**Network Protection Systems**

***Table of Contents Pages***

*Introduction…………………………………………………………………………….(1)*

*Intrusion Detection Systems and Protection Systems…………………………….(1-2)*

* *Intrusion Detection Systems…………………………………………………(1)*
* *Intrusion Protection Systems………………………………………………..(1-2)*

*Web Filtering……………………………………………………………………………(2-3)*

*HoneyPotting……………………………………………………………………………(3)*

*How does honeypots work?……………………………………………………………(3-4)*

*Citations………………………………………………………………………………….(5)*

Daniel Rao

April 25th, 2021

Vince Skinner

**Introduction**

Hackers utilize many tools to attack a network. Some of the methods like words ending in enumeration make it possible for a tacos to determine the services that are running on the computer and gain access to network resources. In this paper I will briefly discuss web filtering, intrusion detection systems, prevention systems and honeypotting.

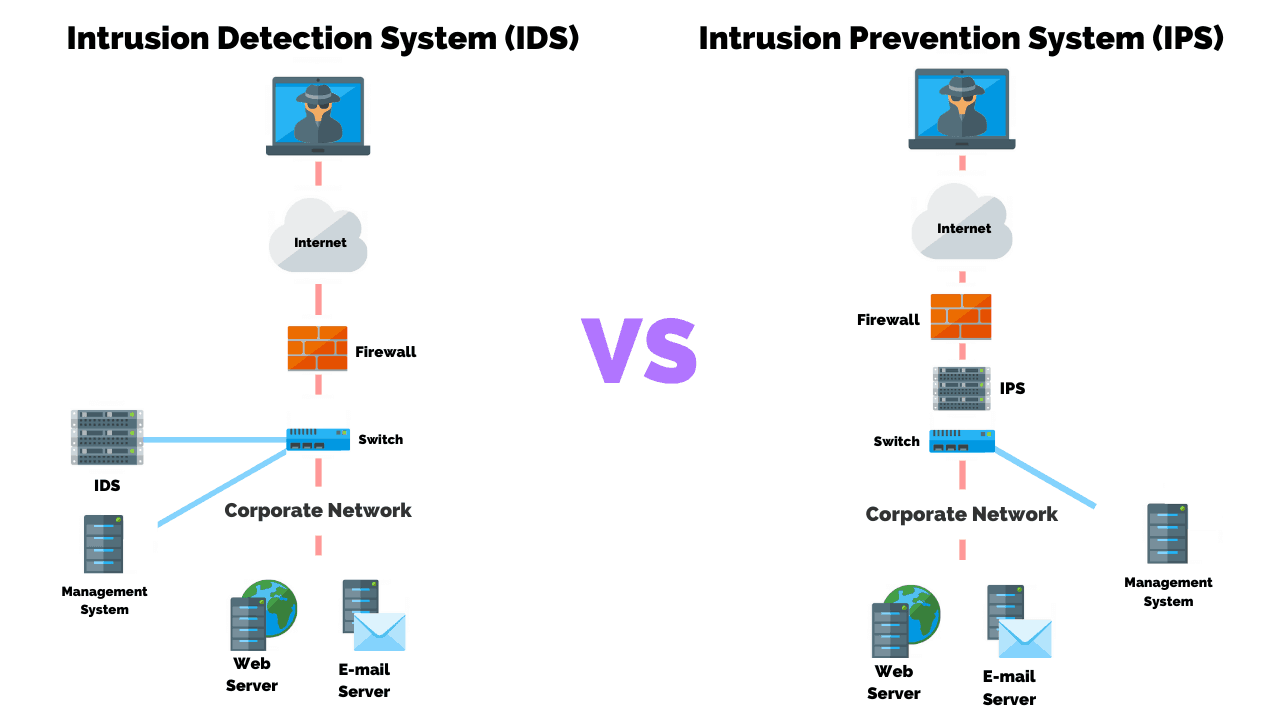
**Intrusion Detection Systems and Protection Systems**

**Intrusion Detection Systems:**

IDs monitor network devices so that the security administrators can identify attacks in progress and stop them. For example, for users to be able to access a VIP server a fireball must allow Port 80 to be open. Unfortunately, opening dysport can also allow hackers to attack the web server. and ideas examines the traffic traversing the connection to Port 80 and Compares it with the known exploits, similar to a virus software using a signature file to identify viruses. if an attacker attempts to exploit an envelope Realty in the web server, the ideas can alert the system of the attacks at the web server Administrator can take action.

**Intrusion Protections Systems:**

There is a slight difference between IDs and IPS. a true network-based IPS is installed in line to the network infrastructure, meaning traffic has to pass through IPS before going into or out of the network. An active IDs however just sniff traffic and can be turned off or unplugged from the network without affecting the network connectivity. because IPS is in line, generally it's more capable of stopping malicious traffic than an active IDs is, especially against UDP based attacks.

****

**Web Filtering**

Attackers, meet arkadiy user workstation that are usually allowed access to the internet. If they can get an internal user to visit a malicious website or install malicious code from an email attachment, they don't need to break through a firewall. After Trojan code is installed on the user's workstation, attackers can control the Trojan remotely but commands that might seem to be normal traffic. They can take advantage of the compromised Network to expand through the network by running Network scans and the compromise workstation, stealing data accessible on or from the victim system, cracking system passwords, and exploiting vulnerabilities they discover on other systems. attackers can hide the command-and-control activity inside what appears to be normal HTTP and HTTPS traffic. In this situation, filtering can be used and some of the filtering can actually block malicious code before it gets to the user workstationor before it has a chance to connect to an attacker's control system outside the network. Companies that sell and support web filtering devices are often categorized to match into different groups. organize cybercriminals often try to hack busy websites that have the best chance of infecting thousands of website visitors with their malicious code. These types of mass compromises are used to initiate drive-by downloads, in which websites download malicious code without their knowledge. usually the drive-by download exploits a security flaw in the browser or a third-party application such as Adobe Reader or Microsoft Office. Because malicious websites and code change Daily, filtering system providers need to update their signatures and databases off malicious websites constantly.

**HoneyPotting**

A Honeypot is a computer placed on a network parameter that contains information or data intended to lure and then trap hackers. The main goal is to distract Hackers from attacking legitimate network resources. A security professional configures the computer to have vulnerabilities so that the attackers spend time trying to exploit these Werner abilities. Another goal of the Honeypot is to have attackers connect to the phony computer long enough to be detected, long enough to trace his or her location. In addition a Honeypot can serve as an excellent data collector an early warning system to help characterize these new attacks and threats information makes it easier for Security Professionals to defend that works against them.

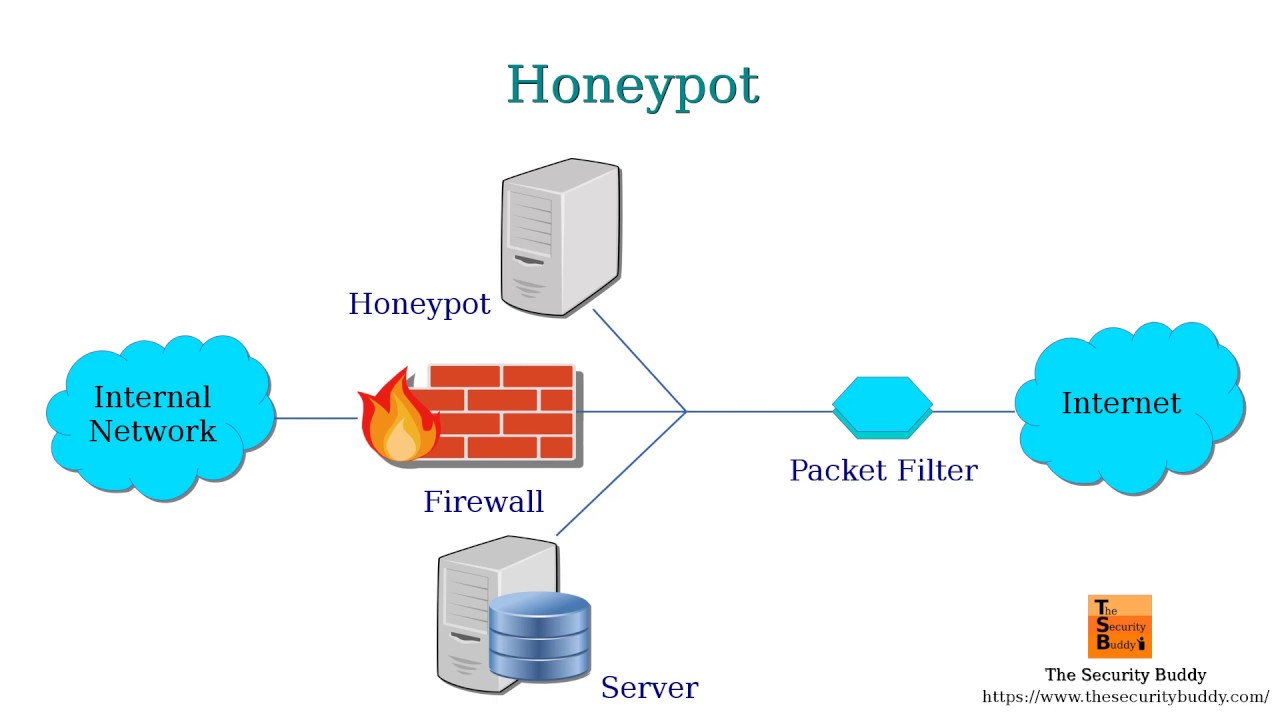
**How does honeypots work?**

If the attacker can get into the internal Network then they can cause a lot of havoc. a Honeypot appears to have important data or sensitive information stored on it. Example it could store fake financial data that temps hackers into attempting to browse through the data. The government and Private Industry have used honey possibly or attackers into Network areas away from the real data for many years. Basically the belief is that if hackers discover a vulnerability in the system, they spend time exploiting the vulnerability and stop looking for another area to exploit and access computer resources. some of the common commercial honey pots are as follows:

* Specter
* KFSensor

some of the open-source honeypots are as follows:

* OpenCanary
* Honeyd
* Cowrie



**Citations**

<https://usa.kaspersky.com/resource-center/threats/what-is-a-honeypot>

<https://www.barracuda.com/glossary/web-filtering>