Chapter 4: Protecting the Organization

This chapter covers some of the technology and processes used by cybersecurity professionals when protecting an organization’s network, equipment and data. First, it briefly covers the many types of firewalls, security appliances, and software that are currently used, including best practices.

Next, this chapter explains botnets, the kill chain, behavior-based security, and using NetFlow to monitor a network.

The third section discusses Cisco’s approach to cybersecurity, including the CSIRT team and the security playbook. It briefly covers the tools that cybersecurity professionals use to detect and prevent network attacks.

Firewall Types

A firewall is a wall or partition that is designed to prevent fire from spreading from one part of a building to another. In computer networking, a firewall is designed to control, or filter, which communications are allowed in and which are allowed out of a device or network, as shown in the figure. A firewall can be installed on a single computer with the purpose of protecting that one computer (host-based firewall), or it can be a stand-alone network device that protects an entire network of computers and all of the host devices on that network (network-based firewall).

Over the years, as computer and network attacks have become more sophisticated, new types of firewalls have been developed which serve different purposes in protecting a network. Here is a list of common firewall types:

- **Network Layer Firewall** – filtering based on source and destination IP addresses
- **Transport Layer Firewall** –filtering based on source and destination data ports, and filtering based on connection states
- **Application Layer Firewall** –filtering based on application, program or service
- **Context Aware Application Firewall** – filtering based on the user, device, role, application type, and threat profile
- **Proxy Server –** filtering of web content requests like URL, domain, media, etc.
- **Reverse Proxy Server –** placed in front of web servers, reverse proxy servers protect, hide, offload, and distribute access to web servers

- **Network Address Translation (NAT) Firewall** – hides or masquerades the private addresses of network hosts
- **Host-based Firewall** – filtering of ports and system service calls on a single computer operating system

Port Scanning

Port-scanning is a process of probing a computer, server or other network host for open ports. In networking, each application running on a device is assigned an identifier called a port number. This port number is used on both ends of the transmission so that the right data is passed to the correct application. Port-scanning can be used maliciously as a reconnaissance tool to identify the operating system and services running on a computer or host, or it can be used harmlessly by a network administrator to verify network security policies on the network.

For the purposes of evaluating your own computer network's firewall and port security, you can use a port-scanning tool like Nmap to find all the open ports on your network. Port-scanning can be seen as a precursor to a network attack and therefore should not be done on public servers on the Internet, or on a company network without permission.

To execute an Nmap port-scan of a computer on your local home network, download and launch a program such as Zenmap, provide the target IP address of the computer you would like to scan, choose a default scanning profile, and press scan. The Nmap scan will report any services that are running (e.g., web services, mail services, etc.) and port numbers. The scanning of a port generally results in one of three responses:

- **Open or Accepted –** The host replied indicating a service is listening on the port.
- **Closed, Denied, or Not Listening –** The host replied indicating that connections will be denied to the port.
- **Filtered, Dropped, or Blocked –** There was no reply from the host.

To execute a port-scan of your network from outside of the network, you will need to initiate the scan from outside of the network. This will involve running an Nmap port-scan against your firewall or router's public IP address. To discover your public IP address, use a search engine such as Google with the query "what is my ip address". The search engine will return your public IP address.

To run a port-scan for six common ports against your home router or firewall, go to the Nmap Online Port Scanner at https://hackertarget.com/nmap-online-port-scanner/ and enter your public IP address in the input box_: IP address to scan…_ and press *Quick Nmap Scan*. If the response is *open* for any of the ports: 21, 22, 25, 80, 443, or 3389 then most likely, port forwarding has been enabled on your router or firewall, and you are running servers on your private network, as shown in the figure.

Security Appliances

Today there is no single security appliance or piece of technology that will solve all network security needs. Because there is a variety of security appliances and tools that need to be implemented, it is important that they all work together. Security appliances are most effective when they are part of a system.

Security appliances can be stand-alone devices, like a router or firewall, a card that can be installed into a network device, or a module with its own processor and cached memory. Security appliances can also be software tools that are run on a network device. Security appliances fall into these general categories:

Routers - Cisco Integrated Services Router (ISR) routers, shown in Figure 1, have many firewall capabilities besides just routing functions, including traffic filtering, the ability to run an Intrusion Prevention System (IPS), encryption, and VPN capabilities for secure encrypted tunneling.

Firewalls - Cisco Next Generation Firewalls have all the capabilities of an ISR router, as well as, advanced network management and analytics. Cisco Adaptive Security Appliance (ASA) with firewall capabilities are shown in Figure 2.

IPS - Cisco Next Generation IPS devices, shown in Figure 3, are dedicated to intrusion prevention.

VPN - Cisco security appliances are equipped with a Virtual Private Network (VPN) server and client technologies. It is designed for secure encrypted tunneling.

Malware/Antivirus - Cisco Advanced Malware Protection (AMP) comes in next generation Cisco routers, firewalls, IPS devices, Web and Email Security Appliances and can also be installed as software in host computers.

Other Security Devices – This category includes web and email security appliances, decryption devices, client access control servers, and security management systems.

Detecting Attacks in Real Time

Software is not perfect. When a hacker exploits a flaw in a piece of software before the creator can fix it, it is known as a zero-day attack. Due to the sophistication and enormity of zero-day attacks found today, it is becoming common that network attacks will succeed and that a successful defense is now measured in how quickly a network can respond to an attack. The ability to detect attacks as they happen in real-time, as well as stopping the attacks immediately, or within minutes of occurring, is the ideal goal.

Unfortunately, many companies and organizations today are unable to detect attacks until days or even months after they have occurred.

- **Real Time Scanning from Edge to Endpoint** - Detecting attacks in real time requires actively scanning for attacks using firewall and IDS/IPS network devices. Next generation client/server malware detection with connections to online global threat centers must also be used. Today, active scanning devices and software must detect network anomalies using context-based analysis and behavior detection.
- **DDoS Attacks and Real Time Response** - DDoS is one of the biggest attack threats requiring real-time response and detection. DDoS attacks are extremely difficult to defend against because the attacks originate from hundreds, or thousands of zombie hosts, and the attacks appear as legitimate traffic, as shown in the figure. For many companies and organizations, regularly occurring DDoS attacks cripple Internet servers and network availability. The ability to detect and respond to DDoS attacks in real-time is crucial.

Protecting Against Malware

How do you provide defense against the constant presence of zero-day attacks, as well as advanced persistent threats (APT) that steal data over long periods of time? One solution is to use an enterprise-level advanced malware detection solution that offers real-time malware detection.

Network administrators must constantly monitor the network for signs of malware or behaviors that reveal the presence of an APT. Cisco has an Advanced Malware Protection (AMP) Threat Grid that analyzes millions of files and correlates them against hundreds of millions of other analyzed malware artifacts. This provides a global view of malware attacks, campaigns, and their distribution. AMP is client/server software deployed on host endpoints, as a standalone server, or on other network security devices. The figure shows the benefits of the AMP Threat Grid.

Security Best Practices

Many national and professional organizations have published lists of security best practices. The following is a list of some security best practices:

- **Perform Risk Assessment** – Knowing the value of what you are protecting will help in justifying security expenditures.
- **Create a Security Policy** – Create a policy that clearly outlines company rules, job duties, and expectations.

- **Physical Security Measures** – Restrict access to networking closets, server locations, as well as fire suppression.
- **Human Resource Security Measures** – Employees should be properly researched with background checks.
- **Perform and Test Backups** – Perform regular backups and test data recovery from backups.
- **Maintain Security Patches and Updates** – Regularly update server, client, and network device operating systems and programs.
- **Employ Access Controls** – Configure user roles and privilege levels as well as strong user authentication.
- **Regularly Test Incident Response** – Employ an incident response team and test emergency response scenarios.
- **Implement a Network Monitoring, Analytics and Management Tool** - Choose a security monitoring solution that integrates with other technologies.
- **Implement Network Security Devices** – Use next generation routers, firewalls, and other security appliances.
- **Implement a Comprehensive Endpoint Security Solution** – Use enterprise level antimalware and antivirus software.
- **Educate Users** – Educate users and employees in secure procedures.
- **Encrypt data** – Encrypt all sensitive company data including email.

Some of the most helpful guidelines are found in organizational repositories such as the National Institute of Standards and Technology (NIST) Computer Security Resource Center, as shown in the figure.

One of the most widely known and respected organizations for cybersecurity training is the SANS Institute. Go here to learn more about SANS and the types of training and certifications they offer.

Botnet

A botnet is a group of bots, connected through the Internet, with the ability to be controlled by a malicious individual or group. A bot computer is typically infected by visiting a website, opening an email attachment, or opening an infected media file.

A botnet can have tens of thousands, or even hundreds of thousands of bots. These bots can be activated to distribute malware, launch DDoS attacks, distribute spam email, or execute brute force password attacks. Botnets are typically controlled through a command and control server.

Cyber criminals will often rent out Botnets, for a fee, to third parties for nefarious purposes.

The figure shows how a botnet traffic filter is used to inform the worldwide security community of botnet locations.

The Kill Chain in Cyberdefense

In cybersecurity, the Kill Chain is the stages of an information systems attack. Developed by Lockheed Martin as a security framework for incident detection and response, the Cyber Kill Chain is comprised of the following stages:

Stage 1. Reconnaissance - The attacker gathers information about the target.

Stage 2. Weaponization - The attacker creates an exploit and malicious payload to send to the target.

Stage 3. Delivery - The attacker sends the exploit and malicious payload to the target by email or other method.

Stage 4. Exploitation - The exploit is executed.

Stage 5 Installation - Malware and backdoors are installed on the target.

Stage 6. Command and Control - Remote control of the target is gained through a command and control channel or server.

Stage 7. Action - The attacker performs malicious actions like information theft, or executes additional attacks on other devices from within the network by working through the Kill Chain stages again.

To defend against the Kill Chain, network security defenses are designed around the stages of the Kill Chain. These are some questions about a company’s security defenses, based on the Cyber Kill Chain:

• What are the attack indicators at each stage of the Kill Chain?

• Which security tools are needed to detect the attack indicators at each of the stages?

• Are there gaps in the company’s ability to detect an attack?

According to Lockheed Martin, understanding the stages of Kill Chain allowed them to put up defensive obstacles, slow down the attack, and ultimately prevent the loss of data. The figure shows how each stage of the Kill Chain equates to an increase in the amount of effort and cost to inhibit and remediate attacks.

Behavior-Based Security

Behavior-based security is a form of threat detection that does not rely on known malicious signatures, but instead uses informational context to detect anomalies in the network. Behavior-based detection involves capturing and analyzing the flow of communication between a user on the local network and a local, or remote destination. These communications, when captured and analyzed, reveal context and patterns of behavior which can be used to detect anomalies. Behavior-based detection can discover the presence of an attack by a change from normal behavior.

- **Honeypots** - A Honeypot is a behavior-based detection tool that first lures the attacker in by appealing to the attacker’s predicted pattern of malicious behavior, and then, when inside the honeypot, the network administrator can capture, log, and analyze the attacker’s behavior. This allows an administrator to gain more knowledge and build a better defense.

- **Cisco’s Cyber Threat Defense Solution Architecture** - This is a security architecture that uses behavior-based detection and indicators, to provide greater visibility, context, and control. The goal is to know who, what, where, when, and how an attack is taking place. This security architecture uses many security technologies to achieve this goal.

NetFlow

NetFlow technology is used to gather information about data flowing through a network. NetFlow information can be likened to a phone bill for your network traffic. It shows you who and what devices are in your network, as well as when and how users and devices accessed your network. NetFlow is an important component in behavior-based detection and analysis. Switches, routers, and firewalls equipped with NetFlow can report information about data entering, leaving, and travelling through the network. Information is sent to NetFlow Collectors that collect, store, and analyze NetFlow records.

NetFlow is able to collect information on usage through many different characteristics of how data is moved through the network, as shown in the figure. By collecting information about network data flows, NetFlow is able to establish baseline behaviors on more than 90 different attributes.

CSIRT

Many large organizations have a Computer Security Incident Response Team (CSIRT) to receive, review, and respond to computer security incident reports, as shown in Figure 1. The primary mission of CSIRT is to help ensure company, system, and data preservation by performing comprehensive investigations into computer security incidents. To prevent security incidents, Cisco CSIRT provides proactive threat assessment, mitigation planning, incident trend analysis, and security architecture review, as shown in Figure 2.

Cisco’s CSIRT collaborates with Forum of Incident Response and Security Teams (FIRST), the National Safety Information Exchange (NSIE), the Defense Security Information Exchange (DSIE), and the DNS Operations Analysis and Research Center (DNS-OARC).

There are national and public CSIRT organizations like the CERT Division of the Software Engineering Institute at Carnegie Mellon University, that are available to help organizations, and national CSIRTs, develop, operate, and improve their incident management capabilities.

Security Playbook

Technology is constantly changing. That means cyberattacks are evolving too. New vulnerabilities and attack methods are discovered continuously. Security is becoming a significant business concern because of the resulting reputation and financial impact from security breaches. Attacks are targeting critical networks and sensitive data. Organizations should have plans to prepare for, deal with, and recover from a breach.

One of the best way to prepare for a security breach is to prevent one. There should be guidance on identifying the cybersecurity risk to systems, assets, data, and capabilities, protecting the system by the implementation of safeguards and personnel training, and detecting cybersecurity event as soon as possible. When a security breach is detected, appropriate actions should be taken to minimize its impact and damage. The response plan should be flexible with multiple action options during the breach. After the breach is contained and the compromised systems and services are restored, security measures and processes should be updated to include the lessons learned during the breach.

All this information should be compiled into a security playbook. A security playbook is a collection of repeatable queries (reports) against security event data sources that lead to incident detection and response. Ideally the security playbook must accomplish the following actions:

- Detect malware infected machines.
- Detect suspicious network activity.
- Detect irregular authentication attempts.
- Describe and understand inbound and outbound traffic.
- Provide summary information including trends, statistics, and counts.
- Provide usable and quick access to statistics and metrics.

- Correlate events across all relevant data sources.

Tools for Incident Prevention and Detection

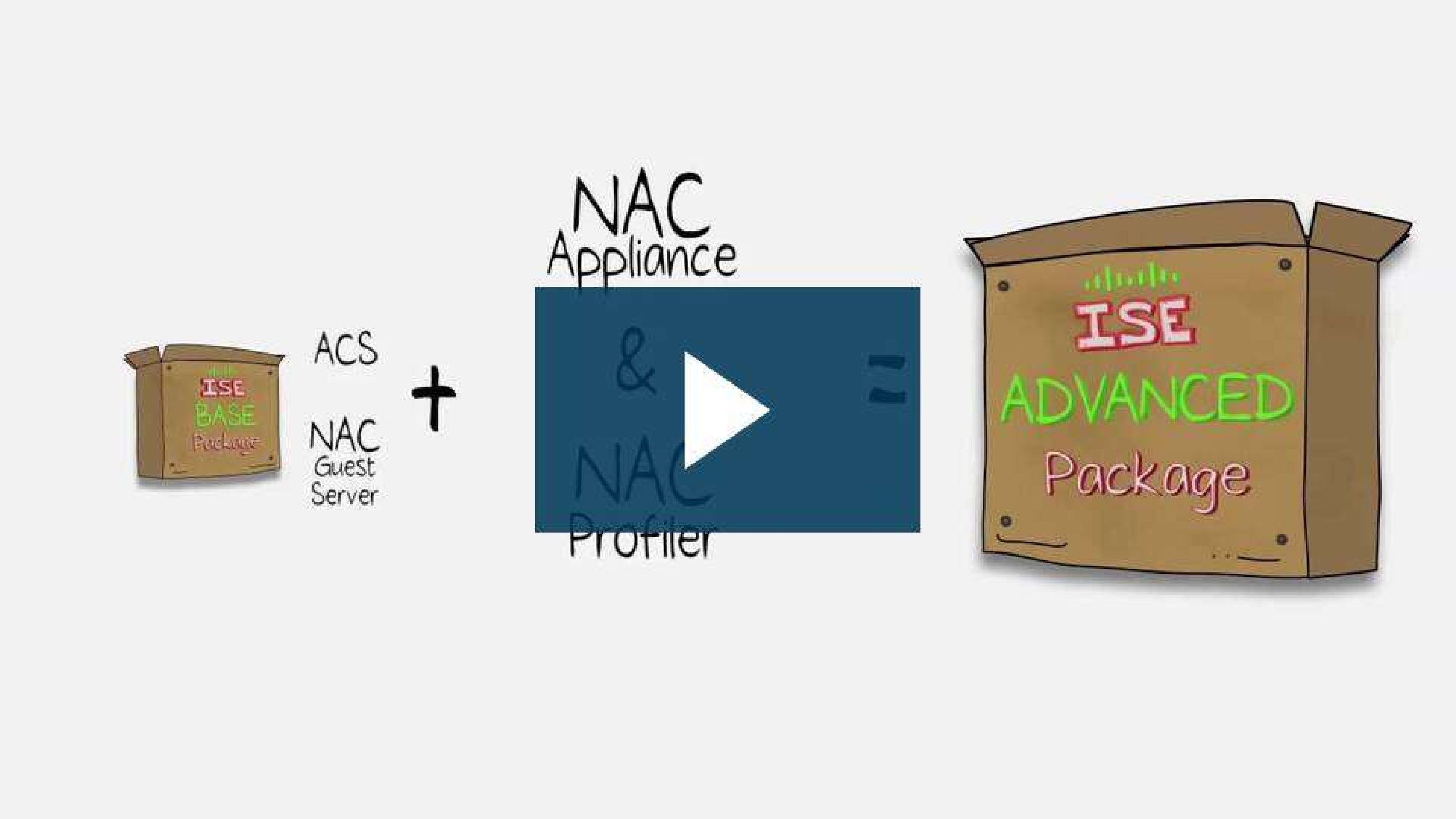
These are some of the tools used to detect and prevent security incidents:

- **SIEM** – A Security Information and Event Management (SIEM) system is software that collects and analyzes security alerts, logs and other real time and historical data from security devices on the network.

- **DLP** – Data Loss Prevention Software (DLP) is a software or hardware system designed to stop sensitive data from being stolen from or escaping a network. A DLP system may focus on file access authorization, data exchange, data copying, user activity monitoring, and more. DLP systems are designed to monitor and protect data in three different states: data in-use, data in-motion and data at-rest. Data in-use is focused on the client, data in-motion refers to data as it travels through the network, and data at-rest refers to data storage.

- **Cisco ISE and TrustSec** – Cisco Identity Services Engine (Cisco ISE) and Cisco TrustSec enforce access to network resources by creating role-based access control policies that segment access to the network (guests, mobile users, employees) without added complexity. Traffic classification is based on user or device identity. Click play in the figure to learn more about ISE.

- Click here to read the transcript of this video.



IDS and IPS

An Intrusion Detection System (IDS), shown in the figure, is either a dedicated network device, or one of several tools in a server or firewall that scans data against a database of rules or attack signatures, looking for malicious traffic. If a match is detected, the IDS will log the detection, and create an alert for a network administrator. The Intrusion Detection System does not take action when a match is detected so it does not prevent attacks from happening. The job of the IDS is merely to detect, log and report.

The scanning performed by the IDS slows down the network (known as latency). To prevent against network delay, an IDS is usually placed offline, separate from regular network traffic. Data is copied or mirrored by a switch and then forwarded to the IDS for offline detection. There are also IDS tools that can be installed on top of a host computer operating system, like Linux or Windows.

An Intrusion Prevention System (IPS) has the ability to block or deny traffic based on a positive rule or signature match. One of the most well-known IPS/IDS systems is Snort. The commercial version of Snort is Cisco's Sourcefire. Sourcefire has the ability to perform real-time traffic and port analysis, logging, content searching and matching, and can detect probes, attacks, and port scans. It also integrates with other third party tools for reporting, performance and log analysis.