ARAIZ NAQVI

INCIDENT REPORT

High Media

08TH OCTOBER, 2024

2024-2025

ARAIZ NAQVI

TABLE OF CONTENT

- Disclaimer
- Incident Summary
- Incident Details
- NIST Frameworks application

2024-2025

ARAIZ NAQVI

DISCLAIMER

This incident report is a project-based simulation for the fictional organization *High Media*, as part of the "Fundamentals of Cybersecurity" course on Google’s Coursera platform.

While the details may resemble real-world scenarios, all data, systems, and findings are entirely fictitious and created for educational purposes. This incident report does not reflect any actual incidents or vulnerabilities affecting any real organization, including *High Media*.

Though based on practical analysis and protocols, the assessments are conducted in a simulated environment and should not be considered representative of any real entity's security posture.

2024-2025

INCIDENT SUMMARY

Time of Incident:	2024-10-08 14:18:32.192571 (08th October, 2024 2:18:32.192571pm)
Summary of Incident:	Last evening the organisations internal network services were attacked my a threat actor using DDOS attack which caused all services to come to halt for the duration of 2 hours.
Location of Incident:	High Media
Reported By:	Araiz Naqvi
Reported On:	2024-10-08 14:25:29.576597 (08th October, 2024 2:25:29.576597pm)

INCIDENT DETAILS

Type of Incident: DDOS ICMP packet flooding.

Description: Last evening, all of the organisations internal networks were compromised by a threat actor who had found a vulnerability in an unconfigured firewall and flooded the servers with ICMP packets which made the servers crash.

The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

ARAIZ NAQVI

NIST FRAMEWORKS APPLICATION

The NIST or National Institute of Standards and Technology frameworks help support ongoing efforts, consisting of standards, guidelines and best practices to manage cyber-security threats.

We will examine today evening's incident under the following topics:

- Identify
- Protect
- Detect
- Respond
- Recover

(PTO)

2024-2025

IDENTIFY

We will create an inventory of organisational systems, processes, assets, data, people, and capabilities that need to be secured.

We will answer the following questions:

(PTO)

Technology/Asset Management:

Which hardware devices, operating systems, and software were affected?

- High traffic led to congestion in routers, switches, and servers, resulting in network slowdowns and even the loss of legitimate traffic. Additionally, the heavy resource load risked a potential data overflow.

- Most Windows computers were vulnerable to ICMP-based DDoS attacks due to their default setting to respond to ping requests. However, only a small number of Linux and Mac devices, configured to accept ICMP packets, were affected.

- Web servers overloaded with constant ICMP packets crashed, rendering the organisation's website non-functional and resulting in significant damage in finances and reputation.

(PTO)

Process/Business environment:

Which business processes were affected in the attack?

- Social Media Marketers rely on Automation tools, Social Media and scheduling systems that often require access to the internet. During the attack, campaigns may have not been executed and marketing data in accessible.

- Graphic designers using net based tools like Figma were unable to access design files, save work or share custom designs to developers.

- The attack halted or severely disrupted the ability of web designers to access servers, tools and resources required for designing and updating websites. Also, without network no collaboration would be possible.

- Severe halt and delays in response to client inquiries.

(PTO)

People:

Who needs access to the affected systems?

- Designers, Developers, Social Media Marketing Teams.
- Sales and Management Teams
- Customer Care and Client Acquisition teams.
- IT and Network Administrators
- Cyber Security Teams

(PTO)

Client Assets:

What assets with respect to Clients were endangered?

- All web based applications built for clients running on organisations servers could be compromised, severely affecting the organisations reputation and dealing massive financial damages.

- Client data such as PII and SPII of Clients as well as records of Client Organisation’s PII and SPII would be compromised. All design files and marketing content could be stolen.

- Agreements with Clients would be breached leading to loss of contracts and a spoilt reputation.

- Clients Social Media campaigns might be tampered with, ideas stolen and account credentials accessed also causing account shut down.

PROTECT

Develop and implement safeguards to protect the identified items and ensure delivery of services.

We will answer the following questions:

(PTO)

Access control:

Who needs access to the affected items? How are non-trusted sources blocked from having access?

- Designers, developers, social media marketing teams, sales and management, customer care and client acquisition teams, IT and network administrators, and Cyber Security teams.

- The following features will help detect and block non-trusted sources:

  1. Use of Next Gen Fire Walls (NGFW) which are stateful as well as capable of filtering IP Addresses based on location, specific IP ranges and other filters.
  2. IDS’ can track suspicious behaviour and IPS’ can prevent their entrance.
  3. Access Control Lists (ACL) govern whether traffic from certain IP Subnets or ranges are allowed or denied access to specific resources.
  4. Use of MFA’s
  5. Zero Trust Architecture which assumes no entity (inside/outside) is automatically trusted.
  6. DNS filtering can prevent employees from connecting with known malicious domains and websites.

(PTO)

Awareness/Training:

Who needs to be made aware of this attack ?

- In the aftermath of a DDoS attack, ensure key stakeholders within and outside organisation are made aware.

Internal Teams

Management/Executives:

- **Why they need to know:** Senior leadership needs to understand the impact on business operations, finances, and reputation. This helps in decision-making, resource allocation, and setting security priorities.
- **How They Can Help Prevent Future Attacks**: By approving budgets for better security infrastructure, personnel training, and emergency response strategies.

(PTO)

IT/Network Teams:

- **Why they need to know:** These teams manage network infrastructure and are directly responsible for handling attacks and securing systems.
- **How They Can Help Prevent Future Attacks**: Put systems and protocols in place to protect the network.

Cyber Security Team:

- **Why they need to know:** They investigate the source of the attack, its impact, and how it exploited weaknesses in the network.
- **How They Can Help Prevent Future Attacks**: Strengthen the security posture and conduct regular pen testing and other operations.

External Parties

Clients:

- **Why they need to know:** Clients may have experienced service disruption due to the attack, and transparency is key to maintaining trust.
- **How They Can Help Prevent Future Attacks**: Clients can implement security best practices on their end, such as strong passwords, and report suspicious activity they notice.

(PTO)

Internet Service Provider (ISP):

- **Why they need to know:** The ISP can assist in mitigating DDoS attacks by blocking malicious traffic upstream.
- **How They Can Help Prevent Future Attacks**: Work with your organisation to provide DDoS protection services that can detect and filter malicious traffic before it hits your network.

Cyber Security Team:

- **Why they need to know:** They investigate the source of the attack, its impact, and how it exploited weaknesses in the network.
- **How They Can Help Prevent Future Attacks**: Strengthen the security posture and conduct regular pen testing and other operations.

Data security:

Is there any affected data that needs to be made more secure?

- Thorough investigation in source codes and file systems of organisation need to be made to detect any possible back-doors or addition of malicious code.
- Any PII/SPII lost must be recovered and regular backups are to be made.

(PTO)

ARAIZ NAQVI

DETECT

Designing and implementing a system with tools needed for detecting threats and attacks.

We will answer some of the following questions:

(PTO)

2024-2025

Anomalies and events:

What tools could be used to detect and alert IT security staff of anomalies and security events?

- SIEM Tools - Helps keep a log of all network activities.
- IDS & IPS - Helps detect abnormal network activities and prevent them.
- Network Analysing Tool - Tracks every packet over communicated over the network.
- Endpoint Detection and Response Tools - Help detect any endpoint level threat.
- Firewalls - Restricts activity going inside/outside the network.

(PTO)

RESPOND

Designing action plans for responding to threats and attacks.

We will ask the following questions:

(PTO)

Response planning:

What action plans need to be implemented to respond to similar attacks in the future?

- Incident Response Plans

  1. Assign a team who's main responsibility is to observe incoming security incidents.
  2. Make a clear list of steps to take to neutralise the situation.
  3. Create a process to quickly identify, classify and analyse any incoming threat.
  4. Make a clear list of instructions of how to contain a fresh attack.

- Regular Vulnerability Assessments

  1. Use automated tools that check for viruses and vulnerabilities.
  2. Conduct regular pen-testing to find vulnerabilities before the actual hackers find it.
  3. Conduct regular security audits and tests.

- Network Hardening Practices
- Employee Training and Awareness

(PTO)

Araiz Naqvi Network Security Engineer

If you find this helpful, you'll love my content!

M @araiz-naqvi

in @araiznaqvi