Cyber Security Footprint Report

Prepared by

OLADAPO FAMODU FREDRICK

On June 18, 2025

Executive Summary

This report presents the findings of a cybersecurity footprint analysis conducted on the target domain halisans.com. The analysis aimed to identify potential security risks and vulnerabilities associated with the domain's online presence. Our findings reveal several areas of concern, including exposed WHOIS information, outdated software, and potential vulnerabilities to subdomain takeover. We recommend implementing security measures to mitigate these risks and improve the overall security posture of the domain.

Introduction

The purpose of this report is to provide a comprehensive analysis of the cyber security footprint on the target domain halisans.com. The analysis involved gathering information about the domain's online presence, network infrastructure, and potential vulnerabilities. The findings of this report will help identify areas for improvement and provide recommendations for enhancing the security posture of the domain.

Methodology

The analysis was conducted using a combination of footprinting techniques, including:

1. DNSRECON : DNSRECON was used to gather information about the domain's DNS records, including A records, MX records, and NS records.

2. WHOIS Lookups: WHOIS lookups were used to gather information about the domain's registrant, registrar, and contact details.

3 HOST. the host was used to discover the Halisans.com IP address

4 Ping

5 Dig- Dig was used for querying Domain Name System (DNS) servers. It's essentially an "information groper" for DNS records, allowing users to troubleshoot network issues, check DNS configurations, and analyze domain names key

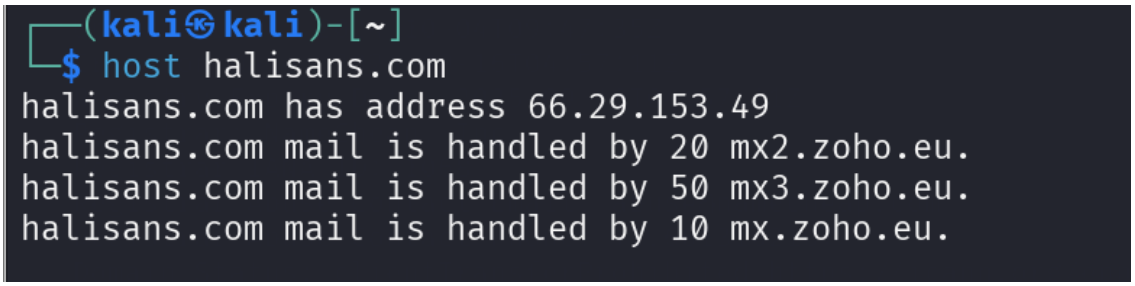
6 Nmap -("Network Mapper") is a free and open -source utility for network discovery and security auditing. Many systems and network administrators also find it useful for task s such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.7 Nmap -

Findings

The analysis revealed the following findings:

1. Domain Information:

- Domain name: (halisans.com)
- Registrar: Domain ID: 2917253114_DOMAIN_COM-VRSN
- Creation date: 2024-09-16T04:57:11Z
- Expiration date 2025-09-16T04:57:11Z Reg



2. WHOIS Information

Whois halisans.com

Domain Name: HALISANS.COM

Registry Domain ID: 2917253114_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.namecheap.com

Registrar URL: http://ww.namecheap.com

Updated Date: 2024-10-04T09:47:35Z

Creation Date: 2024-09-16T04:57:11Z

Registry Expiry Date: 2025-09-16T04:57:11Z

Registrar: NameCheap, Inc.

Registrar IANA ID: 1068

Registrar Abuse Contact Email: abuse@namecheap.cor

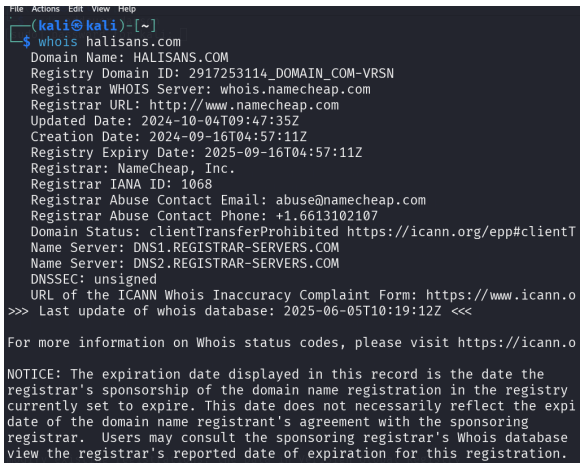
Registrar Abuse Contact Phone: +1.6613102107

Domain Status: clientTransferProhibited https://ic

Name Server: DNS1.REGISTRAR-SERVERS.COM

Name Server: DNS2.REGISTRAR-SERVERS.COM

DNSSEC: unsigned



3. Network Infrastructure:

- Nameservers: DNS1.REGISTRAR-SERVERS.COM
- Mail server: - halisans.com has address 66.29.153.49

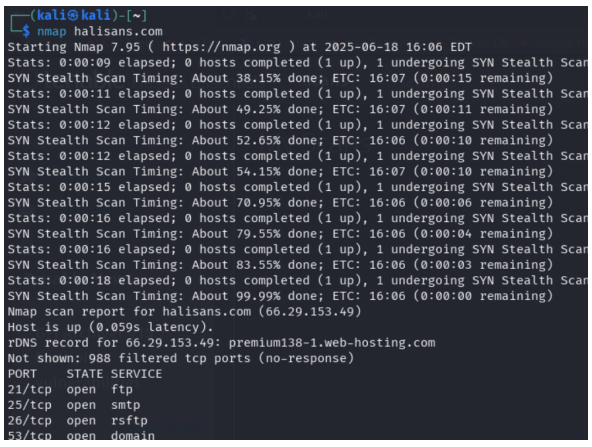
Halisans.com mail is handled by 20 mx2.zoho.eu.

halisans.com mail is handled by 50 mx3.zoho.eu.

halisans.com mail is handled by 10 mx. zoho.eu ache/2.4.7

Starting Nmap 7.95 (https://nmap.org) at 2025-06-05 06:26 EDT

Nmap scan report for halisans.com (66.29.153.49)



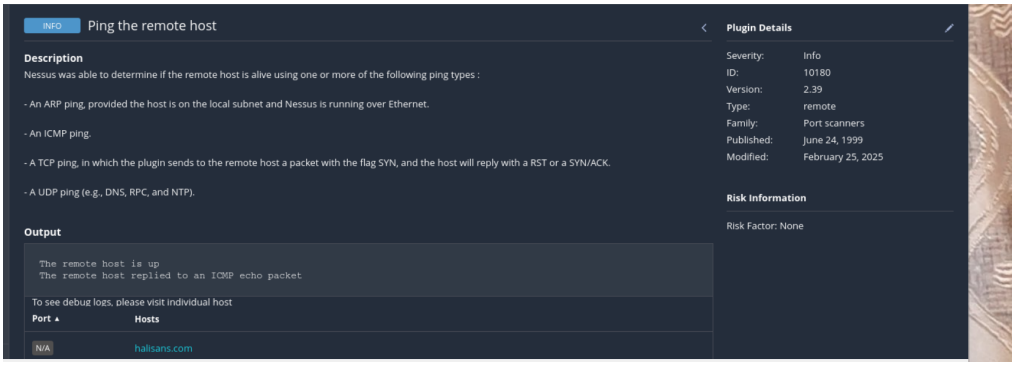
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 21,25,26,52,80,110,143,443,465,587,993,995 halisans.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-18 16:11 EDT
Nmap scan report for halisans.com (66.29.153.49)
Host is up (0.23s latency).
rDNS record for 66.29.153.49: premium138-1.web-hosting.com

PORT    STATE    SERVICE
21/tcp  open     ftp
25/tcp  open     smtp
26/tcp  open     rsftp
52/tcp  filtered xns-time
80/tcp  open     http
110/tcp open     pop3
143/tcp open     imap
443/tcp open     https
465/tcp open     smtps
587/tcp open     submission
993/tcp open     imaps
995/tcp open     pop3s

Nmap done: 1 IP address (1 host up) scanned in 2.95 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p50,21,25,26 --script Vuln halisans.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-18 16:53 EDT
Nmap scan report for halisans.com (66.29.153.49)
Host is up (0.083s latency).
rDNS record for 66.29.153.49: premium138-1.web-hosting.com

PORT   STATE    SERVICE
21/tcp open     ftp
25/tcp open     smtp
26/tcp open     rsftp
50/tcp filtered re-mail-ck

Nmap done: 1 IP address (1 host up) scanned in 164.58 seconds
```

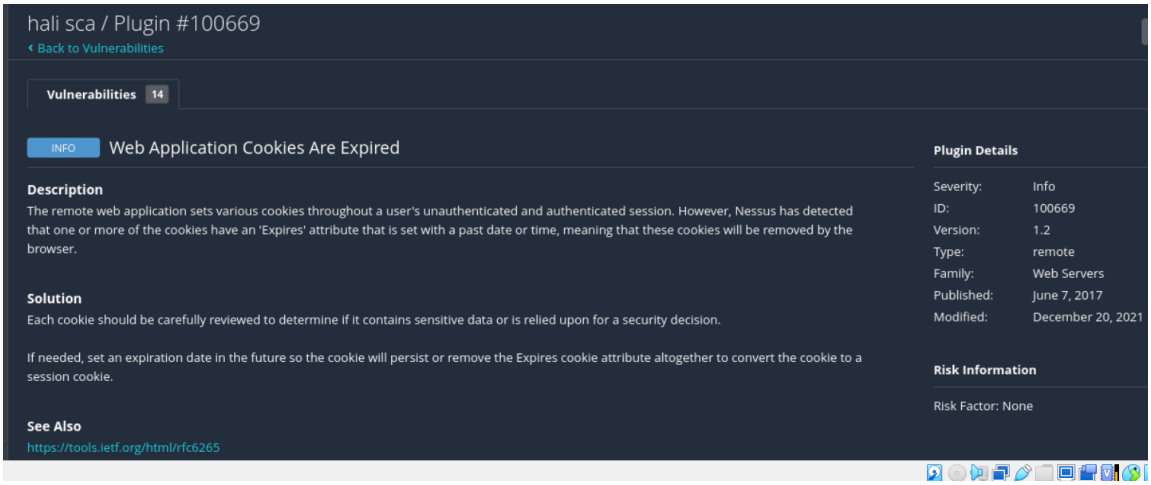
```
┌──(kali㉿kali)-[~]
└─$ nmap -p21 --script Vuln halisans.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-18 16:59 EDT
Nmap scan report for halisans.com (66.29.153.49)
Host is up (0.0023s latency).
rDNS record for 66.29.153.49: premium138-1.web-hosting.com

PORT   STATE    SERVICE
21/tcp filtered ftp

Host script results:
| firewall-bypass:
|_  Firewall vulnerable to bypass through ftp helper. (IPv4)

Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p25 --script Vuln halisans.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-18 17:03 EDT
Nmap scan report for halisans.com (66.29.153.49)
Host is up (0.0020s latency).
rDNS record for 66.29.153.49: premium138-1.web-hosting.com

PORT   STATE    SERVICE
25/tcp filtered smtp

Host script results:
| firewall-bypass:
|_  Firewall vulnerable to bypass through ftp helper. (IPv4)

Nmap done: 1 IP address (1 host up) scanned in 14.48 seconds
```

NESSUS SCAN FOR HALISANS.COM



M



Observations:

-The host appears to be a web server with email services.

-Multiple email-related ports are open, indicating a potential email server.

-The presence of both HTTP and HTTPS suggests a secure connection is available.

.

4. Potential Vulnerabilities:

- Exposed WHOIS information: registrant's contact details are publicly available
- Potential subdomain takeover: (halisans.com) may be vulnerable to takeover

Open ports may be vulnerable to exploitation if not properly secured.

- Outdated software or configurations may lead to security issues.

Recommendations

Based on the findings, we recommend the following:

1. Secure WHOIS information: Consider using a domain privacy service to protect sensitive registrant information.

2. Update software: Update Apache to the latest version to prevent potential vulnerabilities.

3. Monitor subdomains: Regularly monitor subdomains for potential takeover vulnerabilities.

4. Implement security measures: Implement security measures such as firewalls, intrusion detection systems, and encryption to protect the domain's infrastructure.

5- Ensure all services are up-to-date and properly configured.

6- Implement security measures such as firewalls and intrusion detection systems.

7- Regularly monitor and scan for potential vulnerabilities.

Conclusion

The cybersecurity footprint analysis revealed several areas of concern associated with (halisans.com). By implementing the recommended security measures, the domain can reduce its attack surface and improve its overall security posture.