closed, then your vulnerability to these specific attacks is significantly reduced.

Unfortunately, some system administrators do not make policies to close unused ports. This is probably due to the fact that many administrators think that if the firewall is blocking certain traffic, then there is no need to block that port on individual machines. However, this approach provides you only with perimeter security, not layered security. By closing ports on individual machines, you provide a backup in case the firewall is breached.

As a rule, any port you do not explicitly need for operations should be closed, and communication should be disallowed on this port. A port is usually associated with a service. For example, an FTP service is often associated with ports 21 and 20. In order to close a port on an individual machine, you would need to shut down the service that uses that port. This means those unused services on servers and individual workstations should be shut down.

Both Windows and Linux have built-in firewall capability that will block certain ports. This means in addition to shutting down the particular unneeded services on all client machines, you should also shut down the ports.

Unused router ports should also be shut down in your network. If your network is part of a larger wide-area network (WAN), then it is likely you have a router connecting you to that WAN. Every open port is a possible avenue of entry for a virus or intruder. Therefore, every port you can close is one opportunity less, for such attacks to affect your system.

The specifics of how to close a port on a router are particular to the individual router. The documentation that came with your router or your vendor should be able to provide you with specific instructions on how to accomplish this. If you have a vendor servicing your router, then you should make a list of all required ports and request that the vendor closes all other ports on the router.

10.2.3 Protect

The next phase is to ensure that all reasonable protective software and devices are employed. This means having at least a firewall between your network and the outside world. Clearly, more advanced firewalls such as stateful packet inspection firewalls are preferred.

When auditing a system, you must note whether the system has a firewall or not and also what type of firewall it has. You should also consider using an intrusion detection system (IDS) on that firewall and any web servers.

However, IDSs are the only way to know of imminent attacks. There are free, open source IDSs available. For this reason, most experts highly recommend them. The firewall and IDS will provide basic security to your network's perimeter, but virus scanning is also needed. Each and every machine, including servers, must have a virus scanner that is updated regularly. The point that virus infections are the greatest threat to most networks has been stated boldly. As also previously discussed, it is probably prudent to consider anti-spyware software on all of your systems. This will prevent users of your network from inadvertently running spyware on the network.

Finally, a proxy server is also a very good idea. It not only masks your internal IP addresses, but allows you to discover what websites users visit, also allowing you to place filters on certain sites. Many security experts consider a proxy server to be as essential as a firewall.

In addition to protecting your network, you must also protect data that is transmitted, particularly outside your network. All external connections should be made via a VPN. Having data encrypted prevents hackers from intercepting the data via a packet sniffer. For more secure locations, you may even look for internal transmissions to be encrypted also.

In short, when assessing the protection of the network, check to see whether the following items are present, properly configured, and functioning:

- Firewall
- Antivirus protection
- Anti-spyware protection
- IDS
- Proxy server or NAT
- Data transmissions encryption

Be aware that the first two items are met in most networks. Any network that does not have a firewall or antivirus software is so substandard that the audit should probably stop at that point. In fact, it is unlikely that such an organisation would even bother to have a

security audit. The IDS and data encryption options are probably less common; however, they should be considered for all systems.

10.2.4 Physical

In addition to securing your network from unwanted digital access, you must also ensure that it has adequate physical security. The most robustly secure computer that is left sitting unattended in an unlocked room is not secure at all. You must have some policy or procedure governing the locking of rooms with computers as well as the handling of laptops, tablets, and other mobile computer devices. Servers must be in a locked and secure room with as few people as possible having access to them. Backup tapes should be stored in a fireproof safe. Documents and old backup tapes should be destroyed before disposal (e.g., by melting tapes, de-magnetizing hard disks, breaking CDs).

Physical access to routers and switches should also be tightly controlled. Having the most high-tech, professional information security on the planet but leaving your server in an unlocked room to which everyone has access is a recipe for disaster. One of the most common mistakes in the arena of physical security is co-locating a router or switch in a janitorial closet. This means that, in addition to your own security personnel and network administrators, the entire cleaning staff has access to your router or switch, and any one of them could leave the door unlocked for an extended period of time.

Here are some basic rules you should follow regarding physical security:

- **Server rooms:** The room where servers are kept should be the most fire-resistant room in your building. It should have a strong door with a strong lock, such as a deadbolt. Only personnel who actually have a valid reason to enter in the room should have a key. You might also consider a server room log wherein each person logs in when they enter or exit the room. There are also electronic locks that record who enters a room, when they enter, and when they leave. Consult local security vendors in your area for more details on price and availability.
- **Workstations:** All workstations should have an engraved identifying mark. You should also routinely monitor them. It is usually physically impossible to secure them as well as you

secure servers, but you use this step to potentially improve their security.

- **Miscellaneous equipment:** Projectors, CD burners, laptops, and so forth should be kept under lock and key. Any employee that wishes to use one should be required to sign it out. It should be also checked to see that it is in proper working condition and that all parts are present when it is returned.

These measures should be considered by all organisations. Some organisations go much further in ensuring physical security. Most are probably more extreme than businesses require. However, if you are dealing with highly sensitive or classified data, then you might want to consider some or all of these measures:

- Biometric locks to all server rooms, or equipment storage rooms. Such locks are triggered by a fingerprint scan, and the identity of the person as well as the time they entered the room are recorded.
- All visitors to the building are logged in (both their entry and exit time) and are escorted by an employee at all times.
- All bags are inspected when personnel leave, or at least some bags are inspected at random.
- No portable devices that might record data are allowed on the premises. This includes USB drives, camera phones, or any device that might copy data or record screen images.
- All printing is logged. Who printed, the time the printing occurred, the document name, and the document size.
- All copying is logged, similarly to printing.

If you are in a situation that demands a greater level of security than normal, these measures may be considered.