Abstract

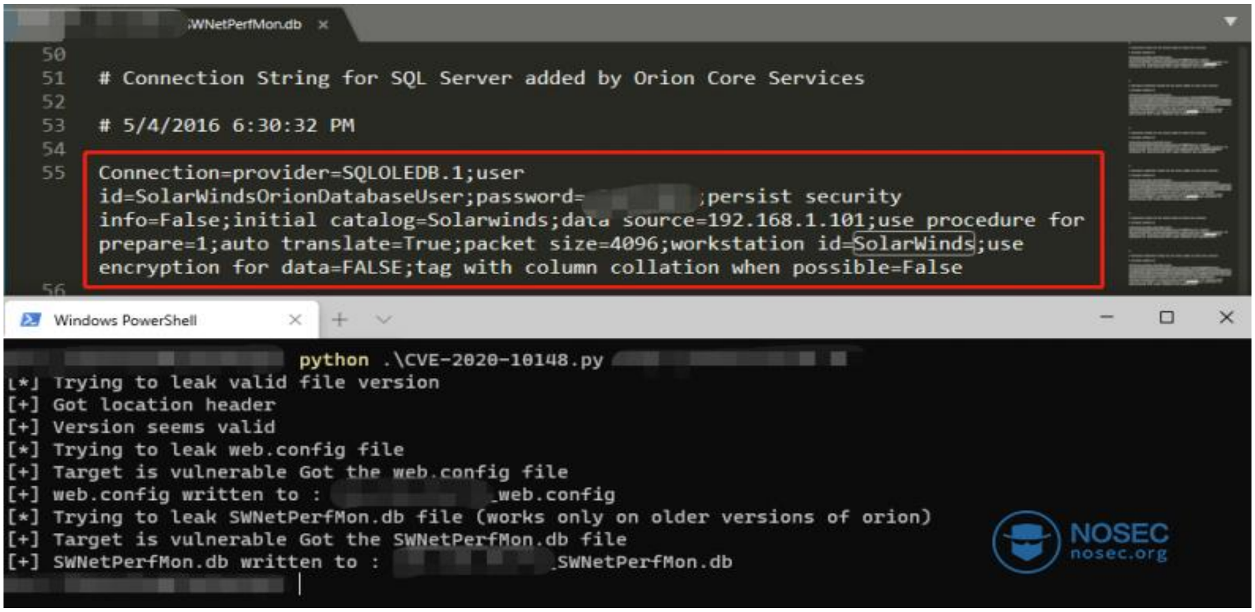
In December 2020, APT29, or Cozy Bear, took advantage of a SolarWinds Orion API vulnerability (CVE-2020-10148) to bring a massive cyber incident across US government agencies, private companies, and critical infrastructures in countries worldwide. This report will study the impact that the breach had on the CIA from compromised systems and data, focusing on the role of supply chain vulnerabilities in modern cybersecurity risks. Since the zero-day flaw was utilized, it allowed the threat actors to execute SUPERNOVA Malware for persistent access, causing huge destruction and raising concerns regarding API security, third-party risk management, and incident response. This paper provides an extensive analysis of the reconnaissance techniques along with OSINT methods, WHOIS lookups, and sub-domain enumeration focusing on JPCERT/CC, the National CERT for Japan. Finally, this article finishes with many recommendations which can further help in enhancing cyber resiliency—like the concept of the zero-trust policies and beefing up API attack surface coverage to gain better regulatory compliance—so that incidents like these do not occur later on.

Table of figures

Task 1: Coursework on SolarWinds Orion (CVE-2020-10148)

1.Introduction

In December 2020, a zero-day vulnerability (**CVE-2020-10148**) in the SolarWinds Orion API allowed attackers to bypass authentication and execute remote commands. **APT29 (Cozy Bear)** exploited this flaw to compromise government agencies and private firms, deploying **SUPERNOVA** malware for persistent access. This breach **severely impacted** confidentiality, integrity, and availability **(CIA)**, exposing critical risks in API security. This report examines the vulnerability, its impact, and countermeasures to mitigate similar threats.



```
# Connection String for SQL Server added by Orion Core Services

# 5/4/2016 6:30:32 PM

Connection=provider=SQLOLEDB.1;user
id=SolarWindsOrionDatabaseUser;password=[redacted];persist security
info=False;initial catalog=Solarwinds;data source=192.168.1.101;use procedure for
prepare=1;auto translate=True;packet size=4096;workstation id=SolarWinds;use
encryption for data=FALSE;tag with column collation when possible=False
```

```
[redacted] python .\CVE-2020-10148.py [redacted]
[*] Trying to leak valid file version
[+] Got location header
[+] Version seems valid
[*] Trying to leak web.config file
[+] Target is vulnerable Got the web.config file
[+] web.config written to : [redacted]_web.config
[*] Trying to leak SWNetPerfMon.db file (works only on older versions of orion)
[+] Target is vulnerable Got the SWNetPerfMon.db file
[+] SWNetPerfMon.db written to : [redacted]_SWNetPerfMon.db
[redacted]
```

Figure 1: SolarWinds Remote Code Execution Vulnerability

Source: www.nosec.org

The image highlights a flaw in the SolarWinds Orion API, where attackers can bypass authentication by modifying URI parameters, enabling unauthorized API commands and remote malware deployment, such as **SUPERNOVA**.

2. Incident Description

In December 2020, APT29 (Cozy Bear) exploited a SolarWinds Orion API zero-day vulnerability (CVE-2020-10148) to compromise thousands of organizations globally, including government agencies and private firms. The attackers bypassed authentication by manipulating URI parameters, allowing them to execute unauthorized commands.

Malicious code, including SUPERNOVA malware, was injected through legitimate SolarWinds software updates, providing persistent access. The breach remained undetected for months, allowing the attackers to move laterally within organizations and exfiltrate sensitive data such as emails and internal reports from U.S. government agencies.

The attack disrupted key operations, causing delays in recovery as organizations scrambled to contain the breach. This prolonged downtime severely damaged client trust, particularly with affected government contractors. The incident highlighted the vulnerabilities in third-party software supply chains, prompting organizations to reassess their vendor security practices and API security measures.

3.CIA Triad Analysis

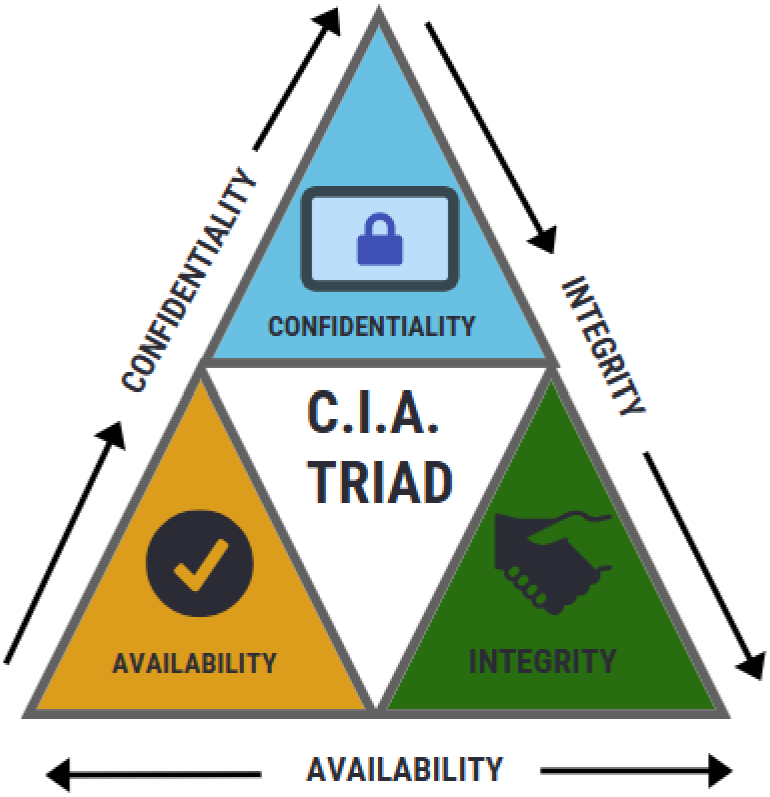


Figure2: C.I.A. TRIAD

The SolarWinds Orion breach had a significant impact on the **Confidentiality, Integrity, and Availability (CIA)** of the compromised systems and data.

3.1Confidentiality:

The attack exposed sensitive data, including internal communications and potentially classified information, to unauthorized access. This breach of confidentiality compromised the privacy and security of affected organizations, leaving critical data vulnerable to theft or exposure.

3.2:Integrity

Although no direct evidence of data manipulation was found, the attackers had the ability to alter or corrupt critical data. The compromise of system integrity posed a serious risk, as unauthorized access to systems could lead to undetected changes in data or security settings, undermining trust in the organization's information.

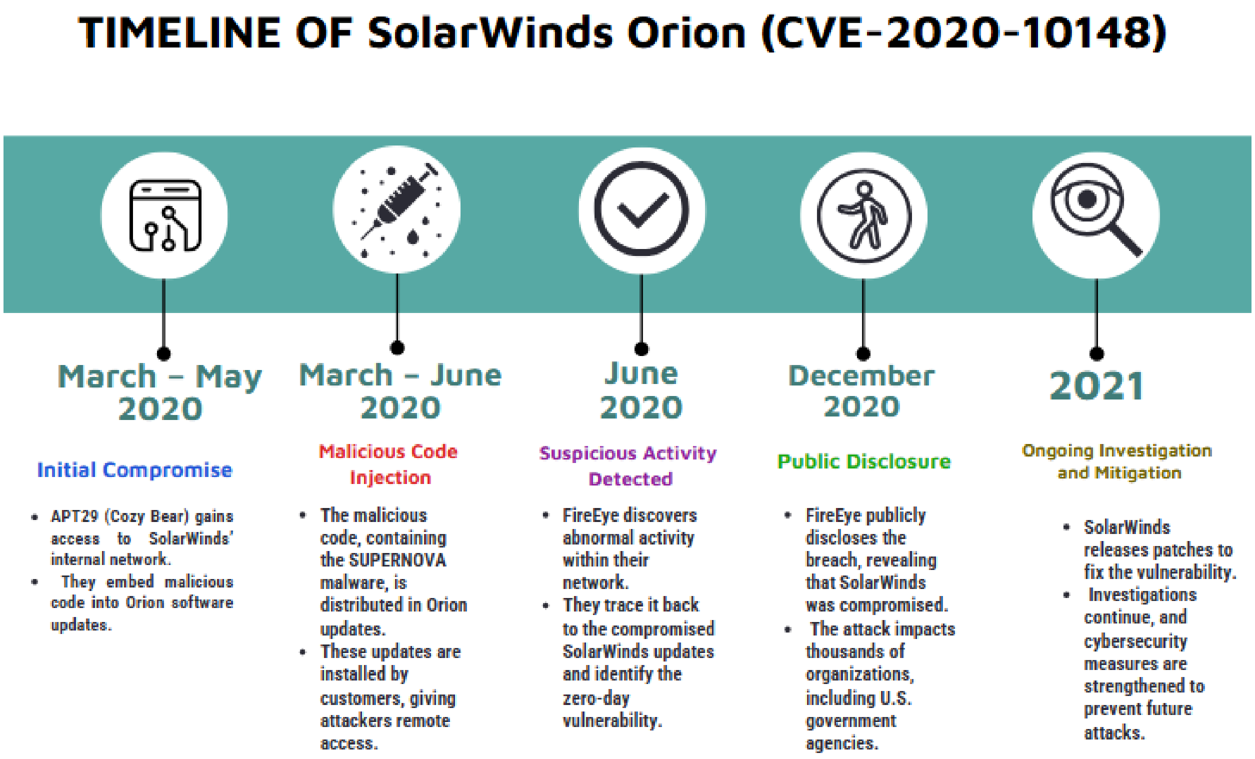
3.3 Availability:

The attack disrupted the availability of key systems and services. As organizations worked to contain the breach, they faced downtime, and operations were hindered. The persistent presence of malware like SUPERNOVA caused delays in restoring normal business functions, impacting the overall availability of services.

Conclusion:

The SolarWinds Orion breach significantly impacted all three elements of the **CIA triad**—confidentiality, integrity, and availability. This highlights the serious risks posed by vulnerabilities in supply chains and underscores the need for more robust security practices to safeguard critical systems and data.

4.Incident analysis



TIMELINE OF SolarWinds Orion (CVE-2020-10148)

March – May 2020

Initial Compromise

- APT29 (Cozy Bear) gains access to SolarWinds' internal network.
- They embed malicious code into Orion software updates.

March – June 2020

Malicious Code Injection

- The malicious code, containing the SUPERNOVA malware, is distributed in Orion updates.
- These updates are installed by customers, giving attackers remote access.

June 2020

Suspicious Activity Detected

- FireEye discovers abnormal activity within their network.
- They trace it back to the compromised SolarWinds updates and identify the zero-day vulnerability.

December 2020

Public Disclosure

- FireEye publicly discloses the breach, revealing that SolarWinds was compromised.
- The attack impacts thousands of organizations, including U.S. government agencies.

2021

Ongoing Investigation and Mitigation

- SolarWinds releases patches to fix the vulnerability.
- Investigations continue, and cybersecurity measures are strengthened to prevent future attacks.

Figure:3 Timeline of SolarWinds Orion Vulnerability

The SolarWinds Orion breach, spanning from March 2020 to December 2020, exposed critical vulnerabilities in software supply chains, demonstrating the sophisticated tactics of APT29. The attack not only compromised sensitive data across multiple sectors but also highlighted the urgent need for stronger security measures in third-party software management and API security.

4.2 Key Assets at Risk

Sensitive Data: Confidential government communications and PII were exposed, risking theft and privacy breaches.

Network Infrastructure: The breach compromised critical systems, allowing unauthorized access to sensitive servers.

System Integrity: Attackers could alter configurations, undermining trust in the security of affected systems.

Reputation: SolarWinds and its clients faced severe reputational damage due to the breach's scale and impact.

Compliance: Exfiltration of sensitive data posed a risk of violating regulatory requirements, leading to potential fines.

4.2 Magnitude of Harm

The exploitation of CVE-2020-10148 caused both immediate and long-term impacts:

Immediate Effects:

The breach had immediate consequences, such as the exfiltration of sensitive data. For instance, data from government agencies, including DHS and the Department of Energy, was stolen. SUPERNOVA malware disrupted operations, especially in organizations like FireEye, which had to devote significant resources to recover and secure their systems.

Long-term Consequences:

Long-term impacts included severe reputational damage to SolarWinds, with organizations like Microsoft and FireEye losing confidence in the security of their supply chain. The breach also raised concerns about API security, leading to increased scrutiny from regulators. Potential regulatory penalties and legal consequences loomed for organizations that had failed to detect or prevent the attack.

4.3 Recommendation

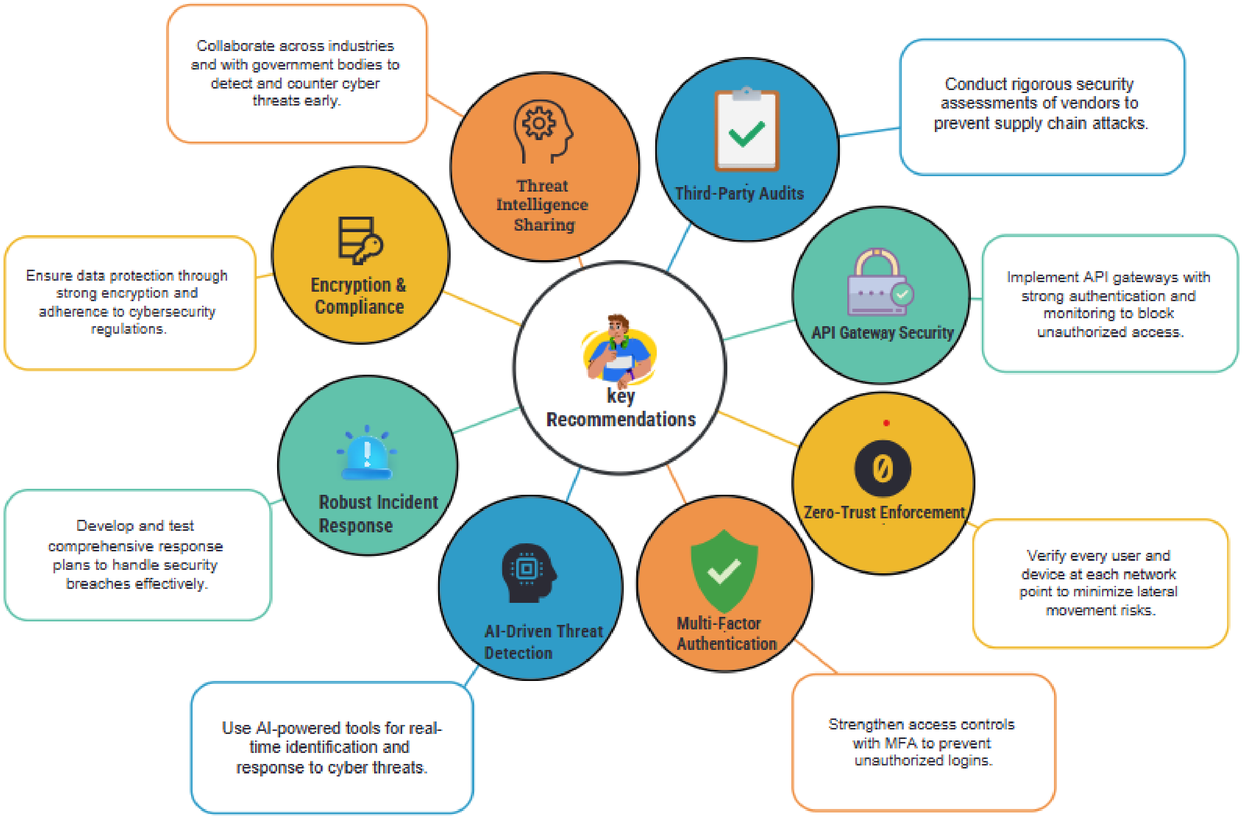

Collaborate across industries and with government bodies to detect and counter cyber threats early.
Threat Intelligence Sharing
Third-Party Audits
Conduct rigorous security assessments of vendors to prevent supply chain attacks.
Ensure data protection through strong encryption and adherence to cybersecurity regulations.
Encryption & Compliance
key Recommendations
API Gateway Security
Implement API gateways with strong authentication and monitoring to block unauthorized access.
Robust Incident Response
Develop and test comprehensive response plans to handle security breaches effectively.
Zero-Trust Enforcement
Verify every user and device at each network point to minimize lateral movement risks.
AI-Driven Threat Detection
Multi-Factor Authentication
Use AI-powered tools for real-time identification and response to cyber threats.
Strengthen access controls with MFA to prevent unauthorized logins.

Figure4: Mind diagram of key Recommendations

To mitigate the SolarWinds compromise, strong prior assessments and audits of third-party systems are crucial. API Gateways should be developed to monitor and secure critical functionality with sophisticated authentication and MFA. A zero-trust policy with strict user verification and network monitoring can limit lateral movement after a breach. Organizations should enhance incident response with AI-driven detection tools and a comprehensive response plan. Emphasizing regulatory compliance, encryption, and training can help protect sensitive information. Collaboration across sectors and with government bodies to share threat information can improve collective defense and early anomaly detection, building resilience across the industry.

5.Conclusion

The 2020 SolarWinds Orion breach exposed critical weaknesses in software supply chains, with API security as a key concern. The APT29 group exploited a zero-day flaw to compromise thousands of entities, causing immediate financial impact and raising long-term issues of trust, compliance, and legal consequences. This incident highlights the need for improved third-party risk management, continuous cybersecurity improvements, and collective organizational response. Organizations must strengthen security protocols, enhance incident response, and foster regulatory compliance to mitigate these risks. The breach underscores that weaknesses in digital supply chains can lead to significant damage, emphasizing the need for proactive, holistic security measures.

Task 2: Passive Reconnaissance of JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)

6. Introduction

Reconnaissance is one of the important elements of any security infrastructure. It involves gathering information about a target organization to understand its security posture. This report looks into one of the major cybersecurity organizations in the Asia-Pacific Region, JPCERT/CC, in an ethical and legal perspective, focusing on the use of OSINT techniques and tools.

7. Organization Overview

7.1 Background

JPCERT/CC was established in 1996 as Japan's first computer emergency response team (CERT). It operates as an independent nonprofit organization, working to detect, analyze, and mitigate cyber threats affecting Japan and the global cybersecurity landscape.

Towards a safer cyber space without incidents.
JPCERT Coordination Center

Figure 5: JPCERT Coordination Center

7.2 Key Cybersecurity Operations

JPCERT/CC handles cyber incidents, threat intelligence, malware analysis, vulnerability coordination, and cybersecurity capacity building. As Japan's national CERT, it plays a key role in detecting, analyzing, and mitigating cyber threats. The organization provides incident response, collaborates on vulnerability disclosures, conducts malware research, and offers training programs to strengthen Japan’s cyber defenses.

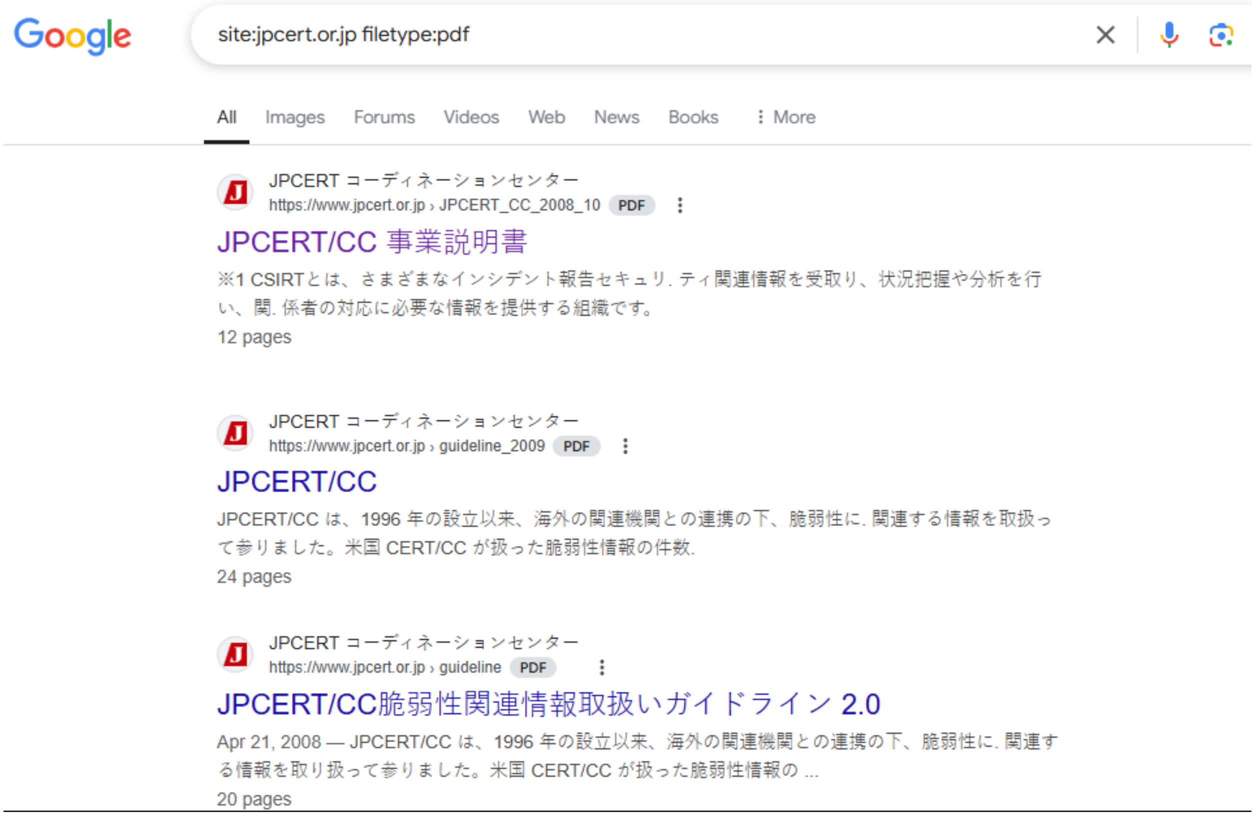
7.3 Relevance to Cybersecurity & Key Incidents

As Japan’s national CERT, JPCERT/CC plays a critical role in securing infrastructure, businesses, and government networks against cyber threats. It collaborates with global agencies like US-CERT and FIRST. Notable incidents include responding to **Operation Cloud Hopper** (a supply chain attack by APT10), **targeted attacks on Japanese companies** involving phishing and APTs, and **coordinating responses to ransomware threats** affecting local industries.

8. Reconnaissance Tools and Techniques

8.1 OSINT (Open-Source Intelligence) Techniques

8.1.1 Google Dorking



site:jpcert.or.jp filetype:pdf

JPCERT コーディネーションセンター
https://www.jpcert.or.jp › JPCERT_CC_2008_10 PDF

JPCERT/CC 事業説明書

※1 CSIRTとは、さまざまなインシデント報告セキュリ. ティ関連情報を受取り、状況把握や分析を行い、関. 係者の対応に必要な情報を提供する組織です。

12 pages

JPCERT コーディネーションセンター
https://www.jpcert.or.jp › guideline_2009 PDF

JPCERT/CC

JPCERT/CC は、1996 年の設立以来、海外の関連機関との連携の下、脆弱性に. 関連する情報を取扱って参りました。米国 CERT/CC が扱った脆弱性情報の件数.

24 pages

JPCERT コーディネーションセンター
https://www.jpcert.or.jp › guideline PDF

JPCERT/CC脆弱性関連情報取扱いガイドライン 2.0

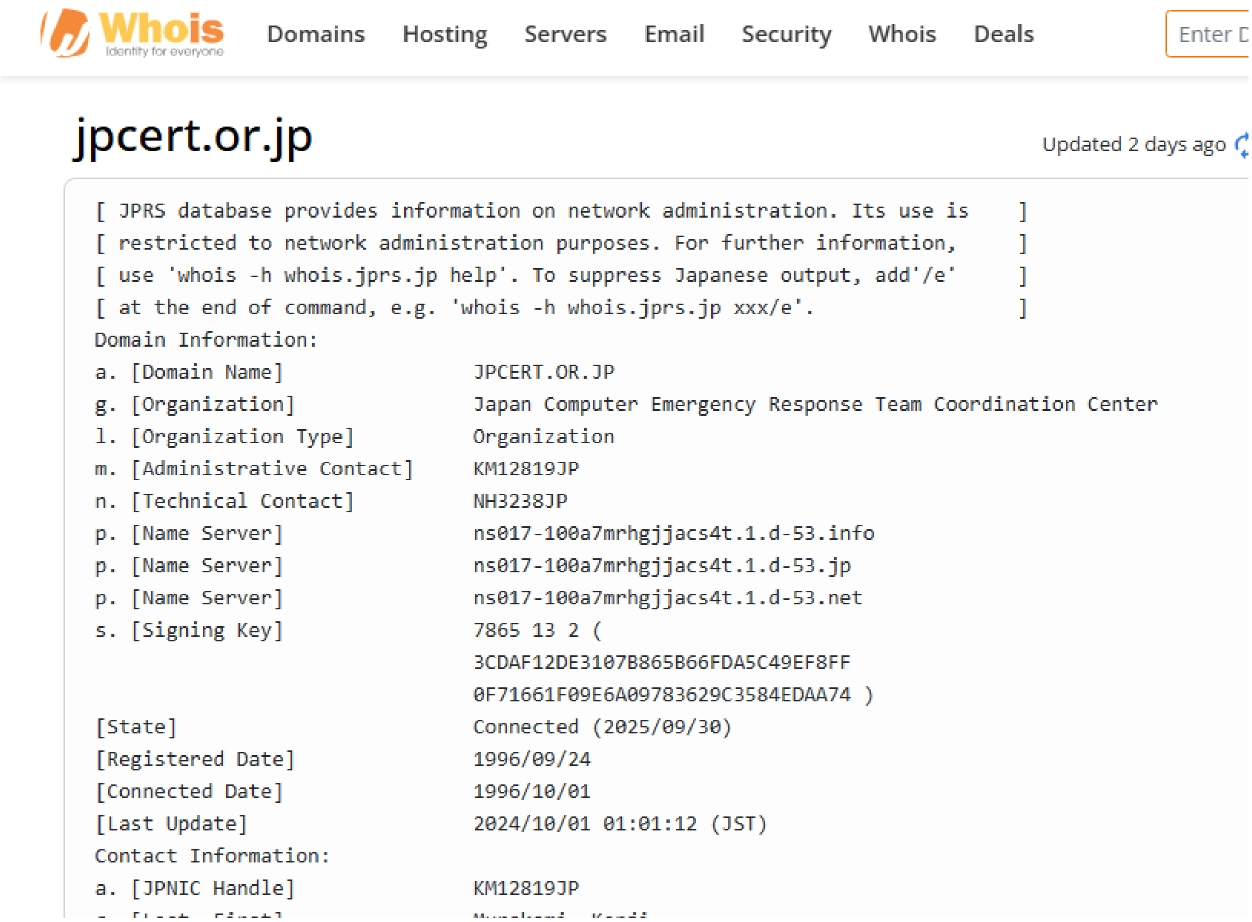
Apr 21, 2008 — JPCERT/CC は、1996 年の設立以来、海外の関連機関との連携の下、脆弱性に. 関連する情報を取り扱って参りました。米国 CERT/CC が扱った脆弱性情報の ...

20 pages

Figure 6: Google Dorking for "JPCERT/CC"

Google Dorking, such as the query "site:jpcert.or.jp filetype:pdf," uses advanced search operators to find specific resources, like PDF files, on a website. It helps uncover hidden or less accessible information.

8.1.2 WHOIS Lookup

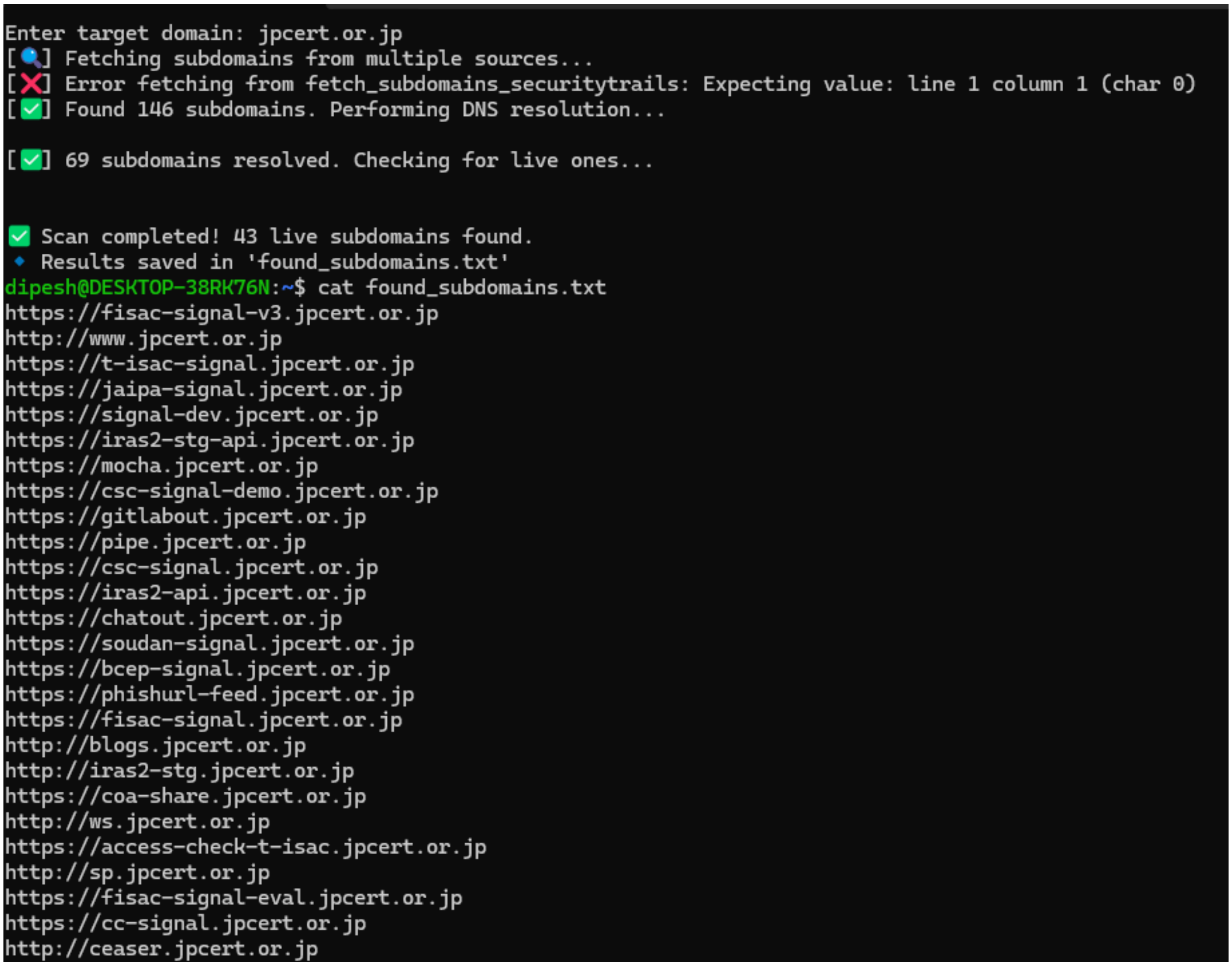


```
[ JPRS database provides information on network administration. Its use is    ]
[ restricted to network administration purposes. For further information,     ]
[ use 'whois -h whois.jprs.jp help'. To suppress Japanese output, add'/e'     ]
[ at the end of command, e.g. 'whois -h whois.jprs.jp xxx/e'.                 ]
Domain Information:
a. [Domain Name]                JPCERT.OR.JP
g. [Organization]               Japan Computer Emergency Response Team Coordination Center
l. [Organization Type]          Organization
m. [Administrative Contact]     KM12819JP
n. [Technical Contact]          NH3238JP
p. [Name Server]                ns017-100a7mrhgjjacs4t.1.d-53.info
p. [Name Server]                ns017-100a7mrhgjjacs4t.1.d-53.jp
p. [Name Server]                ns017-100a7mrhgjjacs4t.1.d-53.net
s. [Signing Key]                7865 13 2 (
                                3CDAF12DE3107B865B66FDA5C49EF8FF
                                0F71661F09E6A09783629C3584EDAA74 )
[State]                         Connected (2025/09/30)
[Registered Date]               1996/09/24
[Connected Date]                1996/10/01
[Last Update]                   2024/10/01 01:01:12 (JST)
Contact Information:
a. [JPNIC Handle]               KM12819JP
c. [Last, First]                Murakami, Kenji
```

Figure 7: WHOis lookup for "JPERT/CC"

A **WHOIS** lookup on the domain jpcert.or.jp retrieves details about domain registration, organization, name servers, and contact information. WHOIS is a protocol used to query databases that store information on domain ownership, registration dates, and administrative contacts.

8.2 Subdomain Enumeration



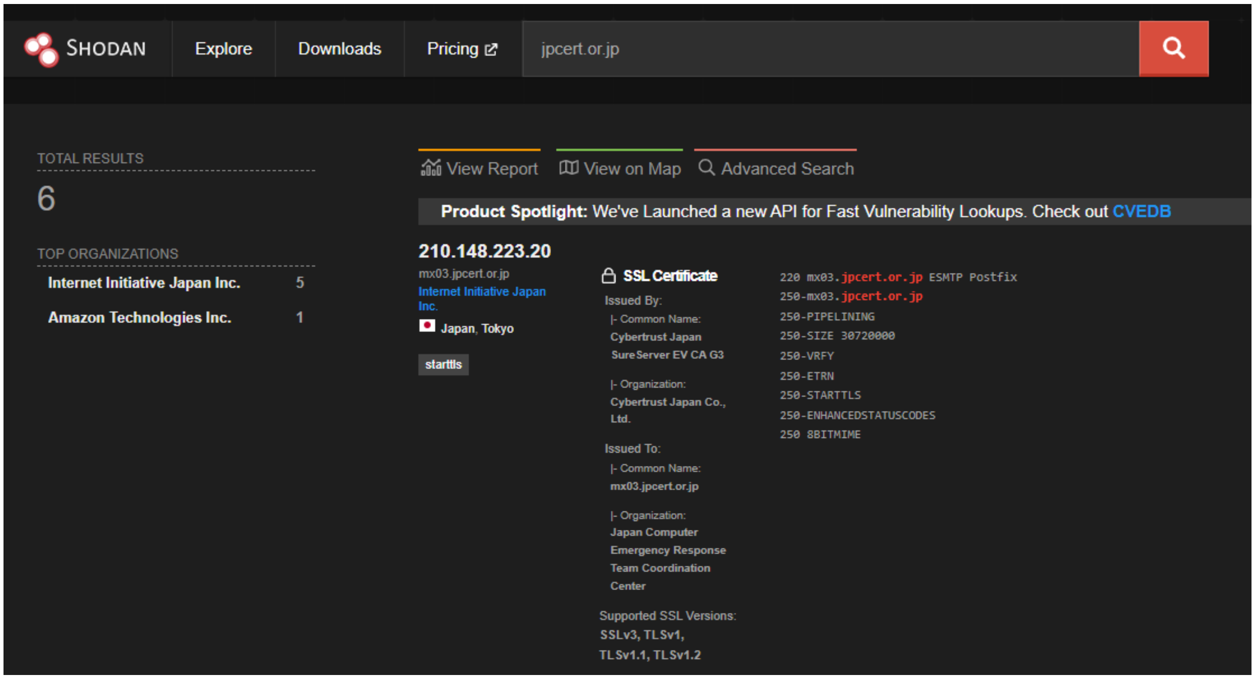
```
Enter target domain: jpcert.or.jp
[🔍] Fetching subdomains from multiple sources...
[❌] Error fetching from fetch_subdomains_securitytrails: Expecting value: line 1 column 1 (char 0)
[✅] Found 146 subdomains. Performing DNS resolution...

[✅] 69 subdomains resolved. Checking for live ones...


✅ Scan completed! 43 live subdomains found.
🔹 Results saved in 'found_subdomains.txt'
dipesh@DESKTOP-38RK76N:~$ cat found_subdomains.txt
https://fisac-signal-v3.jpcert.or.jp
http://www.jpcert.or.jp
https://t-isac-signal.jpcert.or.jp
https://jaipa-signal.jpcert.or.jp
https://signal-dev.jpcert.or.jp
https://iras2-stg-api.jpcert.or.jp
https://mocha.jpcert.or.jp
https://csc-signal-demo.jpcert.or.jp
https://gitlabout.jpcert.or.jp
https://pipe.jpcert.or.jp
https://csc-signal.jpcert.or.jp
https://iras2-api.jpcert.or.jp
https://chatout.jpcert.or.jp
https://soudan-signal.jpcert.or.jp
https://bcep-signal.jpcert.or.jp
https://phishurl-feed.jpcert.or.jp
https://fisac-signal.jpcert.or.jp
http://blogs.jpcert.or.jp
http://iras2-stg.jpcert.or.jp
https://coa-share.jpcert.or.jp
http://ws.jpcert.or.jp
https://access-check-t-isac.jpcert.or.jp
http://sp.jpcert.or.jp
https://fisac-signal-eval.jpcert.or.jp
https://cc-signal.jpcert.or.jp
http://ceaser.jpcert.or.jp
```

Figure 8: Subdomain enumeration on "jpcert.or.jp"

A SubHunter tool was used to perform subdomain enumeration on jpcert.or.jp, identifying 43 live subdomains and saving the results for analysis.

8.3 Network and Infrastructure Analysis

8.3.1 Shodan Scanning (Passive reconnaissance only)



TOTAL RESULTS

6

TOP ORGANIZATIONS

Internet Initiative Japan Inc.	5
Amazon Technologies Inc.	1

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

210.148.223.20
mx03.jpcert.or.jp
Internet Initiative Japan Inc.
Japan, Tokyo

SSL Certificate

Issued By:
|- Common Name:
Cybertrust Japan SureServer EV CA G3
|- Organization:
Cybertrust Japan Co., Ltd.

Issued To:
|- Common Name:
mx03.jpcert.or.jp
|- Organization:
Japan Computer Emergency Response Team Coordination Center

Supported SSL Versions:
SSLv3, TLSv1, TLSv1.1, TLSv1.2

```
220 mx03.jpcert.or.jp ESMTP Postfix
250-mx03.jpcert.or.jp
250-PIPELINING
250-SIZE 30720000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250 8BITMIME
```

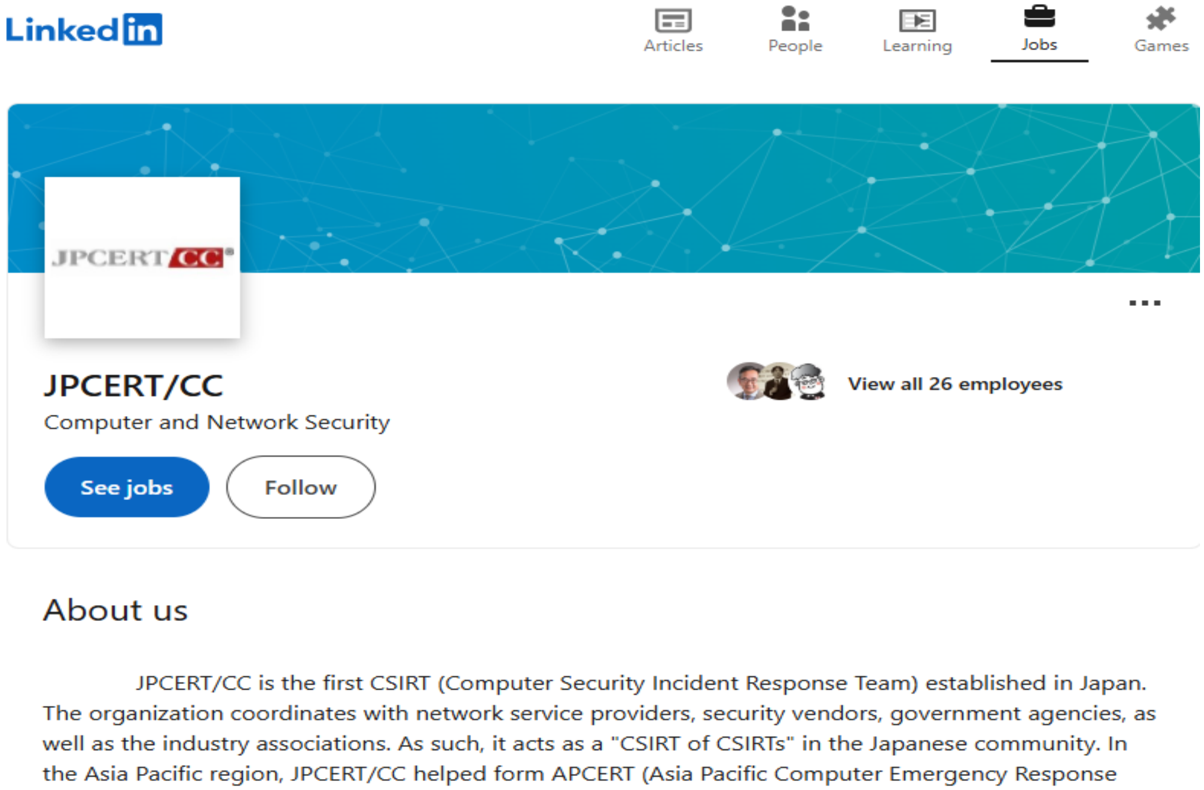
Figure 9: SHODAN Scanning for "jpcert.or.jp"

The scan reveals JPCERT/CC's mail server (mx03.jpcert.or.jp), hosted by Internet Initiative Japan, with details on the **SSL** certificate, supported **TLS** versions, and Postfix capabilities like **STARTTLS** and email size limits.

8.3.2 Social media analysis

Platforms like contact out, twitter, LinkedIn were analyzed to view or inspect the company's information and engagement and details with community with public.

8.3.3 LinkedIn



JPCERT/CC

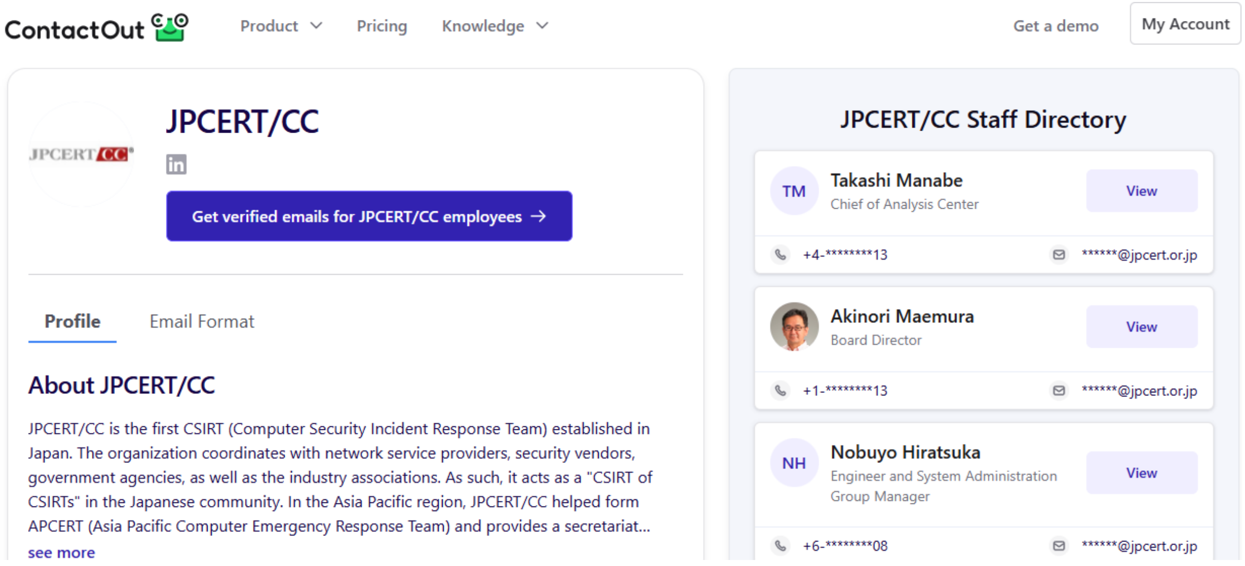
Computer and Network Security

About us

JPCERT/CC is the first CSIRT (Computer Security Incident Response Team) established in Japan. The organization coordinates with network service providers, security vendors, government agencies, as well as the industry associations. As such, it acts as a "CSIRT of CSIRTs" in the Japanese community. In the Asia Pacific region, JPCERT/CC helped form APCERT (Asia Pacific Computer Emergency Response

Figure 10: LinkedIn results of "JPCERT/CC"

8.3.4 ContactOut



JPCERT/CC

About JPCERT/CC

JPCERT/CC is the first CSIRT (Computer Security Incident Response Team) established in Japan. The organization coordinates with network service providers, security vendors, government agencies, as well as the industry associations. As such, it acts as a "CSIRT of CSIRTs" in the Japanese community. In the Asia Pacific region, JPCERT/CC helped form APCERT (Asia Pacific Computer Emergency Response Team) and provides a secretariat...
see more

JPCERT/CC Staff Directory

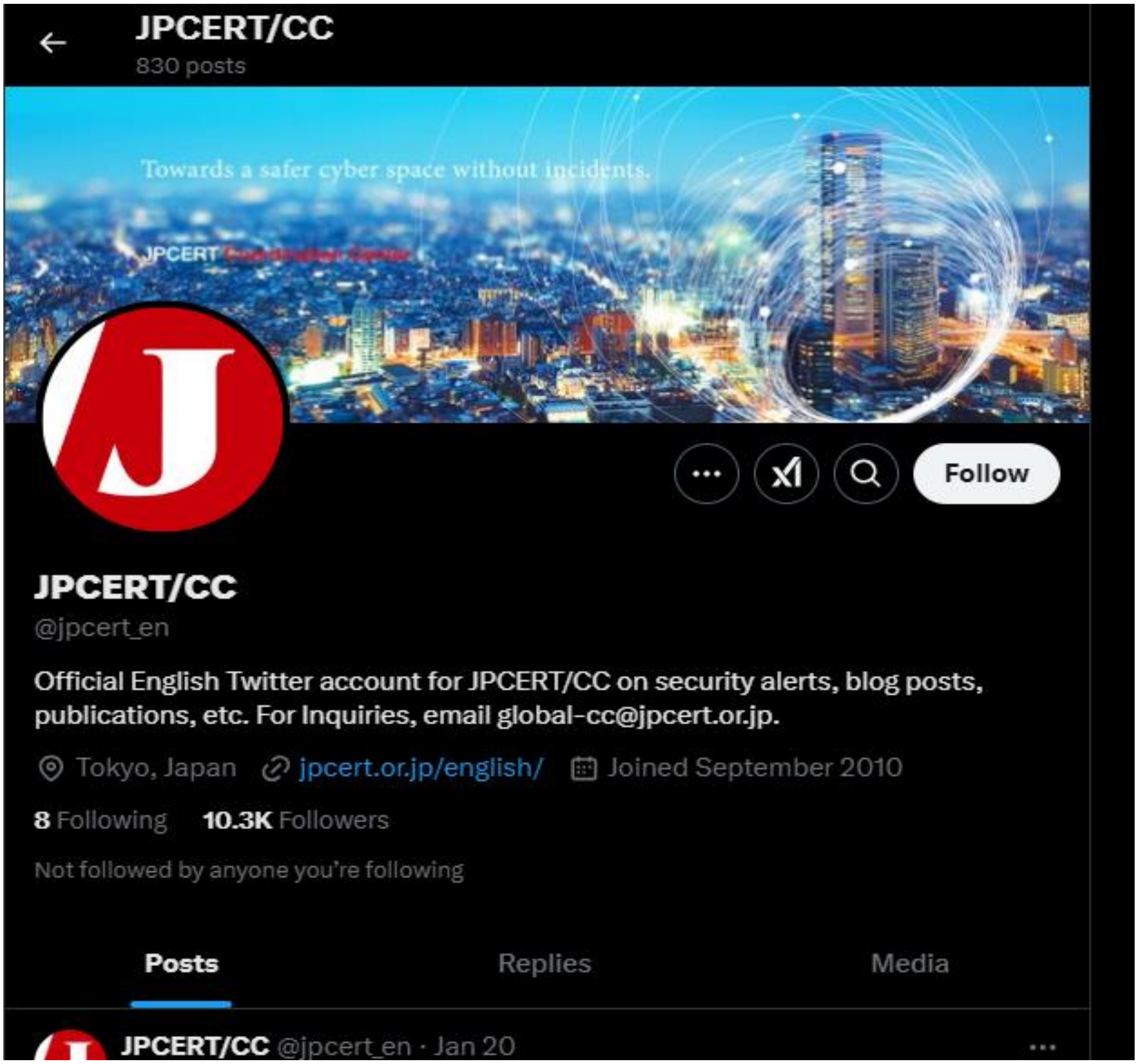
TM Takashi Manabe
Chief of Analysis Center
+4-********13 ******@jpcert.or.jp

Akinori Maemura
Board Director
+1-********13 ******@jpcert.or.jp

NH Nobuyo Hiratsuka
Engineer and System Administration Group Manager
+6-********08 ******@jpcert.or.jp

Figure 11: Staff Directory on ContactOut

8.3.5 Twitter



JPCERT/CC

830 posts

Towards a safer cyber space without incidents.
JPCERT Coordination Center
Follow

JPCERT/CC

@jpcert_en

Official English Twitter account for JPCERT/CC on security alerts, blog posts, publications, etc. For Inquiries, email global-cc@jpcert.or.jp.

Tokyo, Japan jpcert.or.jp/english/ Joined September 2010

8 Following 10.3K Followers

Not followed by anyone you're following

JPCERT/CC @jpcert_en · Jan 20

Figure 12: "JPCERT/CC" on Twitter

8.3.6 Maltego for Relationship Mapping

The Maltego app was used for the Relationship Mapping on the company's website details where

Different entities like DNS, IP and were transformed for this result.

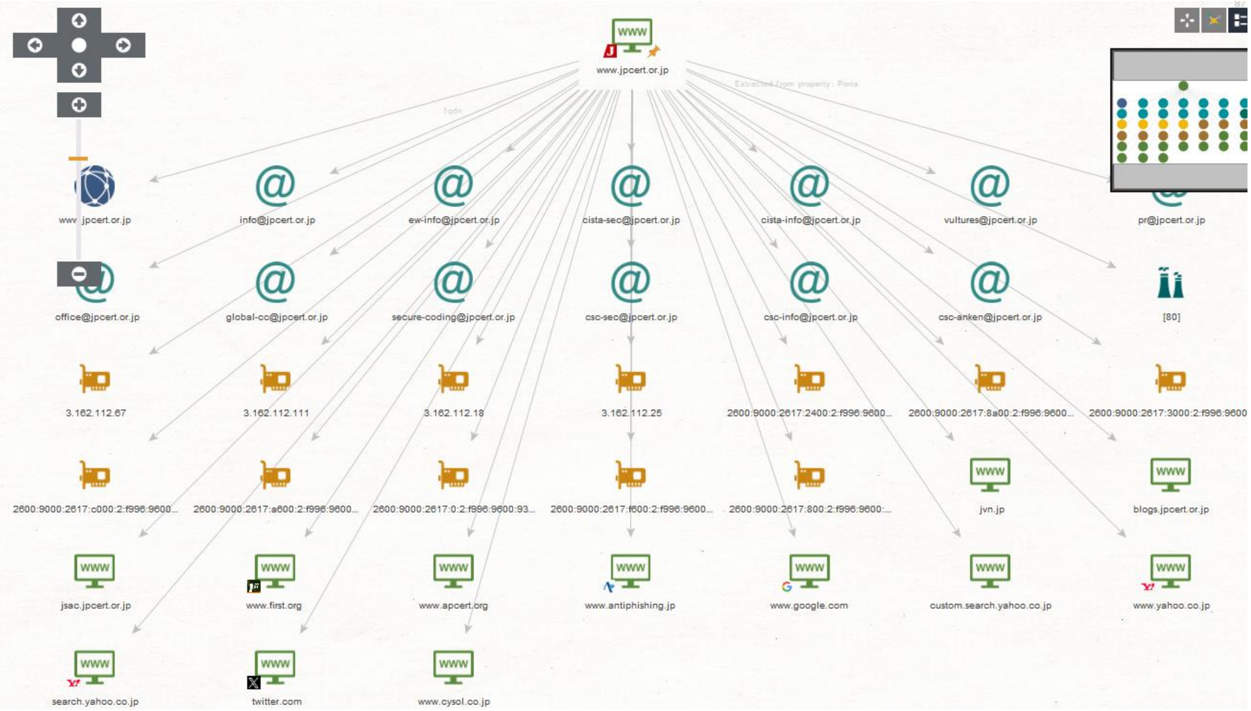


Figure 13: Use of Maltego for Relationship Mapping

8.4 Ethical Considerations and Findings

The reconnaissance was conducted using only publicly available data to comply with ethical standards like the **Computer Misuse Act (1990)**, **Japanese Cybersecurity Laws**, and **GDPR**. JPCERT/CC demonstrates strong security with **TLS encryption**, **restricted WHOIS information**, and secure services, while actively promoting cybersecurity awareness through advisories. No significant vulnerabilities or misconfigurations were identified, showcasing a robust security posture.

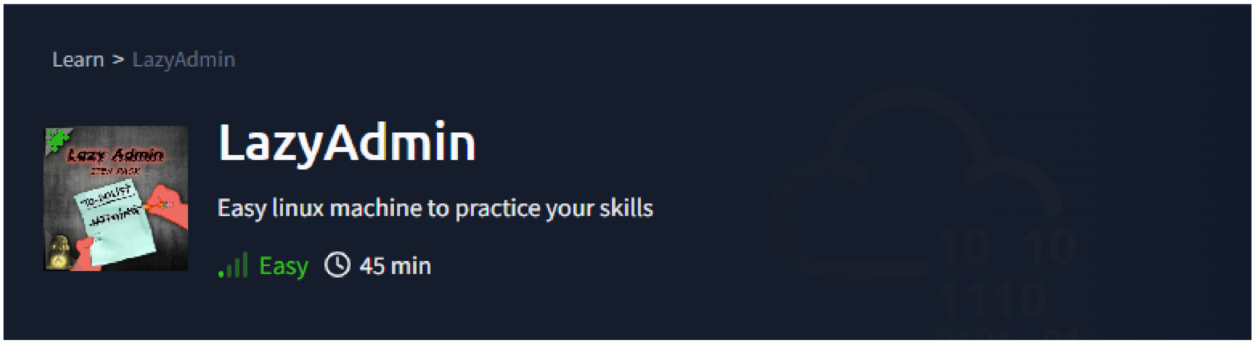
8.5 Conclusion

This reconnaissance exercise on JPCERT/CC demonstrates the organization’s robust cybersecurity posture. The analysis, conducted using ethical OSINT techniques, revealed that JPCERT/CC is a highly secure and reputable cybersecurity entity in the Asia-Pacific region. Future recommendations include continuous monitoring of potential threats and expanding awareness campaigns to counter evolving cyber threats.

Task 3: Active Reconnaissance on LazyAdmin

9.Background

The **LazyAdmin** room on **TryHackMe** is an easy-level challenge. The room simulates a scenario where an attacker must exploit vulnerabilities to escalate privileges on a vulnerable system. For the purpose of this task, we are only conducting active reconnaissance to identify open ports, hidden directories, and potentially sensitive files. This reconnaissance helps map the system and find attack vectors, such as exposed backup files that can be leveraged for further exploitation.



Learn > LazyAdmin

LazyAdmin

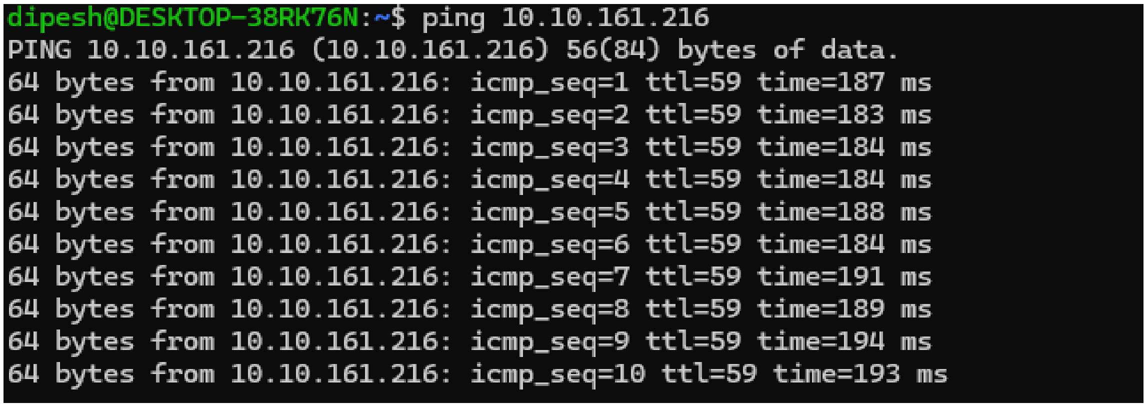
Easy linux machine to practice your skills

Easy 45 min

10.Tools used for active Reconnaissance

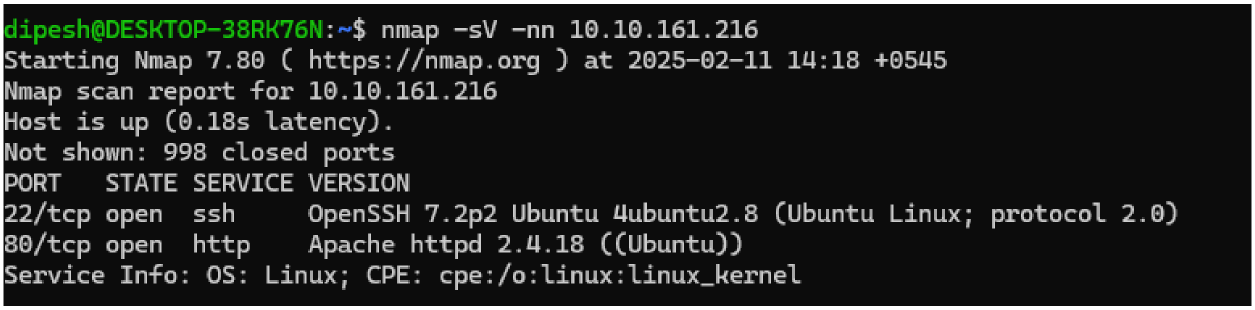
10.1 Ping Scan

A simple way to check if the target is live or if a host is reachable.



```
dipesh@DESKTOP-38RK76N:~$ ping 10.10.161.216
PING 10.10.161.216 (10.10.161.216) 56(84) bytes of data.
64 bytes from 10.10.161.216: icmp_seq=1 ttl=59 time=187 ms
64 bytes from 10.10.161.216: icmp_seq=2 ttl=59 time=183 ms
64 bytes from 10.10.161.216: icmp_seq=3 ttl=59 time=184 ms
64 bytes from 10.10.161.216: icmp_seq=4 ttl=59 time=184 ms
64 bytes from 10.10.161.216: icmp_seq=5 ttl=59 time=188 ms
64 bytes from 10.10.161.216: icmp_seq=6 ttl=59 time=184 ms
64 bytes from 10.10.161.216: icmp_seq=7 ttl=59 time=191 ms
64 bytes from 10.10.161.216: icmp_seq=8 ttl=59 time=189 ms
64 bytes from 10.10.161.216: icmp_seq=9 ttl=59 time=194 ms
64 bytes from 10.10.161.216: icmp_seq=10 ttl=59 time=193 ms
```

10.2 Nmap and Port Scanning



```
dipesh@DESKTOP-38RK76N:~$ nmap -sV -nn 10.10.161.216
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-11 14:18 +0545
Nmap scan report for 10.10.161.216
Host is up (0.18s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

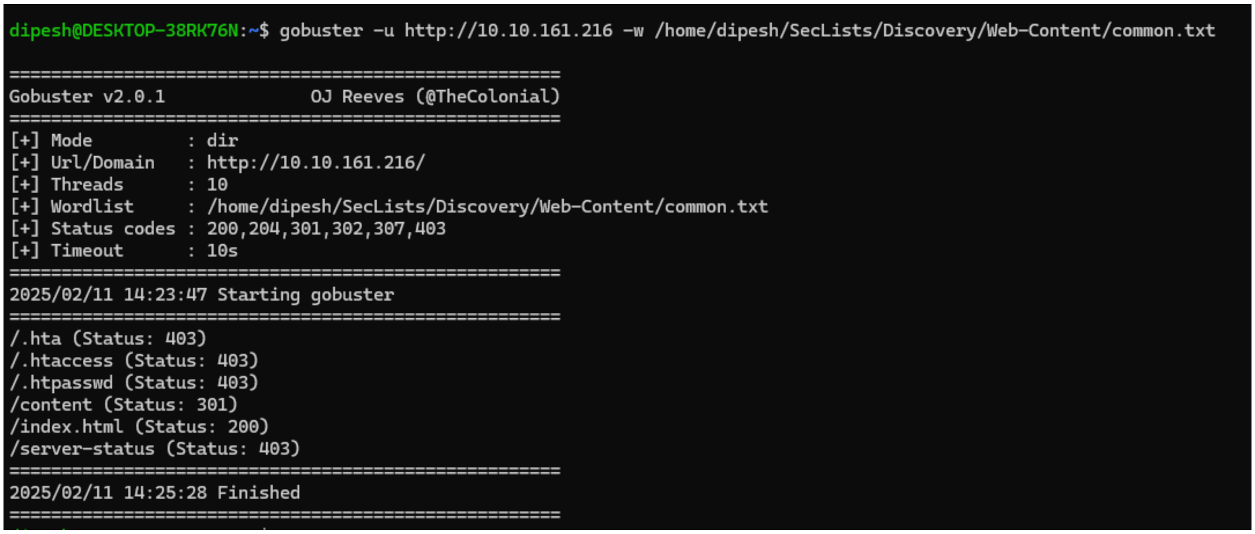
Scanned open ports (22, 80) and identified running services.

Command: nmap -sV -nn <target-IP>

Purpose: Identified Apache 2.4.18 and SSH services.

10.3 Directory Brute Forcing

Tool: gobuster

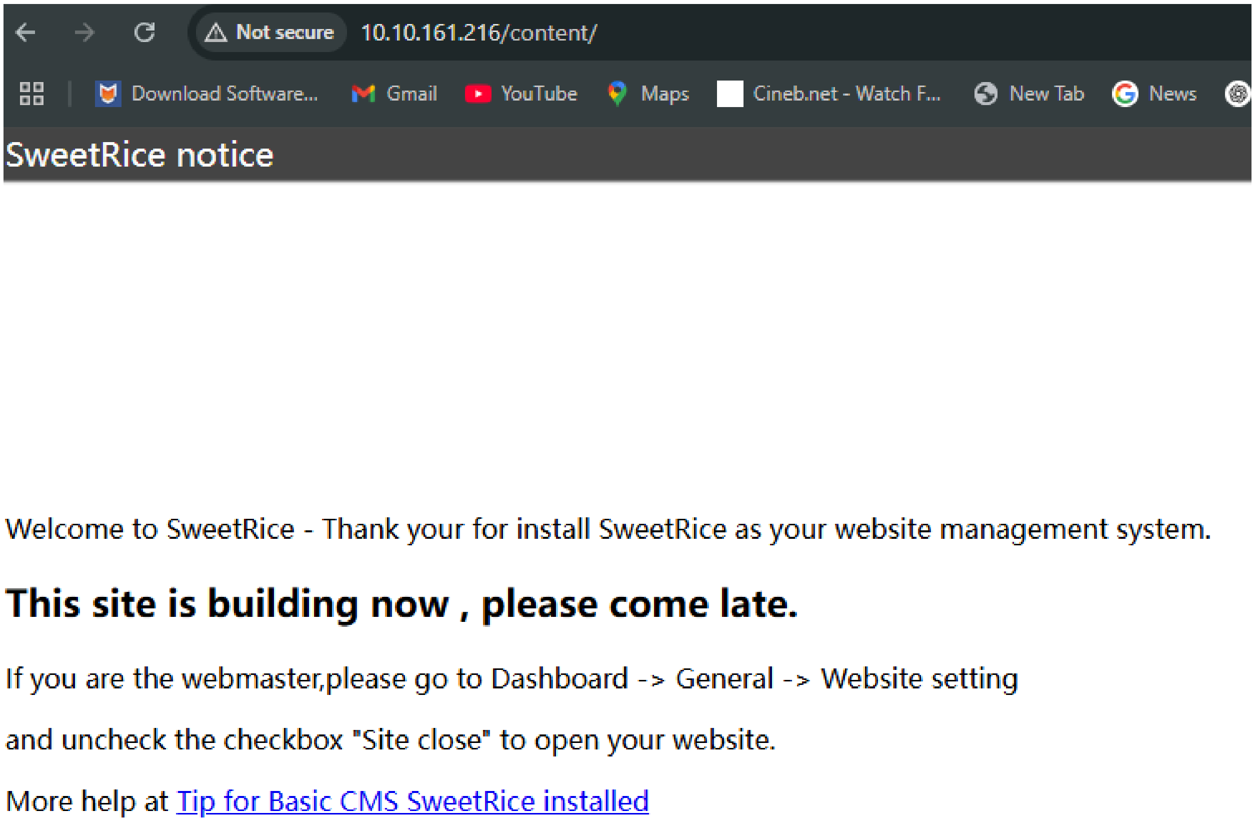


```
dipesh@DESKTOP-38RK76N:~$ gobuster -u http://10.10.161.216 -w /home/dipesh/SecLists/Discovery/Web-Content/common.txt

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.161.216/
[+] Threads      : 10
[+] Wordlist     : /home/dipesh/SecLists/Discovery/Web-Content/common.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
=====================================================
2025/02/11 14:23:47 Starting gobuster
=====================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/content (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
=====================================================
2025/02/11 14:25:28 Finished
=====================================================
```

Enumerated directories on the web server.

Command: gobuster -u http://10.10.245.60 -w /path/to/wordlist.txt

Result: Discovered /content directory.



SweetRice notice

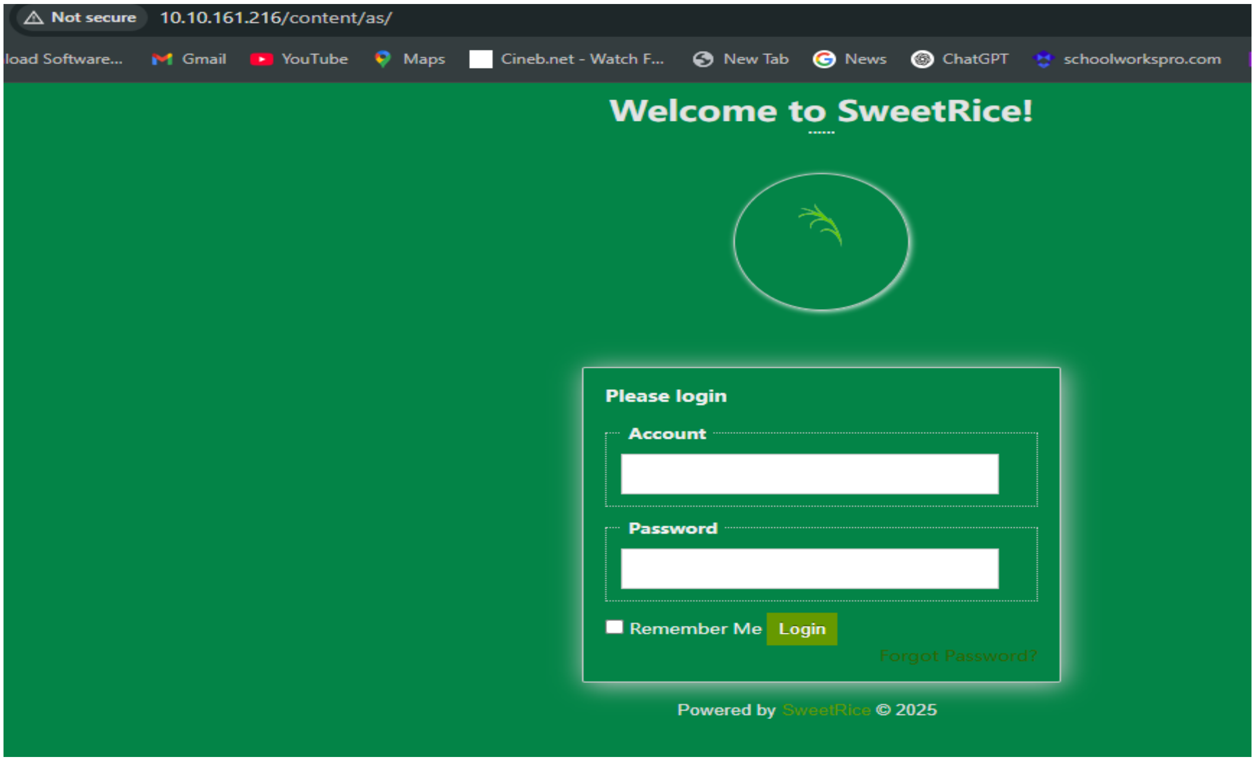
Welcome to SweetRice - Thank your for install SweetRice as your website management system.

This site is building now , please come late.

If you are the webmaster,please go to Dashboard -> General -> Website setting

and uncheck the checkbox "Site close" to open your website.

More help at [Tip for Basic CMS SweetRice installed]()



Welcome to SweetRice!

Please login

Account

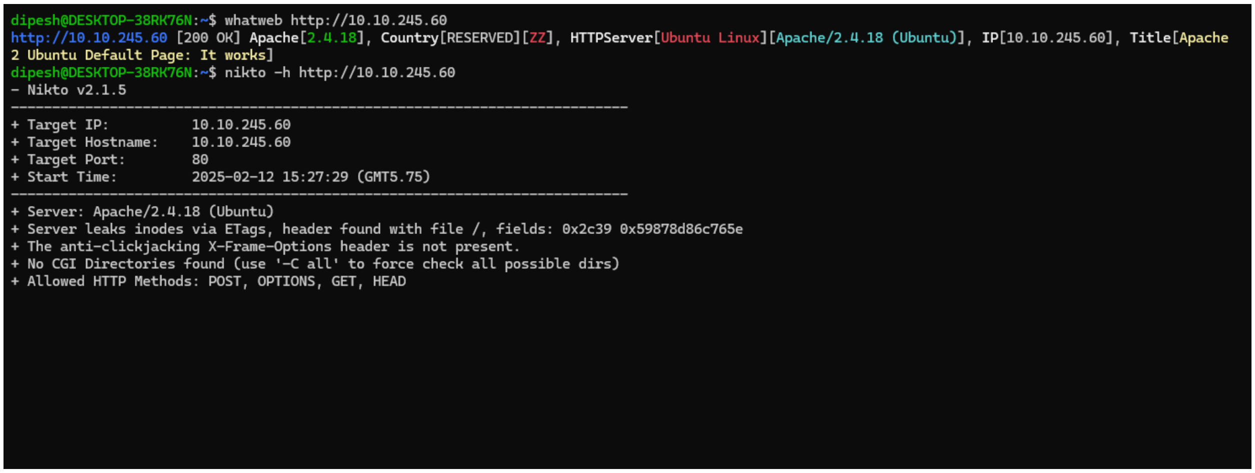
Password

□ Remember Me Login

Forgot Password?

Powered by SweetRice © 2025

10.4 WhatWeb and Nikto Scan



```
dipesh@DESKTOP-38RK76N:~$ whatweb http://10.10.245.60
http://10.10.245.60 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.245.60], Title[Apache
2 Ubuntu Default Page: It works]
dipesh@DESKTOP-38RK76N:~$ nikto -h http://10.10.245.60
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.10.245.60
+ Target Hostname:    10.10.245.60
+ Target Port:        80
+ Start Time:         2025-02-12 15:27:29 (GMT5.75)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x2c39 0x59878d86c765e
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
```

WhatWeb: Detected web technologies.

Result: Apache 2.4.18 on Ubuntu, default web page detected.

Nikto: Scanned for web server vulnerabilities.

Command: nikto -h http://10.10.245.60

Result: ETag leak, missing X-Frame-Options header, and excessive HTTP methods.

11.Probable Vulnerabilities

i. **Outdated Apache (2.4.18):** Could be vulnerable to known exploits like remote code execution (CVE-2017-3169).

ii. **ETag Information Leak:** Server leaks inode data, enabling fingerprinting and cache poisoning.

iii. **Missing Anti-Clickjacking Header:** Site is vulnerable to clickjacking attacks due to no X-Frame-Options.

iv. **Allowed HTTP Methods (POST, OPTIONS, etc.):** Unnecessary methods could expose server behavior.

v. **Default Apache Page:** Indicates misconfiguration and potential exposure of sensitive files.

12.Probable Exploits

i. **Brute-Force SSH (Port 22):** Tools like Hydra can attempt password cracking.

ii. **Directory Traversal:** Potential directory listing vulnerabilities or misconfigurations on /content.

iii. **Clickjacking Exploit:** Embed site in an iframe to trick users into unauthorized actions.

iv. **Apache Exploits:** Public scripts may exist to exploit Apache 2.4.18 vulnerabilities.

13.Conclusion

The active reconnaissance conducted on LazyAdmin’s network revealed several vulnerabilities, including outdated Apache services, missing security headers, and exposed directories. These vulnerabilities highlighted critical entry points and misconfigurations, which were easily detected using tools like Nmap, Gobuster, and Nikto. This underscores the importance of continuous scanning, timely patching, and implementing advanced security measures to mitigate risks effectively.

This exercise demonstrated a solid understanding of reconnaissance techniques and emphasized the need for dynamic system assessments to strengthen defenses against evolving cyber threats.

14. References

Security advisory (no date) *SolarWinds*. Available at: https://www.solarwinds.com/securityadvisory (Accessed: 12 February 2025).

Detecting supernova malware: Solarwinds continued (no date) *Splunk*. Available at: https://www.splunk.com/en_us/blog/security/detecting-supernova-malware-solarwinds-continued.html (Accessed: 12 February 2025).

JPCERT Coordination Center (no date) *JPCERT/CC*. Available at: https://www.jpcert.or.jp/english/ (Accessed: 12 February 2025).

About JPCERT/cc (no date) *JPCERT/CC*. Available at: https://www.jpcert.or.jp/english/about/ (Accessed: 12 February 2025).

Domain names & identity for everyone (no date) *whois.com*. Available at: https://www.whois.com/ (Accessed: 12 February 2025).

OSINT framework (no date) *OSINT Framework*. Available at: https://osintframework.com/ (Accessed: 12 February 2025).

Cyber security training (no date) *TryHackMe*. Available at: https://tryhackme.com/room/lazyadmin (Accessed: 12 February 2025).

(No date) *Homepage*. Available at: https://www.maltego.com/?utm_source=paterva.com&utm_medium=referral&utm_campaign=301 (Accessed: 12 February 2025).

Computer misuse act 1990 (no date) *Legislation.gov.uk*. Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents/enacted (Accessed: 12 February 2025)