Prevention: Network Defenses

We have already covered the basics of network defenses in the Security Fundamentals domain. This lesson is going to dig deeper and explore a number of network defenses that can be used to prevent incidents from occurring, using autonomous defensive actions or alerting security analysts to investigate before an event becomes an incident. The security controls we will focus on firewalls, NIDS/NIPS, event monitoring, and network access control (NAC).

NETWORK INTRUSION DETECTION

Network intrusion detection systems, also known as NIDS, can come in the form of software or physical devices that tap monitor network traffic in order to generate alerts for human analysts to investigate. NIDS can be positioned in the following positions:

- **Inline –** The system running the NIDS software is sitting directly in the path of network traffic, meaning all traffic will pass through the NIDS. In this case, the system becomes a network intrusion prevention system (NIPS). Because the device is inline, it means it can perform reactive measures such as blocking or resetting connections. The risk of using an inline NID/PS is that if the system goes offline, all traffic will be blocked, potentially causing huge issues.
- **Network Tap –** The NIDS will be connected to the network by tapping into a physical connection, such as a cable.
- **Passive –** The NIDS is connected to a SPAN port on a network device. This physical port allows all traffic passing through the device to be mirrored to the SPAN port so that the NIDS will get a copy of all network activity.

The purpose of NIDS is to generate alerts so that human analysts can investigate and take action if needed. If an attack is happening, the NIDS will generate an alert, and it will eventually be investigated (except where an inline NIDS is used, which is technically a NIPS).

Network Intrusion Detection Products

- **Snort** is the world's leading intrusion detection system, and is completely free to use, with tons of community and member rules that can be setup in a matter of minutes to provider immediate value. We will cover how to setup Snort in the next lesson! Find more information here – https://www.snort.org/
- **Suricata** is another free to use network intrusion detection system, but Suricata works at the application layer to analyze traffic in more detail and provide greater visibility. Find more information here – https://suricata-ids.org/
- **Zeek, formerly known as Bro** is another open-source solution that provides network monitoring functionality, and acts as a network intrusion detection and prevention system. Find more information here – https://zeek.org/

NETWORK INTRUSION PREVENTION

Whilst similar to NIDS, network intrusion prevention systems, or NIPS, is able to automatically take defensive actions based on the activity that has been identified. So a NIDS can detect activity and generate an alert, but NIPS can detect activity and take actions to defend against it. As an example, if an internal system begins scanning other systems, which would be classed as unusual activity in most networks, we can pre-program the IPS to block any communications that originate from the suspicious system, and generate an alert so human analysts can investigate further.

further.

Network Intrusion Prevention Products

- Snort, Suricata, and Bro/Zeek can all function as network intrusion detection systems, and prevention systems. Please see the above list to learn more about these three open-source security tools.

FIREWALLS

Firewalls are used to separate parts of a network to create private zones by restricting the traffic that can come in or go out. The most obvious example is having a physical firewall between the internet and your network, only allowing common protocols in such as HTTP, HTTPS, and DNS. This prevents random hosts from connecting to the organization's systems, which could allow them to be exploited and compromised. Below we will cover the three main types of firewalls that will be deployed within organizations.

Traditional Firewalls

Traditional firewalls can be constructed cheaply, by making use of dedicated hardware and open-source firewall software such as Pfsense. These types of firewalls will use rules that will allow or disallow traffic using pre-defined factors such as:

- Source IP
- Destination IP
- Source Port
- Destination Port
- Protocol Used

You can read more about tuning firewalls here – https://www.esecurityplanet.com/network-security/finetune-and-optimize-firewall-rules.html.

Next-Generation Firewalls (NGFWs)

NGFWs are a lot more complex than traditional firewalls. Instead of simply monitoring and acting on the source and destination IP addresses and ports, NGFWs inspect packets as they pass through, looking at each layer of the OSI model. By using an application layer firewall, we can ban the use of specific applications, such as peer-to-peer file-sharing applications, or restrict how applications are used, such as allowing Skype to be used for voice over IP (VOIP) calls, but not restricting the ability to upload or download files. These firewalls are more expensive than conventional firewalls, but they offer much stronger protection.

Web Application Firewalls (WAFs)

A WAF is usually a proxy server that stands between an application running on a server and users who access the application from outside the corporate network. The proxy server accepts incoming data and then establishes its own connection to the application on behalf of the external user. A key benefit of this setup is that the application is shielded from port scans, attempts to determine the software running on the application server, or other malicious activity directed by end-users at the application. But not all applications are easily supported by proxy firewalls, and they can reduce the performance of the protected application to end-users.

Setting up a Firewall

In the activity linked at the bottom of this lesson, we have created a practical exercise, where you'll learn to set up the software firewall 'pfSense' on your Kali Linux virtual machine. This will work to develop your understanding of how firewalls work and give you the chance to write firewall rules, a useful skill to have.

EVENT MONITORING

Network devices can generate logs, and these logs can be sent to a SIEM platform. By having logs come from systems across the environment, the SIEM is able to provide a dashboard that analysts can utilize to monitor

activity and respond to alerts that are generated when suspicious or malicious traffic is detected. Network devices can provide very valuable information, let's take a look at a couple of examples:

- **Web Proxy Logs –** This device processes web-based requests to the internet, and will contain a list of sites visited by employees. This can be combined with a blacklist to generate SIEM alerts when an employee tries to visit a malicious website or explicit website or resource.
- **Perimeter Firewalls –** If a malicious actor starts port scanning the organization, the perimeter firewalls will pick this activity up first as they get smashed with requests from the scanning IP(s). By sending this to a SIEM an alert can be generated when port or vulnerability scanning is being conducted, or when distributed denial-of-service attacks (DDoS) start.

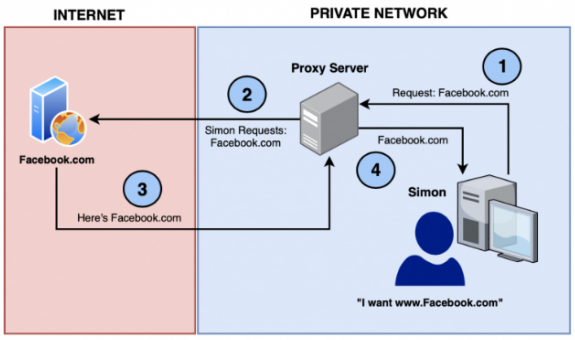
NETWORK ACCESS CONTROL

Pre-admission – Network Access Control (NAC) can work to prevent rogue or non-compliant devices from connecting to a private network. Security teams could require that any devices connecting to the network need the latest patches and security updates, and must be running anti-virus. NAC is able to enforce this, and not let devices connect to the network until they have met all of the policy requirements. This is typically used for Bring Your Own Device (BYOB) or guest networks, where non-corporate devices will be connecting such as employee mobile phones and personal laptops, which may potentially be infected as they aren't protected by company security tools.

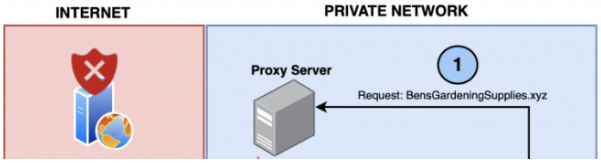
Post-admission – Having checks and requirements before allowing a device to join a network is great, but what makes NAC amazing is the ability to enforce restrictions once the device has been granted access to the network. This can include defining what resources or systems the device can interact with using Role-Based Access (RBAC) functionality, restricting access to specific systems such as file servers.

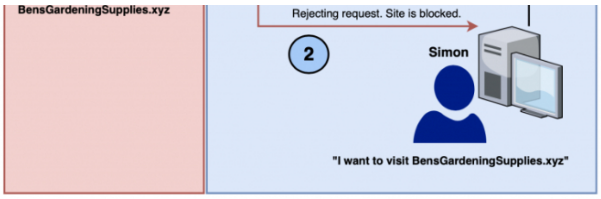
WEB PROXY

Remember back in school when you tried to play games, but you couldn't connect to certain sites? That's a web proxy in work, preventing access to certain resources on the internet for primarily security purposes. Requests for internet resources are sent from the requesting client to the web proxy, then sent on behalf of the proxy to the destination, the request is fulfilled and the resource is sent back to the proxy, where it sends it to the requesting client. We have created a simple diagram to demonstrate this below.



How do web proxies ensure security? They have the ability to reject requests, preventing users from retrieving potentially malicious resources from the internet. This means that are requests trying to reach that resource will be denied, and the request will never leave the organization. Preemptive blocks can be conducted based on intelligence to prevent anyone from accessing a known malicious site, however, this is often conducted when phishing attacks are observed against the organization, and any malicious URLs included in the email are blocked on the web proxy so that if any users have received the email and try to click on the link, they're safe. In the below example, Simon receives a malicious email with a link to a compromised website hosting malware "BensGardeningSupplies.xyz".





Quizzes

Legacy Activity) Setting up a Firewall

Previous Topic

Back to Lesson

Next Topic