

# Active and Passive Reconnaissance Scan Report

## Scan targets:

Domain- Halisans.com (66.29.153.49)

End points I- Window PC:(192.168.1.205)

End point II- Windows server:(192.168.1.201)

Date of recon: 15 Oct 2025

Title: Cybersecurity Analyst

Name: Temitope C Folowosele

**Scope I: halisans.com and Windows Server, Windows PC  
(Passive Reconnaissance).**

**Scope II: halisans.com and Windows Server, Windows PC  
(Active Reconnaissance).**

## Executive Summary

- The target domain serves a public website with recent content.
- This report enumerates: WHOIS/RDAP, authoritative DNS data, HTTPS surface (at a high level), presence of a WAF/CDN (fingerprinted passively) and open-source footprint across common OSINT sources.
- All findings are from passive, active lookups and request fetching public pages. The target domain resolves and serves a public website with recent content.
- Non-intrusive and intrusive scans were performed; all findings are from passive and active tools.
- End-points used for the active and footprint include my Windows PC and Server.
- The authorized website domain for active footprint was Halisans.com.

## Methodology (Passive & Active)

### Tools & Modes

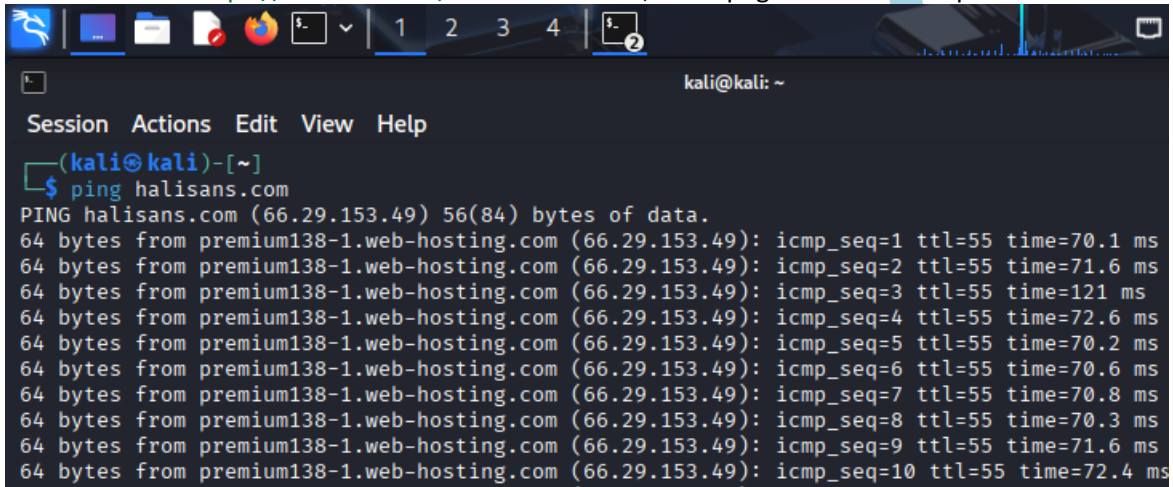
- Nmap: Active footprinting
- **Dig, host, dnsrecon:** Passive DNS lookups (A/AAAA, NS, MX, TXT/SOA/CAA where present) via public resolvers.

- **wafw00f**: Single HTTP(S) request fingerprint (headers/body markers) to infer WAF/CDN; *no evasion, no burst*.
- **SpiderFoot (SF)**: *Passive modules only* (DNS, CT logs, WHOIS, netblocks, leak/site mentions, social).
- **Wapiti**: *Listing only* and passive banner/headers check.
- **OSINT Framework**: As a directory to guide passive pivoting, CT logs, public paste sites, reputation lists, search operators.

## Findings

### 3.1 Public Web Presence (Landing Page)-Domain

- **Site reachable**: <https://halisans.com/> returns content; homepage shows recent posts.



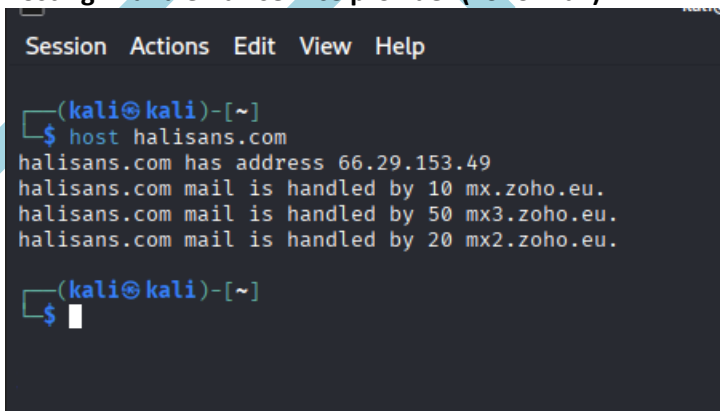
```

kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ ping halisans.com
PING halisans.com (66.29.153.49) 56(84) bytes of data:
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=1 ttl=55 time=70.1 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=2 ttl=55 time=71.6 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=3 ttl=55 time=121 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=4 ttl=55 time=72.6 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=5 ttl=55 time=70.2 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=6 ttl=55 time=70.6 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=7 ttl=55 time=70.8 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=8 ttl=55 time=70.3 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=9 ttl=55 time=71.6 ms
64 bytes from premium138-1.web-hosting.com (66.29.153.49): icmp_seq=10 ttl=55 time=72.4 ms

```

### 3.2 HOST-Domain

- The capture displays the DNS resolution results for halisans.com, revealing both its web hosting IP and email service provider (Zoho Mail).



```

kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ host halisans.com
halisans.com has address 66.29.153.49
halisans.com mail is handled by 10 mx.zoho.eu.
halisans.com mail is handled by 50 mx3.zoho.eu.
halisans.com mail is handled by 20 mx2.zoho.eu.

(kali@kali)-[~]
$

```

- **Name servers**: Capture NS from RDAP and confirm against [dig NS](#).

```

(kali@kali)-[~]
$ dig halisans.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> halisans.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 63379
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;halisans.com.                IN      A
;; ANSWER SECTION:
halisans.com.                1523    IN      A      66.29.153.49

;; Query time: 8 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Wed Oct 15 01:58:40 EDT 2025
;; MSG SIZE rcvd: 57

(kali@kali)-[~]
$

```

○

### 3.6 OSINT: Mentions, Accounts, and Exposure

- SpiderFoot (passive modules):

Spider foot web browser link

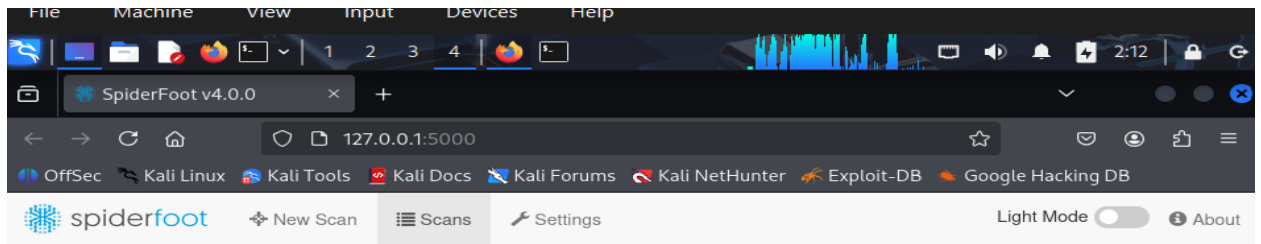
```

(kali@kali)-[~]
$ spiderfoot -l 127.0.0.1:5000
2025-10-15 02:07:25,125 [INFO] sf : Starting web server at 127.0.0.1:5000 ...
2025-10-15 02:07:25,140 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5000/
*****

```

Website landing page

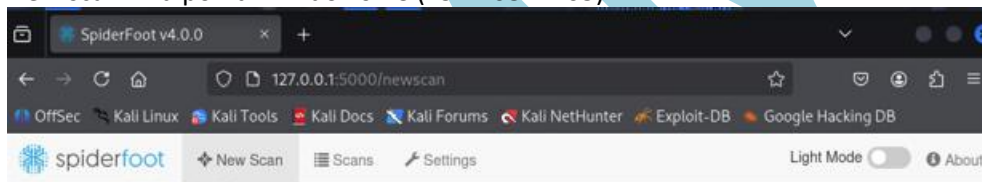


## Scans

No scan history

There is currently no history of previously run scans. Please click 'New Scan' to initiate a new scan.

New scan-End point- Windows PC (192.168.1.205)



**Scan Name**  
Termi Scan

**Scan Target**  
192.168.1.205

**Target Information:**

- Domain Name: e.g. example.com
- IPv4 Address: e.g. 1.2.3.4
- IPv6 Address: e.g. 2606:4700:4700::1111
- Hostname/Sub-domain: e.g. abc.example.com
- Subnet: e.g. 1.2.3.0/24
- Bitcoin Address: e.g. 1HesYJSP1QocyPEjnQ9vzBL1wujruNGe7R
- E-mail address: e.g. bob@example.com
- Phone Number: e.g. +12345678901 (E.164 format)
- Human Name: e.g. "John Smith" (must be in quotes)
- Username: e.g. "jsmith2000" (must be in quotes)
- Network ASN: e.g. 1234

**By Use Case** | By Required Data | By Module

☐ All **Get anything and everything about the target.**  
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

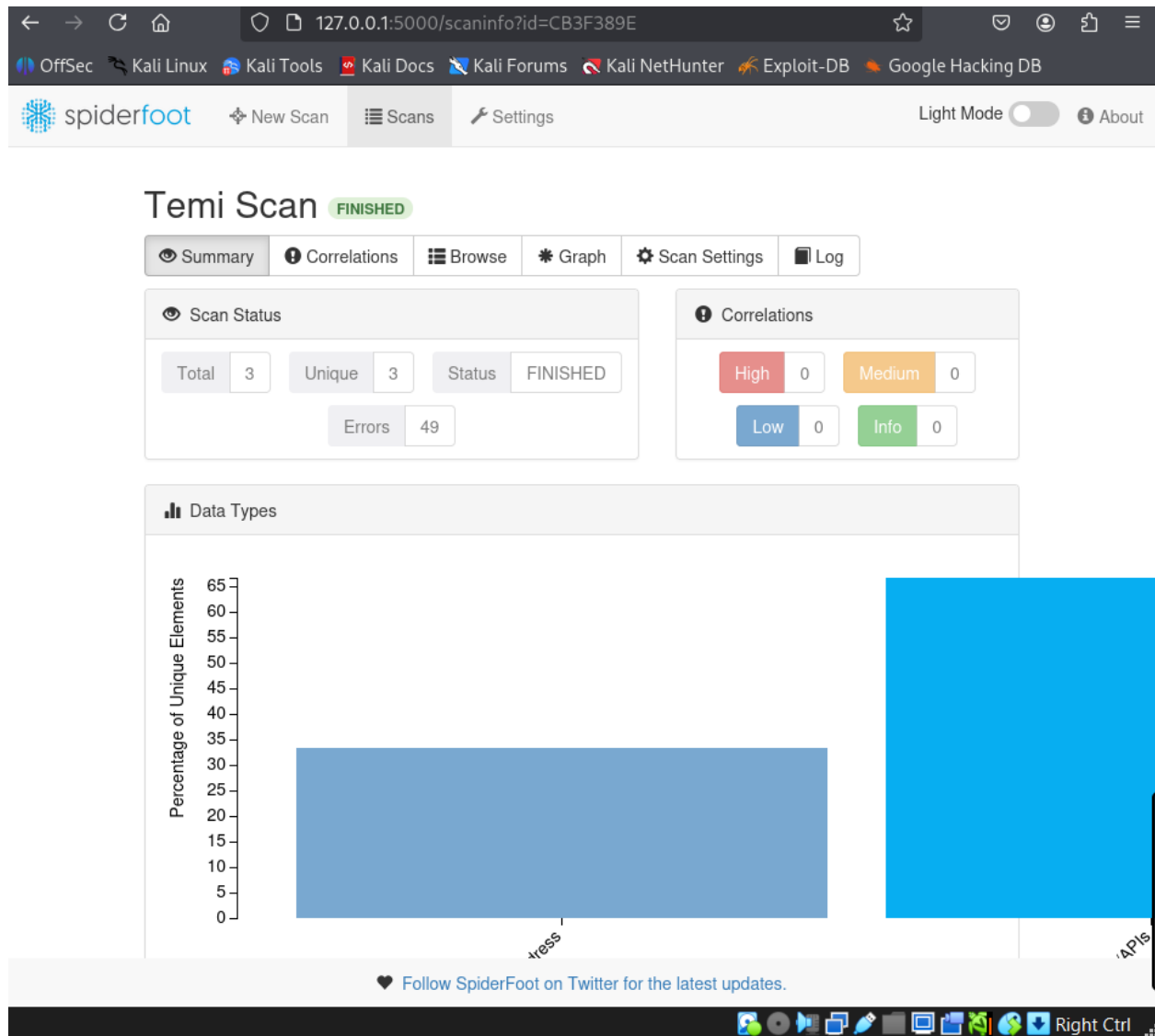
☐ Footprint **Understand what information this target exposes to the Internet.**  
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

☐ Investigate **Best for when you suspect the target to be malicious but need more information.**  
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

☒ Passive **When you don't want the target to even suspect they are being investigated.**

⚡ Want more OSINT automation capabilities? Check out SpiderFoot HX.

- **Endpoint/Hosts:** This captures my new scan result, which is finished, 3 unique elements reported, 49 errors and graphical representation of data types.



Temi Scan FINISHED

- Summary
- Correlations
- Browse
- Graph
- Scan Settings
- Log

Scan Status

Total3

Unique3

StatusFINISHED

Errors49

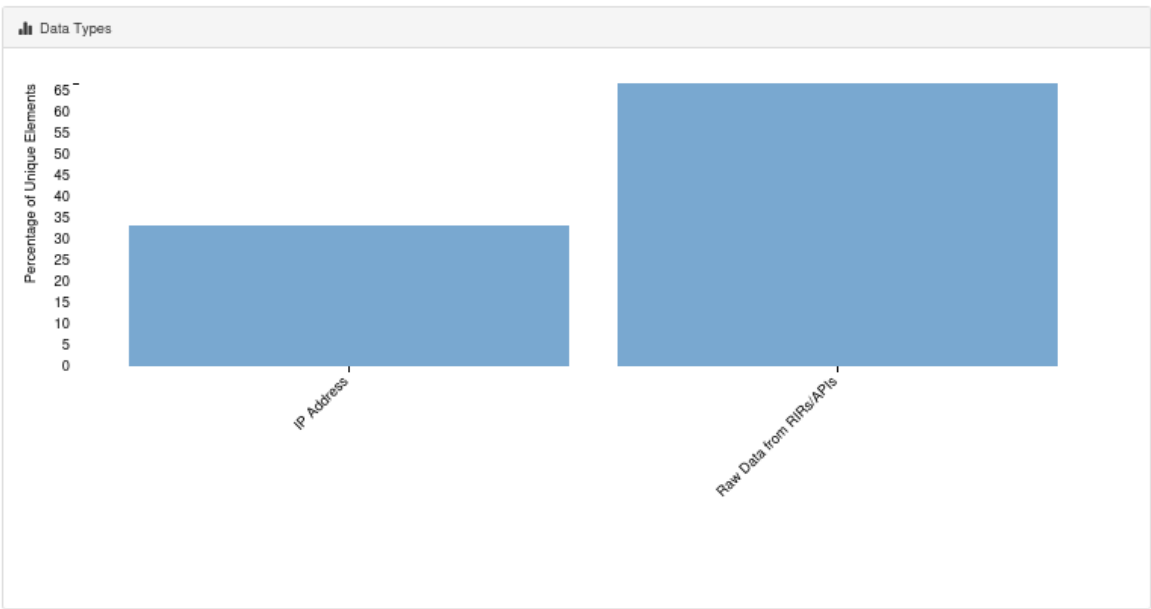
Correlations

High0

Medium0

Low0

Info0



Browse Raw data from RIRs/APIs



Temi Scan FINISHED

Summary

Correlations

Browse

Graph

Scan Settings

Log

Refresh



Search...



Browse / Raw Data from RIRs/APIs

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	<pre>{"status": "ok", "act": [], "acth": [], "pas": [{"o": "apollo.nexus-iservices.com", "t": 1623611920}, {"o": "xn--2qup42anjh2v2a.com", "t": 1482088536}, {"o": "ns.ch-6hosting.co.uk", "t": 1479885510}, {"o": "xn--0ns65uhul47i.com", "t": 1504272322}, {"o": "server-acer.upga.com.tw", "t": 1476082610}, {"o": "hthgouwv.com", "t": 1442708076}, {"o": "moonlight.com", "t": 1529196690}, {"o": "weishantrading.com", "t": 1533361350}, {"o": "omni.pixlinc.com", "t": 1480270748}, {"o": "cookmfc.com", "t": 1441440666}], "pash": [{"o": "mail.toledowebdev.com", "t": 1458971137}, {"o": "dns02.gigmarketing.net", "t": 1503793527}, {"o": "biometrika.sk", "t": 1491298025}, {"o": "mail.marcogagliardi.ch", "t": 1462125111}, {"o": "darkhelios.com", "t": 1532561751}, {"o": "win-ucd4v97lrp0.william123617.com", "t": 1502641233}, {"o": "hthgouwv.com", "t": 1584980260}, {"o": "go1.datagate.co.kr", "t": 1506190101}, {"o": "mail.ez9.ca", "t": 1482630805}, {"o": "moonlight.com", "t": 1623807699}], "asdesc": "UECOMM UeComm Pty Ltd (Australia)"}</pre>	192.16 8.1.2 05	sfp_robtx	2025-10-15 02:20:21
<input type="checkbox"/>	<pre>{'ip': '192.168.1.205', 'ptr_record': None, 'prefixes': [], 'rir_allocation': {'rir_name': None, 'country_code': None, 'ip': '192.168.0.0', 'cidr': '16', 'prefix': '192.168.0.0/16', 'date_allocated': None, 'allocation_status': None}, 'iana_assignment': {'assignment_status': 'legacy', 'description': 'Administered by ARIN', 'whois_server': 'whois.arin.net', 'date_assigned': None, 'maxmind': {'country_code': None, 'city': None}}</pre>	192.16 8.1.2 05	sfp_bgpv iew	2025-10-15 02:20:18

Temi Scan FINISHED

SummaryCorrelationsBrowseGraphScan SettingsLog

RefreshDownload

Search...

Q

Refresh

GridListImage

Browse / IP Address

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	192.168.1.205	192.168.1.205	SpiderFoot UI	2025-10-15 02:20:15

Temi Scan FINISHED

SummaryCorrelationsBrowseGraphScan SettingsLog

Refresh

Meta Information

Name:	Temi Scan
Internal ID:	CB3F389E
Target:	192.168.1.205
Started:	2025-10-15 02:20:02
Completed:	2025-10-15 02:20:43
Status:	FINISHED

Global Settings

Option	Value
Enable debugging?	0
Override the default resolver with another DNS server. For example, 8.8.8.8 is Google's open DNS server.	
Number of seconds before giving up on a HTTP request.	5
List of usernames that if found as usernames or as part of e-mail addresses, should be treated differently to non-generics.	abuse,admin,billing,compliance,devnull,dns,ftp,hostmaster,inoc,ispfeedb ack,isp support,list-request,list,maildaemon,marketing,noc,no-reply,noreply,null,peering,peering-notify,peering-request,phish,phishing,postmaster,privacy,registrar,registry,root,routerouting-registry,rr,sales,security,spam,support,sysadmin,tech,undisclosed-recipients,unsubscribe,usenet,uucp,webmaster,www
List of Internet TLDs.	https://publicsuffix.org/list/effective_tld_names.dat
Hours to cache the Internet TLD list. This can safely be quite a long time given that the list doesn't change too often.	72
Max number of modules to run concurrently	3

♥ Follow SpiderFoot on Twitter for the latest updates.





←

→

↺

🏠

🔒 127.0.0.1:5000/scaninfo?id=CB3F389E

80%

☆

📧

👤

📄

☰

OffSecKali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DB

spiderfoot

New Scan

Scans

Settings

Light Mode

About

Temi Scan

FINISHED

Summary

Correlations

Browse

Graph

Scan Settings

Log

🔄

📄

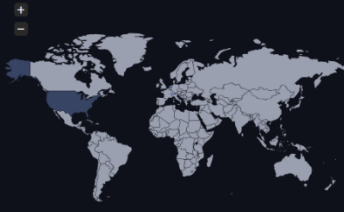
Time	Component	Type	Event
2025-10-15 02:20:43	sflib	STATUS	Running 37 correlation rules.
2025-10-15 02:20:41	sfp_leakix	DEBUG	No information found for host 192.168.1.205
2025-10-15 02:20:41	sfp_leakix	ERROR	Failed to retrieve content from LeakIX
2025-10-15 02:20:40	sflib	ERROR	Failed to connect to https://leakix.net/host/192.168.1.205
2025-10-15 02:20:38	sfp_mnemonic	DEBUG	Record 192.168.1.205 found for 192-168-1-205.522ca470b8544c6f87e71cf71bc12dab.plex.direct is too old, skipping.
2025-10-15 02:20:38	sfp_mnemonic	DEBUG	Record 192.168.1.205 found for 192-168-1-205.1324ca85fbc444c68378cbef7f6e8fd51.plex.direct is too old, skipping.
2025-10-15 02:20:38	sfp_mnemonic	DEBUG	Record 192.168.1.205 found for 192-168-1-205.768aad6e6e2a43c5ade6835045bf70ea.plex.direct is too old, skipping.
2025-10-15 02:20:38	sfp_mnemonic	DEBUG	Record 192.168.1.205 found for 192-168-1-205.89cc47d7c70147d0ab7f70cbbfd7e44.plex.direct is too old, skipping.
2025-10-15 02:20:38	sfp_mnemonic	DEBUG	Record 192.168.1.205 found for 192-168-1-205.6b736a6af22848c6be934684cb4c8ff0.plex.direct is too old, skipping.
2025-10-15 02:20:38	sfp_mnemonic	DEBUG	Record 192.168.1.205 found for 192-168-1-205.a277805d4fa04c5cbb5df03a009f1aab.plex.direct is too old, skipping.
2025-10-15 02:20:38	sfp_mnemonic	DEBUG	Record 192.168.1.205 found for 192-168-1-205.6483586000ff4850acf2327c73b71bda.plex.direct is too old, skipping.

♥

Follow SpiderFoot on Twitter for the latest updates.

OSINT Framework-DNS

System Locations




Hosting / Networks

ZOHO-EU, NL

SECURITYSERVICES

NAMECHEAP-NET

COMPUTERLINE Com



Services / Banners

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
halisans.com	66.29.153.49	ASN: 22612	NAMECHEAP-NET		574
	premium138-1.web-hosting.com	66.29.153.0/24	United States		

MX Records

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
halisans.com	66.29.153.49	ASN: 22612	NAMECHEAP-NET		574
	premium138-1.web-hosting.com	66.29.153.0/24	United States		

MX Records

10 mx.zoho.eu	185.230.214.166	ASN: 205111	ZOHO-EU, NL		
	mx.zoho.eu	185.230.214.0/23	The Netherlands		
50 mx3.zoho.eu	185.230.212.166	ASN: 205111	ZOHO-EU, NL		
	mx3.zoho.eu	185.230.212.0/23	The Netherlands		
20 mx2.zoho.eu	89.36.170.166	ASN: 41913	COMPUTERLINE Computerline, Schlierbach,		
	mx.zoho.eu	89.36.170.0/24	Switzerland, CH		
			Switzerland		

NS Records

dns1.registrar-servers.com	156.154.132.200	ASN: 12008	SECURITYSERVICES		
	dns1.registrar-servers.com	156.154.132.0/24	United States		
dns2.registrar-servers.com	156.154.133.200	ASN: 12008	SECURITYSERVICES		
	dns2.namecheaphosting.com	156.154.133.0/24	United States		

TXT Records

## TXT Records

"v=spf1 include:zohomail.eu ~all"

"zoho-verification=zb01879578.zmverify.zoho.eu"

Download xlsx



## DNS Records

Domain: **halisans.com**.

Added: 2025-01-21

Last updated: 2025-10-09

What points here by: **CNAME / NS / MX / PTR**

View: **SubDomains / Check DNS Propagation / Dig**.

### SOA - (History:2)

2025-06-01 -> 2025-10-09

MName: dns1.registrar-servers.com

Serial: 1728096930

Refresh: 43200

Retry: 3600

Expire: 3601

### NS - (History:4)

2025-06-01 -> 2025-10-09 **dns2.registrar-servers.com**

2025-06-01 -> 2025-10-09 **dns1.registrar-servers.com**

### MX - (History:6)

2025-06-01 -> 2025-10-09 **10** -> **mx.zoho.eu**

2025-06-01 -> 2025-10-09 **20** -> **mx2.zoho.eu**

2025-06-01 -> 2025-10-09 **50** -> **mx3.zoho.eu**

### A - (History:2)

2025-06-01 -> 2025-10-09 **66.29.153.49**

### AAAA

AAAA

## Recommendations (Based on Passive Posture Only)

**HTTP Security Headers:** Verify presence of **Strict-Transport-Security**, **Content-Security-Policy**, **X-Content-Type-Options**, **Referrer-Policy**, and **Permissions-Policy**.

## Active Footprinting- Nmap

End point devices scanned

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ nmap 192.168.1.205  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 23:43 EDT  
Nmap scan report for LivingroomPC (192.168.1.205)  
Host is up (0.0022s latency).  
Not shown: 992 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
554/tcp   open  rtsp  
2869/tcp  open  iclslap  
5357/tcp  open  wsdapi  
10243/tcp open  unknown  
49155/tcp open  unknown  
MAC Address: 08:00:27:00:0D:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 4.68 seconds  
(kali@kali)-[~]  
$
```

This captures all the scan report for my endpoint device: the open ports, state, service, MAC Address, time the scan ended and Port 135 scanned only.

```
(kali㉿kali)-[~]
$ nmap 192.168.1.205
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 00:38 EDT
Nmap scan report for LivingroomPC (192.168.1.205)
Host is up (0.0024s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsdapi
10243/tcp  open  unknown
49155/tcp  open  unknown
MAC Address: 08:00:27:00:0D:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 12.23 seconds

(kali㉿kali)-[~]
$ nmap -p135 192.168.1.205
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 00:40 EDT
Nmap scan report for LivingroomPC (192.168.1.205)
Host is up (0.0011s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
MAC Address: 08:00:27:00:0D:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

(kali㉿kali)-[~]
$
```

List to contain all the ports.

```
(kali㉿kali)-[~]
$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

(kali㉿kali)-[~]
$
```

## Aggressive scan for more comprehensive and detailed data of the device (Window PC)

```
(kali㉿kali)-[~]
$ nmap -p139 -A 192.168.1.205
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 00:52 EDT
Nmap scan report for LivingroomPC (192.168.1.205)
Host is up (0.0014s latency).

PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Windows 8.1 Pro 9600 netbios-ssn
MAC Address: 08:00:27:00:0D:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 8.1 Pro 9600 (Windows 8.1 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_8.1::-
|   Computer name: LivingroomPC
|   NetBIOS computer name: LIVINGROOMPC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-10-15T07:41:50-07:00
|_ nbstat: NetBIOS name: LIVINGROOMPC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:00:0d:a4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
|_ smb2-time:
|   date: 2025-10-15T07:41:50
|_  start_date: 2025-10-15T06:00:22
|_ smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 5h08m45s, deviation: 4h02m29s, median: 2h48m45s
|_ smb2-security-mode:
|   3.0:2:
|_   Message signing enabled but not required

TRACEROUTE
HOP RTT      ADDRESS
1   1.37 ms  LivingroomPC (192.168.1.205)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.53 seconds
```

## Service version of the endpoint scanned.

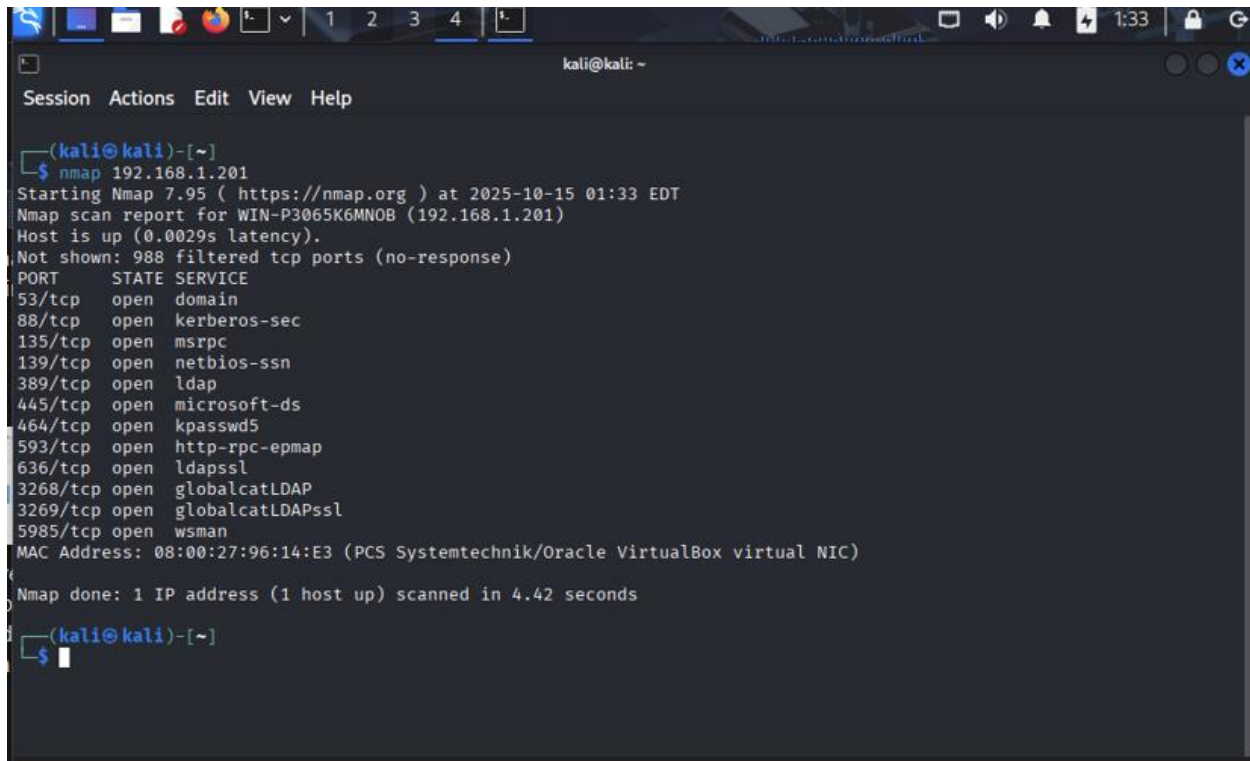
```
(kali㉿kali)-[~]
$ nmap -p139 -sV 192.168.1.205
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 00:59 EDT
Nmap scan report for LivingroomPC (192.168.1.205)
Host is up (0.0018s latency).

PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
MAC Address: 08:00:27:00:0D:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.27 seconds

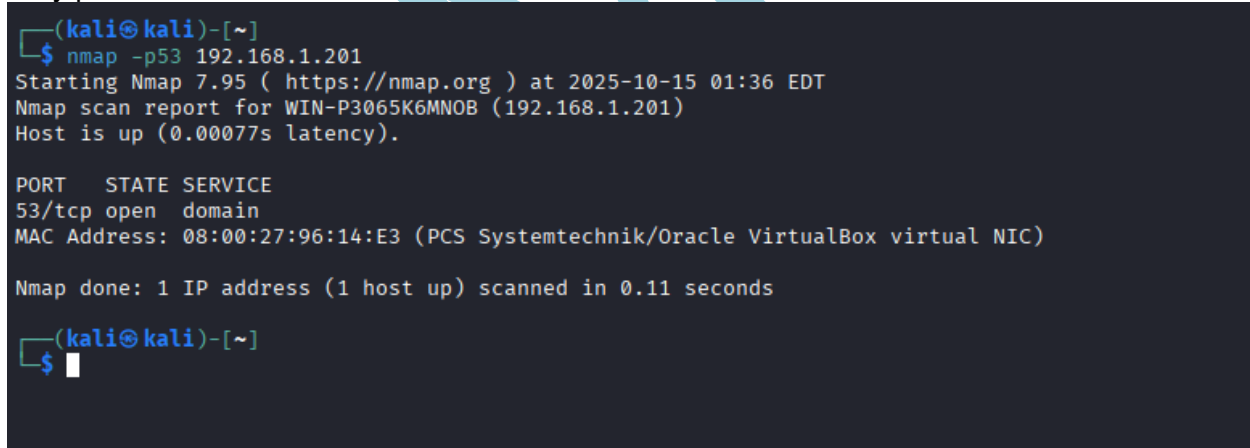
(kali㉿kali)-[~]
$
```

Second endpoint device. (Windows Server)



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ nmap 192.168.1.201  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 01:33 EDT  
Nmap scan report for WIN-P3065K6MNOB (192.168.1.201)  
Host is up (0.0029s latency).  
Not shown: 988 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
53/tcp    open  domain  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
5985/tcp  open  wsman  
MAC Address: 08:00:27:96:14:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 4.42 seconds  
(kali@kali)-[~]  
$
```

Only port 53 scanned



```
(kali@kali)-[~]  
$ nmap -p53 192.168.1.201  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 01:36 EDT  
Nmap scan report for WIN-P3065K6MNOB (192.168.1.201)  
Host is up (0.00077s latency).  
  
PORT      STATE SERVICE  
53/tcp    open  domain  
MAC Address: 08:00:27:96:14:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds  
(kali@kali)-[~]  
$
```

Aggressive scan: comprehensive data



```

(kali㉿kali)-[~]
$ nmap -p88 -A 192.168.1.201
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 01:41 EDT
Nmap scan report for WIN-P3065K6MNOB (192.168.1.201)
Host is up (0.0018s latency).

PORT      STATE SERVICE      VERSION
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-09-22 07:13:05Z)
MAC Address: 08:00:27:96:14:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows 11 21H2 (91%), Microsoft Windows Server 2016 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT      ADDRESS
1   1.78 ms  WIN-P3065K6MNOB (192.168.1.201)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.53 seconds

(kali㉿kali)-[~]
$

```

## Service version

```

(kali㉿kali)-[~]
$ nmap -p88 -sV 192.168.1.201
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 01:49 EDT
Nmap scan report for WIN-P3065K6MNOB (192.168.1.201)
Host is up (0.00073s latency).

PORT      STATE SERVICE      VERSION
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-09-22 07:21:21Z)
MAC Address: 08:00:27:96:14:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.27 seconds

(kali㉿kali)-[~]
$

```

## Aggressive scan for Domain

```

(kali@kali)-[~]
$ nmap halisans.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 23:47 EDT
Nmap scan report for halisans.com (66.29.153.49)
Host is up (0.071s latency).
rDNS record for 66.29.153.49: premium138-1.web-hosting.com
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
25/tcp    open  smtp
26/tcp    open  rsftp
53/tcp    open  domain
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 4.99 seconds

```

```

(kali@kali)-[~]
$

```

Only 21 port scanned

```

(kali@kali)-[~]
$ nmap -p21 halisans.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 23:56 EDT
Nmap scan report for halisans.com (66.29.153.49)
Host is up (0.070s latency).
rDNS record for 66.29.153.49: premium138-1.web-hosting.com

PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

(kali@kali)-[~]
$

```

Port 25, 53, 143 scanned.

```
(kali㉿kali)-[~]  
$ nmap -p25,53,143 halisans.com  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 00:01 EDT  
Nmap scan report for halisans.com (66.29.153.49)  
Host is up (0.072s latency).  
rDNS record for 66.29.153.49: premium138-1.web-hosting.com  
  
PORT      STATE SERVICE  
25/tcp    open  smtp  
53/tcp    open  domain  
143/tcp   open  imap  
  
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds  
  
(kali㉿kali)-[~]  
$
```

Ls to contain all the ports created

```
map done: 1 IP address (1 host up) scanned in 0.25 seconds  
  
(kali㉿kali)-[~]  
$ ls  
desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  
  
(kali㉿kali)-[~]  
$
```

## Aggressive scan run (Domain)

```
(kali@kali)-[~]
$ nmap -p21 -A halisans.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 00:17 EDT
Nmap scan report for halisans.com (66.29.153.49)
Host is up (0.072s latency).
rDNS record for 66.29.153.49: premium138-1.web-hosting.com

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPD
| ssl-cert: Subject: commonName=*.web-hosting.com
| Subject Alternative Name: DNS:*.web-hosting.com, DNS:web-hosting.com
| Not valid before: 2025-03-13T00:00:00
|_ Not valid after: 2026-04-05T23:59:59
|_ ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:4
Aggressive OS guesses: Linux 3.10 (87%), Linux 3.10 - 3.16 (87%), Linux 3.10 - 4.11 (85%), Linux 3.11 - 4.9 (85%),
Linux 3.2 - 4.14 (85%), Linux 4.15 (85%), Linux 4.19 - 5.15 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   2.88 ms  G3100.mynetworksettings.com (192.168.1.1)
2   3.09 ms  lo0-100.BLTMMO-VFTTP-316.verizon-gni.net (71.245.162.1)
3   6.66 ms  ae1316-20.BLTMMOCH-MSE01-AA-IE1.verizon-gni.net (100.41.128.16)
4   ...
5   9.73 ms  verizonwireless-gw.customer.alter.net (63.65.77.26)
6  11.64 ms  rest-bb1-link.ip.twelve99.net (62.115.121.156)
7  10.06 ms  ash-b2-link.ip.twelve99.net (62.115.138.190)
8  14.59 ms  imperva-ic-377610.ip.twelve99-cust.net (62.115.55.139)
9   ... 10
11 72.01 ms  199.193.7.170
12 ... 13
14 70.79 ms  premium138-1.web-hosting.com (66.29.153.49)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.94 seconds

(kali@kali)-[~]
$
```

## Service version scanned

```
(kali@kali)-[~]
$ nmap -p21 -sV halisans.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 00:27 EDT
Nmap scan report for halisans.com (66.29.153.49)
Host is up (0.076s latency).
rDNS record for 66.29.153.49: premium138-1.web-hosting.com

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPD

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
```

## Recommendation

**Security Policy:** Decommissioning EOL operating system, SMB signing is required- secure feature for file transfer, old and insecure protocols NetBIOS, FTP must be disabled, newest SSL/TLS are required for all public facing services.