Cybersecurity Portfolio

Certifications, Audits, Assessments, and Incident Reports

Certifications

Foundations of Cybersecurity
Coursera - Cybersecurity Certification Program
Issued: Juney 2023

Play It Safe: Manage Security Risks
Coursera - Cybersecurity Certification Program
Issued: July 2023

Connect and Protect: Networks and Network Security
Coursera - Cybersecurity Certification Program
Issued: September 2023

Audits

Botium Toys

Summary of Assignment: Perform an audit of Botium Toys' cybersecurity program. The audit needs to align current business practices with industry standards and best practices. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as "high risk," and present an overall strategy for improving the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

TO: IT Manager, Stakeholders
FROM: Daphne Kraft
DATE: 07-02-2023
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, summary and recommendations.

Scope:

- The following systems are in scope: accounting, end point detection, firewalls, intrusion detection system, and SIEM tool. They will be evaluated for:
    - User permissions
    - Implemented controls
    - Procedures and protocols set
- Ensure current user permissions, implemented controls, procedures, and protocols follow GDPR, PCI DSS, and SOC compliance
- Ensure current technology is accounted for

Goals:

- Adhere to NIST CSF
- Establish a better process for their systems to ensure they are compliant
- Fortify system controls
- Implement the concept of least privileges when it comes to credential management
- Establish their policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements

Critical findings:

The following should be addressed immediately.

- Multiple controls need to be implemented to meet audit goals, including:
    - Least privilege and separation of duties
    - Disaster recovery plans
    - Password, access control, account management policies along with a password management system
    - IDS

    - Encryption
    - Backups
    - AVS
    - Manual monitoring, maintenance, and intervention of legacy systems
    - Fire detection and prevention
- Policies need to be developed and implemented to meet GDPR and PCI DSS compliance requirements
- Policies need to be developed and implemented to meet SOC1 and SOC2 compliance requirements

Findings:

The following controls should be implemented when possible.

- Time-controlled safe
- Adequate lighting
- Locking cabinets
- Signage indicating alarm service provider

Summary/Recommendations:

It is recommended that critical findings relating to compliance with PCI DSS and GDPR be promptly addressed since Botium Toys accepts online payments from customers worldwide, including the E.U. Additionally, since one of the goals of the audit is to adapt to the concept of least permissions, SOC1 and SOC2 guidance related to user access policies and overall data safety should be used to develop appropriate policies and procedures. Having disaster recovery plans and backups is also critical because they support business continuity in the event of an incident. Integrating an IDS and AV software into the current systems will support our ability to identify and mitigate potential risks, and could help with intrusion detection, since existing legacy systems require manual monitoring and intervention. To further secure assets housed at Botium Toys' single physical location, locks and CCTV should be used to secure physical assets (including equipment) and to monitor and investigate potential threats. While not necessary immediately, using encryption and having a time-controlled safe, adequate lighting, locking cabinets, fire detection and prevention systems, and signage indicating alarm service provider will further improve Botium Toys' security posture.

Risk Assessment

Social Media Organization

Summary of Assignment: You are a security analyst working for a social media organization. The organization recently experienced a major data breach, which compromised the safety of their customers' personal information, such as names and addresses. Your organization wants to implement strong network hardening practices that can be performed consistently to prevent attacks and breaches in the future.

After inspecting the organization's network, you discover four major vulnerabilities. The four vulnerabilities are as follows:

1. The organization's employees' share passwords.
2. The admin password for the database is set to the default.
3. The firewalls do not have rules in place to filter traffic coming in and out of the network.
4. Multi-factor authentication (MFA) is not used.

If no action is taken to address these vulnerabilities, the organization is at risk of experiencing another data breach or other attacks in the future.

Assessment Report

Based off the current evaluation of the team and the most recent data breach the following are three hardening tools the organization should implement to provide better security going forward:

1) Setting and enforcing password regulations
2) Implementing multi-factor authorization (MFA)
3) Configuring and maintaining a firewall

Password regulations look like updating passwords every 30-60 days, setting specific requirements for passwords (like length, letters, numbers, and symbols to be added), limiting the amount of password attempts, and educating the team on password security (such as not sharing passwords, or what passwords make for stronger passwords).

Multi-factor authorization looks like requiring multiple means of identification in order to gain authorization to company websites and assets. Think of an ID scanner, pin numbers, passwords, or even scanning fingerprints.

Firewall maintenance and configuration looks like setting up a firewall to filter through traffic coming in and out of a network and ensuring the settings are operating appropriately to keep the network safe from malicious attacks.

Setting and enforcing password regulations is necessary to keep malicious attackers from successfully performing a brute force attack. By keeping passwords simple, reused, and shared amongst peers means it is significantly easier for an attacker to guess login credentials correctly, therefore giving them free authorization to any company information. This safeguards against brute force attacks in particular.

Multi-factor authorization validates a user attempting to access a restricted website or area within the company. It is necessary to make sure that the user is who they say they are and they have the authorization they are claiming they do. It can be used for physical and digital assets, whether it requires a specific pin to accompany a password or a fingerprint to go alongside a badge being scanned. It adds security in case a malicious actor finds credentials and attempts to use them.

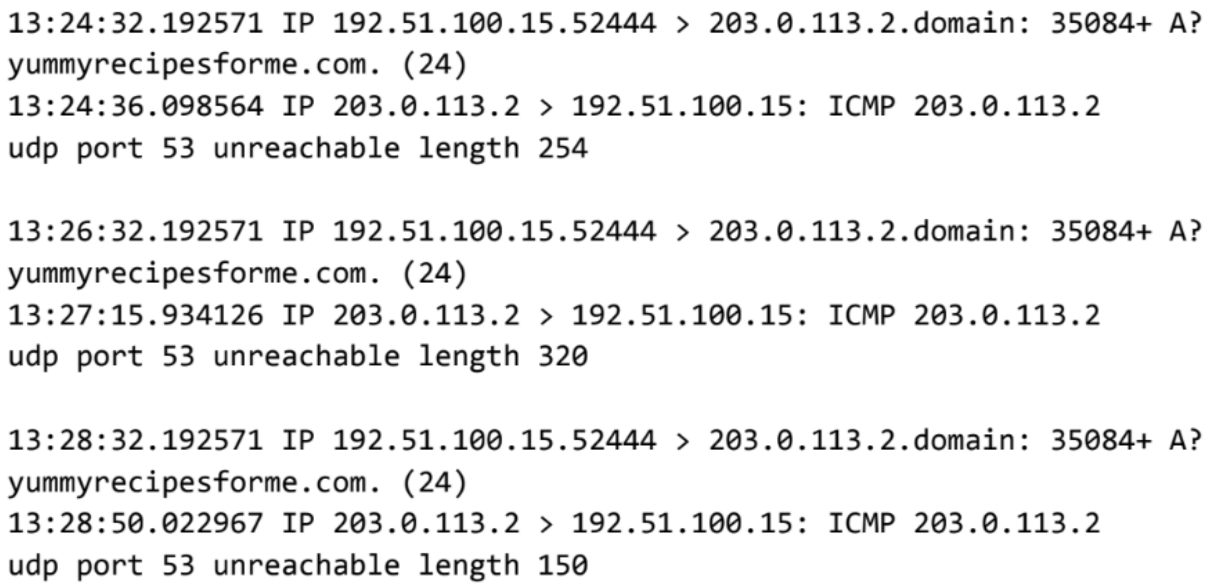
Firewalls should be regularly maintained and updated especially in the event of a security event like one that allows suspicious activity to move in and out of the network. This is particularly helpful against DoS and DDos attacks.

Incident Reports

IT Consultant Company

Summary of Assignment: You are a cybersecurity analyst working at a company that specializes in providing IT consultant services. Several customers contacted your company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

You are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, you visit the website and you also receive the error “destination port unreachable.” Next, you load your network analyzer tool, tcpdump, and load the webpage again. This time, you receive a lot of packets in your network analyzer. The analyzer shows that when you send UDP packets and receive an ICMP response returned to your host, the results contain an error message: “udp port 53 unreachable.”



```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

Incident Report

The UDP protocol reveals that the DNS server is unreachable or down at this time. This is based on the results of the network analysis in which the ICMP echo reply returned the error message “udp port 53 unreachable” three times. Port 53 is commonly used with DNS protocol traffic which likely means the issue is that the DNS server is not responding to requests at this time.

This particular incident occurred at 1:24 p.m. We became aware of the issue due to a high volume of calls from customers reporting that they were receiving the error message “destination port unreachable” when attempting to reach the website. Network security professionals within the department launched an investigation where we conducted packet sniffing tests with tcpdump. The resulting log file determined that DNS port 53 was unreachable. Next steps are determining whether port 53 is unreachable due to traffic volume or if it is blocked via firewall. The DNS server could be down due to a DDoS attack.

Travel Agency

Summary of Assignment: You work as a security analyst for a travel agency that advertises sales and promotions on the company's website. The employees of the company regularly access the company's sales webpage to search for vacation packages their customers might like.

One afternoon, you receive an automated alert from your monitoring system indicating a problem with the web server. You attempt to visit the company's website, but you receive a connection timeout error message in your browser.
You use a packet sniffer to capture data packets in transit to and from the web server. You notice a large number of TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. You suspect the server is under attack by a malicious actor.
You take the server offline temporarily so that the machine can recover and return to a normal operating status. You also configure the company's firewall to block the IP address that was sending the abnormal number of SYN requests. You know that your IP blocking solution won't last long, as an attacker can spoof other IP addresses to get around this block. You need to alert your manager about this problem quickly and discuss the next steps to stop this attacker and prevent this problem from happening again. You will need to be prepared to tell your boss about the type of attack you discovered and how it was affecting the web server and employees.

Incident Report

A potential explanation for the website's connection timeout error message is a type of DoS attack known as a SYN flood attack. According to the logs, there is a large number of SYN requests coming from an unrecognized IP address which would be overwhelming the server.

When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. A handshake happens as follows:

1. Their device sends a SYN request to a server
2. The server then returns a SYN/ACK packet to accept the request and leaves space open for the connection to be established
3. Once the final ACK packet is received the TCP connection is established

In situations like these when a malicious actor sends a large amount of SYN requests all at once, it can overwhelm the server and cause it to shut down especially when the amount of requests coming in is larger than the space available to reserve a connection.

Right now the logs indicate that the servers are overwhelmed due to a high volume of SYN requests so users are unable to access the site due to lack of availability with the server. Since the server is unable to open up to new requests, visitors are receiving a connection timeout error.

Yummy Recipes for Me

Summary of Assignment: You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A disgruntled baker has decided to publish the website's best-selling recipes for the public to access for free. The baker executed a brute force attack to gain access to the web host. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the right one. After they obtained the login credentials, they were able to access the admin panel and change the website's source code. They embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website. After running the downloaded file, the customers are redirected to a fake version of the website where the seller's recipes are now available for free. Several hours after the attack, multiple customers emailed yummyrecipesforme's helpdesk. They complained that the company's website had prompted them to download a file to update their browsers. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly. In response to this incident, the website owner tries to log in to the admin panel but is unable to, so they reach out to the website hosting provider. You and other cybersecurity analysts are tasked with investigating this security event. To address the incident, you create a sandbox environment to observe the suspicious website behavior. You run the network protocol analyzer tcpdump, then type in the URL for the website, yummyrecipesforme.com. As soon as the website loads, you are prompted to download an executable file to update your browser. You accept the download and allow the file to run. You then observe that your browser redirects you to a different URL, greatrecipesforme.com, which is designed to look like the original site. However, the recipes your company sells are now posted for free on the new website.

Traffic Logs:

```
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?
yummyrecipesforme.com. (24)
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A
203.0.113.22 (40)


14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859
ecr 0,nop,wscale 7], length 0
```

```
14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS
val 3302576859 ecr 3302576859,nop,wscale 7], length 0
14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr
3302576859], length 73: HTTP: GET / HTTP/1.1
14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
…<a lot of traffic on the port 80>...


14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A?
greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A
192.0.2.17 (40)

14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649
ecr 0,nop,wscale 7], length 0
14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags
[S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS
val 3302989649 ecr 3302989649,nop,wscale 7], length 0
14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr
3302989649], length 73: HTTP: GET / HTTP/1.1
14:25:29.576597 IP greatrecipesforme.com.http > your.machine.56378: Flags
[.], ack 74, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
…<a lot of traffic on the port 80>...
```

Incident Report

This particular incident takes advantage of the DNS protocol. According to the logs, attempting to connect with the company's DNS and IP, it is triggering a data pull from the website which then forces user IPs to be redirected to a different DNS with a different IP address. This is likely a brute force attack where a malicious actor gained access to our internal system to reroute the website.

Users reported the company website was prompting them to download a file to update their browsers once arriving at yummyrecipesforme.com and once the file was downloaded, users were rerouted to greatrecipesforme.com. Upon alert of this error, we loaded up a sandbox environment and loaded yummyrecipes.com where we were also directed to download a file and then were rerouted to goodrecipes.com where company recipes were listed for free. When looking at the logs, at 2:18pm our system attempted to connect to yummyrecipes.com with port 52444 but once yummyrecipesforme.com responded to the connection request there was a shift in which port our sandbox was being directed to. At 2:18 the connection with the new port (36086) was made with yummyrecipesforme.com which prompted a request to pull data from the website (HTTP: Get / HTTP/1.1). This request to pull data is most likely the file that is being prompted to be downloaded. Once the data was pulled from yummyrecipesforme.com, a new connection was attempted and successfully made a connection to greatrecipesforme.com at 2:20pm.

It looks like this was a brute force attack where a malicious actor was able to gain access to our systems most likely by repeatedly attempting to find the correct user credentials to access our systems. Going forward we should implement multi factor-authorization to ensure anyone attempting to use company credentials can verify they have correct authorization. It would also be important to salt and hash our passwords so they are harder to guess or discover.

Multimedia Company

Summary of Assignment: You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack. To address this security event, the network security team implemented:

- A new firewall rule to limit the rate of incoming ICMP packets
- Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
- Network monitoring software to detect abnormal traffic patterns
- An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity incident and integrate your analysis into a general security strategy

Incident Report Analysis

The company experienced a security incident in which all network services came to a halt. Our cybersecurity team discovered the disruption of normal operation to be a result of an attack known as a distributed denial of service (DDoS) where a malicious attacker flooded the network with ICMP packets. The attack was blocked and any non-critical network services were stopped as a result so that the team could restore all critical services.

The company was targeted by a type of network attack called a denial of service attack or DDoS. This was discovered by our cybersecurity team after the company experienced high volume network traffic and was being flooded with ICMP packets. As a result all network services ceased immediately and all normal internal traffic could no longer access any network resources. Upon further investigation, the cybersecurity team identified an unconfigured firewall within the company's network which is what the malicious actor used to their advantage to flood our network.

Going forward from this security attack, the team has implemented a new firewall rule that limits the rate of incoming ICMP packets. By limiting the rate of incoming packets, a DDoS attack would be harder to achieve as the firewall would prevent the network from becoming overloaded with pings. Another security measure the team implemented for better firewall configuration is source IP address verification. This will allow for the firewall to check for spoofed IP addresses on incoming ICMP packets. Lastly, our cybersecurity team is investing in an intrusion prevention system (IPS).

In order to better observe network traffic and detect any potential threats coming in, the team has implemented a network monitoring software that will search for abnormal traffic patterns. Going forward there will also be an intrusion detection system (IDS) that will sort through network traffic and filter out ICMP packets based on suspicious characteristics.

Our cybersecurity responded to the attack by blocking incoming ICMP packets.

They then stopped all non-critical network services offline to then be able to restore and continue critical network services.

The team will recover normal operation by properly configuring all firewalls, as the team found one unconfigured firewall. The team will resume network activity first with critical services and finally with non-critical activity once all new security measures have been implemented.