

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 Our findings reveal several areas of concern, including exposed WHOIS information, outdated software, and potential vulnerabilities to subdomain takeover.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

```
(kali㉿kali)-[~]  
$ host halisans.com  
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.
```

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://www.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

```
File Actions Edit View Help
(kali@kali)-[~]
$ whois halisans.com
Domain Name: HALISANS.COM
Registry Domain ID: 2917253114_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.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.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientT
Name Server: DNS1.REGISTRAR-SERVERS.COM
Name Server: DNS2.REGISTRAR-SERVERS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.o
>>> Last update of whois database: 2025-06-05T10:19:12Z <<<

For more information on Whois status codes, please visit https://icann.o

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry
currently set to expire. This date does not necessarily reflect the expi
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database
view the registrar's reported date of expiration for this registration.
```

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 halisans.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-18 16:06 EDT
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 38.15% done; ETC: 16:07 (0:00:15 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.25% done; ETC: 16:07 (0:00:11 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 52.65% done; ETC: 16:06 (0:00:10 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 54.15% done; ETC: 16:07 (0:00:10 remaining)
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 70.95% done; ETC: 16:06 (0:00:06 remaining)
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 79.55% done; ETC: 16:06 (0:00:04 remaining)
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.55% done; ETC: 16:06 (0:00:03 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 16:06 (0:00:00 remaining)
Nmap scan report for halisans.com (66.29.153.49)
Host is up (0.059s latency).
rDNS record for 66.29.153.49: premium138-1.web-hosting.com
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
26/tcp    open  rsftp
53/tcp    open  domain
```

```
(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
```

INFO

Ping the remote host

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Output

The remote host is up
The remote host replied to an ICMP echo packet

To see debug logs, please visit individual host

Port ▲

Hosts

N/A

halisans.com

Ping Details

Severity: Info

ID: 10180

Version: 2.39

Type: remote

Family: Port scanners

Published: June 24, 1999

Modified: February 25, 2025

Risk Information

Risk Factor: None

hali sca / Plugin #100669

[← Back to Vulnerabilities](#)

Vulnerabilities

14

INFO

Web Application Cookies Are Expired

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

See Also

<https://tools.ietf.org/html/rfc6265>

Plugin Details

Severity:	Info
ID:	100669
Version:	1.2
Type:	remote
Family:	Web Servers
Published:	June 7, 2017
Modified:	December 20, 202

Risk Information

Risk Factor: None

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.