CCDC Bootcamp Week 6

https://da.gd/ccdc2023

https://kamino.sdc.cpp/

Clone a CCDCWeek6 Pod

Table of Contents

Inject!

Sorry for the lack of memes, I'm making this at 2am. It has been a long week.

Swiss Bank XChange

Hello Team!

In order to help us out with maintaining our security posture, we'll be leveraging some of what we already have in our infrastructure.

As you have found, or maybe not until I told you at this minute, you will have a pfSense firewall/router. Please install Snort on it in order to help your team detect malicious and suspicious activity. Once you have Snort installed, please enable it on all interfaces for inbound and outbound traffic.

For your report, I would like for your team to show screenshots of Snort installed as well as monitoring on all interfaces for inbound and outbound traffic.

Thank you.

- Sebastian Herzig Gartmann

Swiss Bank XChange

Snort on PfSense

Team 01

2/18/2023

Swiss Bank XChange

Team 01
Date: 2/18/2023
To: Sebastian

Re: 02.75 - Snort on PfSense

Table of Contents

Swiss Bank XChange

Team 01
Date: 2/18/2023
To: Sebastian

Re: 02.75 - Snort on PfSense

Memo

Good morning Sebastian,

I hope this message finds you well. As instructed, we have set up Snort on our PfSense. Attached is information relevant to its configuration.

Thank you,
Team 01

Swiss Bank XChange

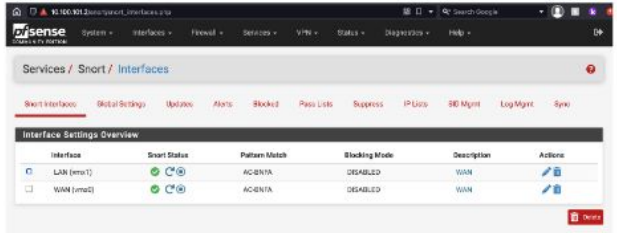
Team 01
Date: 2/18/2023
To: Sebastian

Re: 02.75 - Snort on PfSense

Full Inject Response

Snort is an open-source intrusion detection system designed to monitor network traffic. An effective IDS/IPS combination, Snort could be used to analyze and log all packets transmitted within the network. It can also be configured to block connections that are suspected to carry malicious traffic.

Artifacts/Screenshots



Snort enabled on both LAN and WAN interfaces on the network.

Hello Team!

As our business is one of many within the financial industry, we are often targeted by malicious actors. As such, it is important for us as well as the stakeholders to understand the top threats to companies in such a field.

Please provide for me a report on what the top three types of cyber attacks to financial institutions are as well as a description of what the attack comprises, what threat actors we should expect to be launching such types of attacks, as well as historical examples of such attacks.

Additionally, for each attack type, please provide a basic rubric on how to train our employees to avoid such types of attacks, who to contact if such an attack occurs, as well as how to mitigate the effects of such attack when they happen.

- Sebastian Herzig Gartmann

Re: Industry Specific Threats Reports

Full Inject Response

Introduction

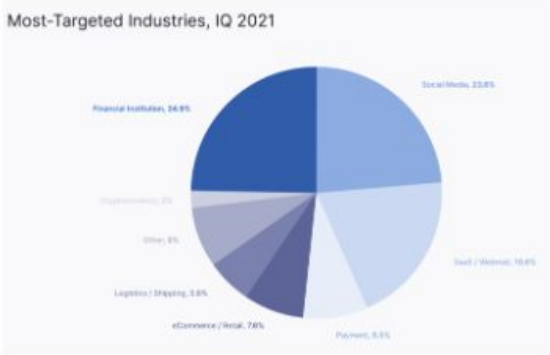
After some research, we have determined that the top three threats to financial businesses are phishing, ransomware, and DDoS attacks.

Phishing

Description

Phishing is a form of social engineering used to get login credentials to gain access to an internal network or PII about employees. The most common form of phishing is email phishing where a malicious email is created to look legitimate, but in reality, it contains a phishing link or attachment.

In 2021, phishing attacks in the financial sector increased by 22%, causing it to be the most attacked sector in quarter 1 of 2021.



Common Threat Actors

Organized cybercriminals are commonly the culprit behind phishing attacks, especially those of large scale and in pursuit of money. However, since phishing is a relatively simple attack to perform technically, almost anyone with malicious intent and access to the internet can create an effective phishing scheme.

Historical Examples

Operation Phish Phry: Over $1.5 million stole from banks due to bank frauds across Egypt and the United States.
(https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709)

Dyre Phishing Scam: Millions of dollars lost over hackers from Russia pretending to be tax consultants.
(https://www.cisa.gov/uscert/ncas/alerts/TA14-300A)

Rubric

Phishing
How to avoid
1. Do not click on unauthorized links contained within emails and other communications 2. Do not log in to pages from links within emails 3. Validate the source of each email received and other communications 4. Do not download unauthorized files contained within emails and other communications
Who to contact

Swiss Bank XChange

Date: 2/
To: S

Industry Specific Threats Reports

1. If suspected of falling victim to a phishing attack, contact the Incident Response Team at once
How to mitigate
1. Change password immediately for all affected accounts 2. Delete all files downloaded

LAMP

L(inux) A(pache) M(ySQL) P(HP)

Apache

Your Web Server
(Web - Debian 10)

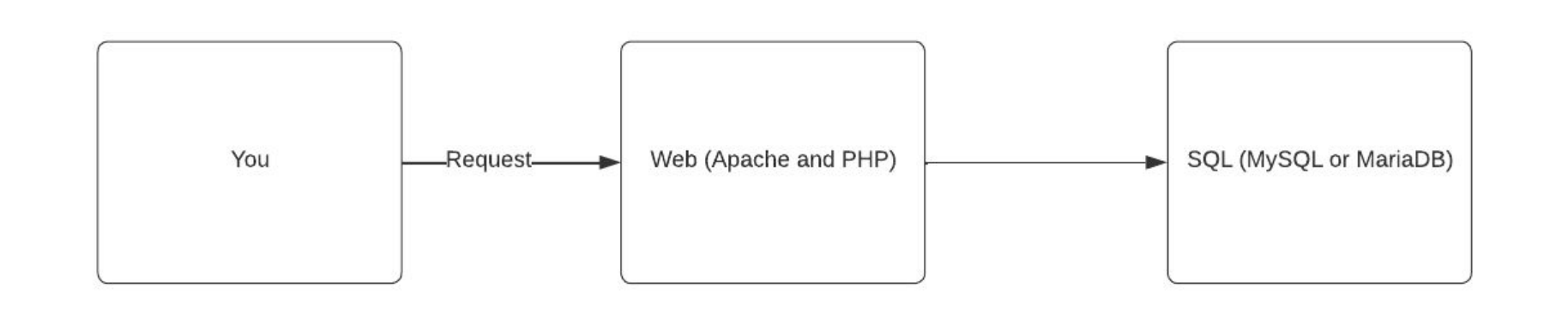
PHP

Server-side
Scripting

MySQL

Holding
Content

The Topology of LAMP



A Quick Google Search

How to set up LAMP stack Debian 10