Security Controls

Jacob L. Silva, Network Security

University of Advancing Technology

Intrusion Detection Systems

An Intrusion Detection System (IDS) is a network security technology built to monitor network traffic, suspicious activity, and alerts the system or network administrator. As an example of one of the functions an IDS can do is respond automatically to malicious traffic by taking actions like blocking the user or the source IP address. Our plan is to review a couple IDS and figure out which would work better in different situations.

Snort (IDS):

Snort is a free open source IDS that is capable of performing real time traffic analysis and packet logging on networks.

Pros:

- Free and open source
- Easy to set rules
- Flexible and dynamic with live deployments
- Constantly being developed and improved

Cons:

- No graphical user interface
- Can be slow in processing network packets
- Cannot detect signature splits over multiple TCP packet if the packets are configured in inline mode

BroIDS:

BroIDS is an open source network traffic analyzer that is used for collecting network measurements, forensic investigations, and traffic-based lining.

Pros:

- BroIDS is a highly flexible IDS that allows users to make monitoring rules to each protected object
- Works good in networks that have large volumes of traffic
- Can-do, in-depth analysis of traffic and can analyze multiple protocols

Cons:

- BroIDS can be harder to handler because of its complex architecture
- Programming experience will be required if you want to properly utilize BroIDS

Password Managers

Password managers help generate complex passwords and store them in a database that's encrypted and only accessed through a master password so you can access them for later use. The purpose for creating multiple different passwords for different accounts is because if one of those accounts become compromised, they won't have the login info to any other accounts. The main issue with a password manager is if someone manages to get access to your password managers master password, they will have access to all your login details. Our plan is to look through the most popular manager and see which would work best for our needs.

LastPass:

LastPass is a widely used and known password manager LastPass is primarily used as plugins for many web browsers along with IOS and Android apps.

Features:

- Uses one master password to access your database of passwords.
- Automatic form filling which fill your information into web forms when requested
- One click logs you into websites you have made accounts for when requested
- Encrypts sensitive account login data on your PC
- Generates strong random passwords

KeePass:

KeePass is a free open source password manager, and another widely used known password manager that’s installed on your computer. The currently supported operating systems are Windows, Mac, Linux, Android, IOS and more.

Features:

- KeePass supports Advanced Encryption Standard (AES) to keep your personal information secure
- One master password decrypts your login database
- KeePass is portable and can be carried on a USB stick
- All fields and notes are able to drag and drop into other windows
- Generates strong random passwords

Anti-virus software’s

Anti-virus software is a software that is designed to search, prevent, detect, and remove viruses. It's important when using an antivirus to keep the virus definitions up to date so the Anti-virus can stop the latest viruses.

Avast Business Antivirus:

Plans:

- 1 Device for 1 year is $49.99
- 1 Device for 2 years $74.99
- 1 Device for 3 years $89.98

Features:

- Light on resources
- Updates software automatically
- SharePoint and Exchange server protection
- Smart Scan
- Behavior Shield

Symantec Endpoint Protection 14:

Plans:

- 1 Year Subscription $28.00
- 2 Year Subscription $46.68
- 3 Year Subscription $56.00

Features:

- Network Firewall & intrusion prevention
- Anti-Virus scans and removes malware on systems
- Memory exploit mitigation blocks zero-day exploits against vulnerabilities in popular software
- Controls file, registry, device behavior, whitelisting, and blacklisting

Resources

The Best Open Source Network Intrusion Detection Tools. Retrieved February 25, 2018, from http://opensourceforu.com/2017/04/best-open-source-network-intrusion-detection-tools/

KeePass. (2018, February 25). Retrieved February 25, 2018, from https://en.wikipedia.org/wiki/KeePass

Reichl, D. (n.d.). KeePass Password Safe. Retrieved February 25, 2018, from https://keepass.info/

Reichl, D. (n.d.). Features - KeePass. Retrieved February 25, 2018, from https://keepass.info/features.html

What is Anti-Virus Software? (n.d.). Retrieved February 25, 2018, from https://www.webroot.com/us/en/home/resources/tips/pc-security/security-what-is-anti-virus-software

Avast Business Antivirus Pro Plus. (n.d.). Retrieved February 25, 2018, from https://www.futuredigital360.com/plans-and-prices/avast-business-antivirus-pro-plus/ Avast Business Antivirus Pro. (n.d.). Retrieved February 25, 2018, from https://www.avast.com/en-us/business-antivirus-pro

What's new in Symantec Endpoint Protection 14. (n.d.). Retrieved February 25, 2018, from https://support.symantec.com/en_US/article.HOWTO125362.html

Small & Medium Business. (n.d.). Retrieved February 25, 2018, from https://www.symantec.com/smb