**Lab2 04: Research Project Milestone 3 – Website Map**

Aldo Alvarez, Cesar Cardenas, David Wang, Matthew Guzman, Yilinda Li

**Home Page features:**

Introduction of Malware

**Home Page**

**Sub Topic 1**

]

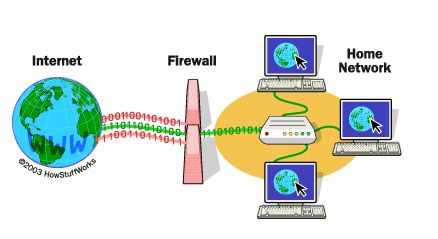
Aldo Alvarez

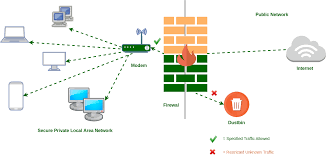
[

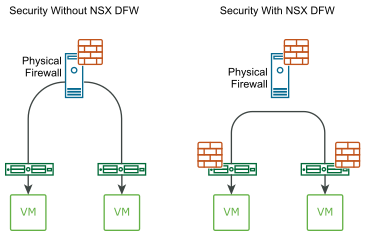
Provide links to subtopic pages

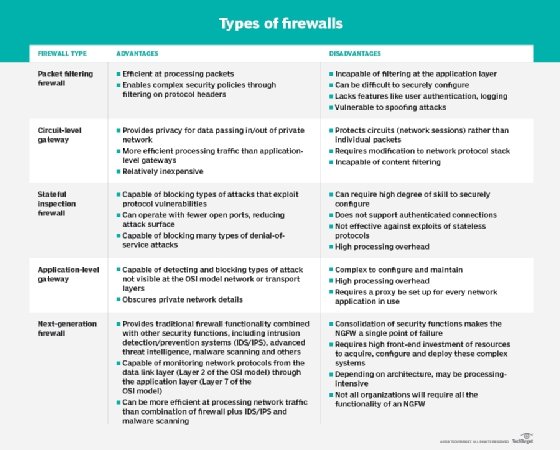
**Topic: Firewall**

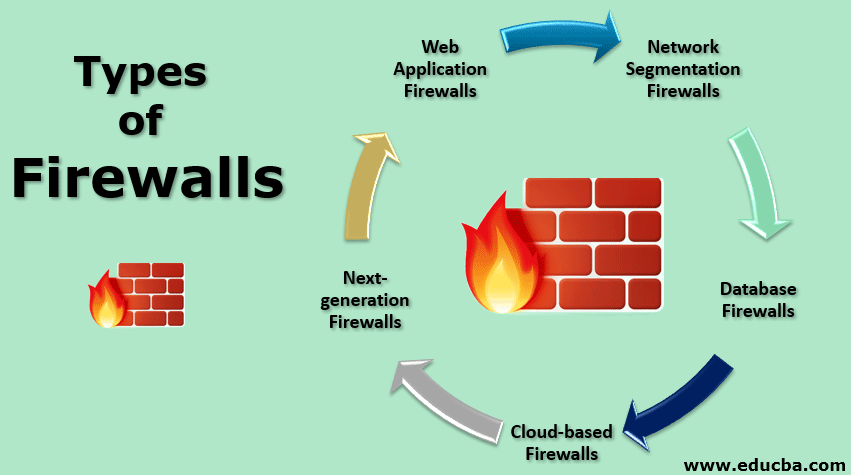
Introduction

Images:









Data from articles and images of each type of firewall.

Content:

* + - * + Item 1: Discuss what a fire wall is

Demonstrate and show what a fire wall is and give a demonstration on why a firewall is important to networks and the effects it has on malware

* + - * + Item 2 : Distributed firewall, conventional and others used today

This would show different areas off firewall which are used throughput different industries each firewall will have an image demonstrating how each one is used.

* + - * + Item 3: Explain how a fire wall works

Gives a brief explanation on how firewalls work and on how they help with viruse and shows how malware is affective in a business or at home network.

* + - * + Conclusion:

**Sub Topic 2**

]

Cesar Cardenas

[

Give a conclusion on how these are all tied together and give a brief summarization of everything you have read.

**Topic: Trojan**

Introduction Images/Data/etc.

A picture containing building, outdoor, truck, street

Description automatically generatedA picture containing toy

Description automatically generated

Just like the Greeks used a trojan horse to trick the people of Troy into letting troops into the city, Trojan disguises itself to get into your system.

A screenshot of a cell phone

Description automatically generated Here is an example of a malware that was downloaded that made people play a game a chance before it destroyed all their data.A screenshot of text

Description automatically generated Data graphs of Trojan attacks percentageA screenshot of a cell phone

Description automatically generated (2020 top, 2018 bottom)

Content:

* + - * + Introduction: Trojan mimics the classical trojan story that that is a decoy horse giftwrapped to hide its true intentions. This type of malware can damage your computer, but it only happens if you let it into your computer. The malware presents itself as something that you might need, persuading you to download it, only to unknowingly let it wreak havoc on your computer.
        + Item 1:

https://www.avg.com/en/signal/what-is-a-trojan

Contains explanations on what a Trojan Horse is, how it works, it’s history & examples, how to know if you’re infected, and how to check/prevent it.

* + - * + Item 2 :

https://www.csoonline.com/article/3403381/what-is-a-trojan-horse-how-this-tricky-malware-works.html

Contains more indebt info. on what a Trojan Horse is, how this malware works and affects your computer, and how to remove it.

* + - * + Item 3:

https://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software/

Contains info. Not only about the Trojan Horse, but it also goes over viruses and other malware (shows history, examples, developments, different types, how they are spread, and how to prevent them).

* + - * + Conclusion:

Trojan is one of the most common forms of malware. It sneaks into your system, let in by the user, then begins to attack your system. These attacks can be straight forward or can go completely undetected for a period of time. Trojan has the potential to access and take; login info, screenshots, system info, banking info., and other sensitive info. The saying goes, “Always beware Greeks – or strangers online – bearing gifts.”

**Sub Topic 3**

]

David Wang

[

**Topic: Malware Detection**

Introduction Images/Data/etc.

Content:

* + - * + Item 1: History of Malware Detection systems

Discuss the way that malware has evolved over time, starting from the first anti-malware program, Flushot Plus in 1987, to today’s most used detection systems. Discuss McAfee’s VirusScan program, provide overall timeline on how it has progressed.

* + - * + Item 2 : Malware Detection Techniques

Discuss the types techniques that are used to detect malware, and the similarities and differences between them. Provide brief explanation of how each technique works.

Potential malware detection subtopics

Signature-based detection

Specification-based detection

Behavioral-based detection

* + - * + Item 3:

Discuss Malware Propagation and Attack Techniques

Methods of Propagation: How does Malware spread to infect devices?

What kinds of techniques does malware use to infect devices

* + - * + Conclusion:

Discuss the future of anti-malware, how will we combat malware in the future? How do anti-malware developers keep up with the constantly changing malware

**Sub Topic 4**

]

Matthew Guzman

[

**Topic: Adware**

Introduction Images/Data/etc.





Content:

* + - * + Item 1: About Adware

Adware is defined as the advertising that we see on websites that collect our information without our approval and interfere with the user’s ability to read the website by moving them to other pages, as opposed to the advertisements that are legally made and prompted on a website on the side panels that have been bought by advertisers to promote their product, which can be closed.

* + - * + Item 2 : Marketing

Planning for the future, many of the current plans that are being implemented into the market have started to establish basic principles that all business’ in the Internet world have to abide by in order to remain within the guidelines of the established rules that will be developing in the near future.

* + - * + Item 3:Spyware Regulation

Highlights on the advantages in establishing a more harmonized, commerce friendly environment for rising business’ as more platforms that could help the economy rise has always been looked upon favorably if they are established in an ethical manner.

* + - * + Conclusion:

It depends heavily on the rules and regulations that are imposed on the whole concept of what advertisements on the internet can and can’t do.

**Topic: Computer Worms**

**Sub Topic 5**

[

Yilinda Li

]

Introduction Images/Data/etc.

Content:

* + - * + Item 1: Introducing what a worm is

how computers get worms

\*image\*

* + - * + Item 2 : How do worms spread in the computer

What do they do to the computer

How hackers spread the worm

Checking if a computer has a worm

If files are deleted

Computer is crashing

No space in computer

Add image of how the computer worm spread\*

* + - * + Item 3: Preventing malwares from going on the computer

\*image\*

Download a software to protect the computer

Update the computer regularly

Do not click on anything suspicious

Install firewall

* + - * + Conclusion:

Worm is a malware that happens to computers and it is important to know what the signs are in order to protect it.