Security Applications and Devices

Software Firewalls

Personal Firewalls

These are software-based applications that protect just a single computer or server from unwanted Internet traffic. Now, these are also referred to as host-based firewalls. These firewalls work by applying a set of rules and policies against traffic that's attempting to come into or go out of our protected computer.

Windows firewall

One is a basic version that's found within your control panel, and then there's a more advanced version called the Windows firewall with advanced security. This advanced firewall can be accessed by typing wf.msc at the command prompt. The basic firewall is useful for most home users, while the more advanced version is well-suited for businesses and systems where more in-depth configurations of your inbound and outbound traffic is required.

OSX - PF and IPFW firewalls

A basic version of the firewall is accessed through the system preference panel under the security and privacy panel. In addition to the graphic user interface-based firewall, there's also a command line version. This version is called PF for packet filter. It's available in OSX 10.10 and higher operating systems. Packet filter is the name because it's essentially what a firewall is designed to do. It filters packets. In older versions of OSX, there was a different command line firewall used called IPFW, which stood for Internet protocol firewall, but that program was replaced by PF for most modern versions of the OSX operating system. Both PF and IPFW are also used in the FreeBSD operating system, which is what OSX is actually based on.

Linux - iptables

In Linux systems, this program is called iptables and can be configured from the command line using different accept and reject rules based upon the type of network traffic that's expected and the port being utilized for that communication.

IDS

Host-based Intrusion Detection System(HIDS)

This usually takes the form of a piece of software that's installed on your computer or on a server and it will protect it. Now, the host-based Intrusion Detection System will sit there and log everything that it thinks is suspicious.

Network-based Intrusion Detection System(NIDS)

This is a piece of hardware that's installed on your network. And all the traffic goes through that switch, and then it will get a copy of that sent down to the Network Intrusion Detection System. If it's suspicious, it'll log it and it'll alert on it.

Alert Types

1. signature-based
2. policy-based
3. anomaly-based detection

Data loss prevention

Data loss prevention is set up to monitor the data of a system while it's in use, in transit, or at rest. These systems come as either software or hardware solutions.

Endpoint DLP system

An endpoint system is usually a piece of software that's installed on a workstation or a laptop, and it's going to monitor the data that's in use on that computer. And if someone tries to do a file transfer, it'll either stop that file transfer, or it'll alert the admin of the occurrence based on certain rules and policies. Very much like an IDS or an IPS would, but focused on data. DLPs can be set to detection mode or prevention mode.

Network DLP system

This is a piece of software or hardware that's a solution placed at the perimeter of your network. It's sole function in life is to check all of the data going into and out of your network, with a special focus on things going out of the network. They want to detect data in transit that shouldn't be leaving the building.

Storage DLP

This is a software that's installed on a server in the data center and inspects the data while its at rest on the server. This is usually because they've encrypted it or watermarked it, and we want to make sure that nobody's accessing the data at times that they shouldn't be.

Cloud-based DLP system

These systems are usually offered as software-as-a-service, and it's part of your cloud service and storage needs. They're going to protect your data when it's stored inside those cloud services.

Bios

BIOS is a type of firmware which is software on a chip.

The BIOS stands for the basic input output system. It's firmware that provides the computer's instructions for how it's going to accept input and send output. So, anytime the motherboard is going to talk to a keyboard, a mouse, a network card, a hard drive, a video card, whatever it is, it has to have instructions on how to do that. That's what the BIOS provides.

Now, most modern computers don't have a traditional or legacy BIOS anymore. Instead, they use a U-E-F-I, or UEFI, known as the Unified Extensible Firmware

Interface, but it's essentially the same thing. It's just more of an updated and robust version of it.

Flashing the BIOS

Flashing the BIOS is simply ensuring that it has the most up-to-date software on that chip. Because it's firmware, you have to do a process called flashing the BIOS to upgrade the BIOS.

BIOS password

This'll prevent anyone from being able to log into the BIOS and change the boot order or other settings without having this administrative password.

BIOS’ boot order

As you can see here on the screen, I've deselected the disk drive, the CD drive, and the USB drive. I only want to be able to boot from the internal hard disk and then from the network card. This helps me protect somebody from putting in a bootable distribution of a Linux CD or something like that and taking control of my computer. If I control the boot order, I control what's loaded.

Disable any external ports and devices

For example, do you still use a parallel port? Most people don't, and so you should disable it. The same thing happens with a serial port. No one really uses them anymore. We use USB, so you can disable it. You might have an onboard network card that you don't use. Whatever you're not using, you should always disable. It's one less thing for somebody to use as part of their attack.

Secure boot

When you enable the secure boot option, your computer is going to go through additional processes as it boots up. When the BIOS or the UEFI is loaded, it's going to go through and load the public key from the trusted platform module chip, known as the TPM, that's sitting inside your processor. It's going to use this to verify the code of the operating system that's being loaded and ensure that it's been digitally signed by the manufacturer and that it hasn't been modified since.

Securing Storage Devices

- USB thumb stick that already has hardware encryption built in
- removable media controls
  - Ex: technical controls inside your group policies

- administrative controls
  - policies

- NAS - Network Attached Storage device
  - These storage devices connect directly into your organization's network
  - NAS systems are going to implement some form of a RAID array that gives you high availability

- Storage Area Network or a SAN
  - A SAN is a network designed specifically to perform block storage functions and it may consist of many NAS devices connected together

Disk Encryption

Two types of encryption:

- hardware-based
- software-based

Hardware-based Encryption

ex: self-encrypting drive. It looks like an external hard drive and it has embedded hardware that performs full disk or whole disk encryption. These are very fast, unfortunately, they're also very expensive, so they're not commonly used.

Software-based Encryption

- **Mac**. On a Mac, we have a system called FileVault where we can turn on whole disk encryption with a single click. This is located under your system preferences and under the security tab.
- **Windows.** On Windows, we use a system called BitLocker. BitLocker, again, is very easy to turn on. If I want to encrypt my D drive I simply right-click it, turn on BitLocker, and then I'll be able to encrypt the entire drive with a single click.
  BitLocker specifically, you're actually going to be using a hardware key that resides on your motherboard. It's called the **Trusted Platform Module, or TPM**.

  This TPM chip resides on the motherboard and it contains the encryption key inside of it.

Both BitLocker and FileVault use the same type of encryption. They use Advanced Encryption Standard, also known as AES. AES is a symmetric key encryption that supports 128-bit and 256-bit keys and is considered unbreakable as of the time of this recording.

Drawbacks

Encryption adds additional security for us, but it comes with a lower performance for your system. If I'm doing whole disk encryption, that means before I can even boot up the computer and read things from that drive, I have to decrypt it, and that takes time and processing. So, you have to remember there is a sacrifice in speed and performance when you're using full disk encryption. Because of this performance hit, some people decide not to use full disk encryption. Instead, they rely on file-level encryption. In Windows, we use a system called **EFS** or the Encrypting File System.

Counter

But going back to our security performance issue, there is a way that we can speed up encryption. We can use hardware-based encryption. It's much faster than using software-based encryption because we have dedicated hardware to do the processing for us. One of the ways we do that is using a hardware security module, or **HSM**.

An HSM is a physical device that acts as a secure cryptoprocessor during the encryption process or during digital signing, which is also an encryption process. HSMs come in many forms, but most commonly you'll see them as an adapter card that plugs in through a USB or a network-attached device.

Endpoint Analysis

An endpoint is simply any device that we may use to connect to our network. Now, for example, your desktop or your laptop at the office, that's considered an endpoint, so is your smartphone or your tablet. As a cybersecurity analyst, you must be able to use tools to identify behavioral anomalies and then identify the techniques used by malware to achieve privilege escalation and persistence on your host.

Now, there are lots of different endpoint protection tools out there

These are

- antivirus AV
- host intrusion detection systems IDS
- host intrusion prevention systems IPS
- endpoint protection platforms EPP
- endpoint detection response platforms EDR
- user and entity behavioral analytics UEBA

AV

Antivirus is a software that's capable of detecting and removing virus infections. And in most cases, other types of malware, such as worms, Trojans, rootkits, adware, spyware, password crackers, network mappers, denial of service tools, and others. Often, you'll hear this called antivirus or anti-malware.

Host-based IDS and IPS - HIDS or HIPS

This is a type of IDS or IPS that monitors a computer system for unexpected behavior and drastic changes to the system state on a given endpoint. Now, most of these are going to use signature-based detection using log or file monitoring systems to figure out if something bad is trying to happen to your endpoint. They may use file system integrity monitoring too to see if your operating system files have been changed, or drivers have been changed, or an application has been changed. All of these things are things that a host-based intrusion detection system or intrusion prevention system can help you with that a network-based intrusion detection or intrusion prevention system really can't see.

EPP

This is a software agent and monitoring system that performs multiple security tasks. They can do things like antivirus. They can do host intrusion detection or prevention systems. It can have a firewall. It can have data loss prevention, or DLP, and it can have file encryption, all of this in a single product. Essentially, it's your Swiss army knife of security tools. We call this an EPP. Now, there are a lot of EPPs on the market and every year, there's a thing called the Magic Quadrant that's put out by Gartner. Gartner goes and rates all the different systems to see who's the best, which ones are the leaders, who are the challengers, who of them are niche players, and who of them are visionaries. The top three is Microsoft, CrowdStrike, and Symantec.

EDR

Now, where EPP is mostly based on signature detection, EDR is focused more on behavioral and anomaly analysis. It starts logging the endpoint's observables and indicators and combines that with analysis and tries to figure out what's wrong. So, this is a software agent that's going to collect system data and logs for analysis by monitoring the system to provide early detection of threats. Now, because of that, the aim of EDR is not to prevent an initial execution, but instead, to provide runtime and historical visibility into a compromise, and once you've been detected, it can start responding to that and it helps you as an incident responder to gather more information and facilitate your remediation to get it back to its original state.

UEBA

This is a system that can provide automated identification of suspicious activity by user accounts and computer hosts Now, this solution is less about endpoint data collection and more about the actual process of analyzing the data you're getting. The idea here is to have a baseline of good knowledge, and then we're going to compare anything that goes outside that baseline and start thinking that might be suspicious and look into it further. Now, a lot of UEBA is focused on the analytics and because of that, there's a lot of data that has to be processed. So, UEBA solutions are heavily dependent on advanced computing techniques, things like artificial intelligence and machine learning. There's a lot of these different players out there in the marketplace that are doing UEBA. Two of the big ones out there right now is Microsoft and **Splunk**. Microsoft has the **Microsoft Advanced Threat Analytics**.

What’s next

Many companies are starting to market **advanced threat protection-ATP**, **advanced endpoint protection-AEP**, and **NextGen AV**, which is **NGAV**, and all of this just becomes essentially a hybrid of the different technologies we talked about before, like the endpoint protection platform, the endpoint detection response, or the user and entity behavior analytics.