



Network Discovery & Security Report

Company Name: GT50 Srl

Date: 01/09/2026 16:09

Prepared by: DeepScan v2.0.1

Table of Contents

1. Executive Summary	2
2. Compliance Report	4
2.1 Recommended remediations for NOT COMPLIANT items	4
3. Technical Discovery Report	5
3.1 Summary by IP Address	5
3.2 Summary by Open Port	5
4. FingerPrintX Analysis	7
5. ZGrab2 Analysis	12
6. TLSX Analysis	13

1. Executive Summary

This section provides a high-level overview of the network discovery results, highlighting key findings and potential risks.

Target audience: CIO, CTO, CISO, top management

Purpose: High-level overview, risks, trends, compliance.

Network scan ID: 20260901155832

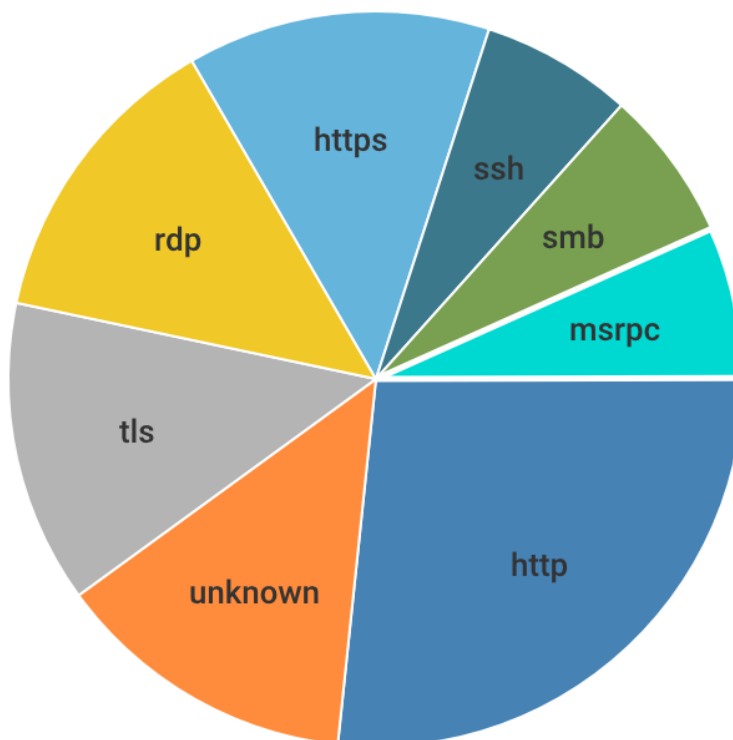
Key Metrics:

Total Active IPs

4

Most Common Service

http, unknown, https, tls, msrpc, smb, rdp, ssh





Network Discovery & Security Report

Protocol	Count
http	4
https	2
msrpc	1
rdp	2
smb	1
ssh	1
tls	2
unknown	2

2. Compliance Report

PARTIAL COMPLIANCE: The verification has identified a heterogeneous configuration. While some services are already protected by Post-Quantum Cryptography (PQC) standards, others are still using legacy cryptographic suites. To ensure uniform long-term security, it is recommended to upgrade the remaining non-compliant services to quantum-resistant configurations.

Detailed Compliance Table:

Hostname / IP	Port	Service	PQC Status
myfastgate.nexxt 192.168.1.254	443	https	NOT COMPLIANT
unknown 192.168.1.50	8443	https	NOT COMPLIANT
server 192.168.1.58	22	ssh	NOT COMPLIANT

2.1 Recommended remediations for NOT COMPLIANT items

Hostname / IP	Port	Service	Note	External Link
server 192.168.1.58	22	ssh	Detected version 8.9 is below required 9.0 for PQC support	Open Link

3. Technical Discovery Report

Detailed mapping of active services on all detected IP addresses within the subnet.

3.1 Summary by IP Address

IP Address	Port	Protocol
192.168.1.50	8008	http
192.168.1.50	8009	unknown
192.168.1.50	8443	https
192.168.1.50	9000	tls
192.168.1.50	10001	tls
192.168.1.55	135	msrpc
192.168.1.55	139	unknown
192.168.1.55	445	smb
192.168.1.55	3389	rdp
192.168.1.55	3389	rdp
192.168.1.58	22	ssh
192.168.1.58	80	http
192.168.1.254	80	http
192.168.1.254	443	https
192.168.1.254	8080	http

3.2 Summary by Open Port

Port	Identified IP Addresses
22	192.168.1.58
80	192.168.1.58, 192.168.1.254
135	192.168.1.55
139	192.168.1.55
443	192.168.1.254
445	192.168.1.55



Network Discovery & Security Report

Port	Identified IP Addresses
3389	192.168.1.55, 192.168.1.55
8008	192.168.1.50
8009	192.168.1.50
8080	192.168.1.254
8443	192.168.1.50
9000	192.168.1.50
10001	192.168.1.50

4. FingerPrintX Analysis

Field	Value
ip	192.168.1.254
port	80
protocol	http
response_headers.Expires.0	0
response_headers.Server.0	
response_headers.Content-Type.0	text/html
response_headers.X-Content-Type-Options.0	nosniff
response_headers.X-Xss-Protection.0	1; mode=block
response_headers.Cache-Control.0	no-cache,no-store,max-age=0
status	200 Ok
status_code	200
response_headers.Date.0	Tue, 01 Sep 2026 16:09:23 GMT
response_headers.Content-Language.0	en
response_headers.Content-Length.0	190
response_headers.Prama.0	no-cache
response_headers.X-Frame-Options.0	DENY
response_headers.Content-Security-Policy.0	default-src 'self' 'unsafe-inline' 'unsafe-eval' api-cdn.amazon.com na.account.amazon.com

Field	Value
ip	192.168.1.254
port	443
protocol	https
response_headers.X-Xss-Protection.0	1; mode=block
response_headers.Content-Type.0	text/html
title	302 Found
response_headers.Content-Language.0	en
response_headers.Date.0	Tue, 01 Sep 2026 16:09:20 GMT
response_headers.Prama.0	no-cache

Field	Value
response_headers.Content-Security-Policy.0	default-src 'self' 'unsafe-inline' 'unsafe-eval' api-cdn.amazon.com na.account.amazon.com
response_headers.Location.0	/login.html
response_headers.Server.0	
response_headers.X-Content-Type-Options.0	nosniff
status_code	302
response_headers.Expires.0	0
response_headers.Cache-Control.0	no-cache,no-store,max-age=0
response_headers.X-Frame-Options.0	DENY
status	302 Found

Field	Value
ip	192.168.1.254
port	8080
protocol	http
response_headers.Content-Type.0	application/json
response_headers.Server.0	Boost.Beast/347
status	404 Not Found
status_code	404
response_headers.Content-Length.0	27

Field	Value
ip	192.168.1.50
port	8008
protocol	http
response_headers.Content-Length.0	0
response_headers.Content-Type.0	text/html
status	404 Not Found
status_code	404

Field	Value
ip	192.168.1.50
port	8443
protocol	https
status	404 Not Found
status_code	404
response_headers.Content-Length.0	0
response_headers.Content-Type.0	text/html

Field	Value
ip	192.168.1.55
port	135
protocol	msrpc

Field	Value
ip	192.168.1.55
port	445
protocol	smb
dns_domain_name	TEST
os_version	10.0.26100
dns_computer_name	TEST
netbios_computer_name	TEST
netbios_domain_name	TEST
signing_enabled	true
signing_required	false

Field	Value
ip	192.168.1.55
port	3389
protocol	rdp

Field	Value
ip	192.168.1.55
port	3389
protocol	rdp

Field	Value
ip	192.168.1.58
port	22
protocol	ssh

algo	map[CiphersClientServer:chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com CiphersServerClient:chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com CompressionClientServer:none,zlib@openssh.com CompressionServerClient:none,zlib@openssh.com Cookie:ce24f51117f5f0e816060f80b98e8eec KexAlgos:curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,sntrup761x25519-sha512@openssh.com,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,kex-strict-s-v00@openssh.com LanguagesClientServer: LanguagesServerClient: MACsClientServer:umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 MACsServerClient:umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 ServerHostKeyAlgos:rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519]
banner	SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.16
password_auth_enabled	false

Field	Value
ip	192.168.1.58
port	80
protocol	http
status_code	302
response_headers.Content-Length.0	0
response_headers.Referrer-Policy.0	no-referrer
status	302 Found
response_headers.X-Frame-Options.0	SAMEORIGIN
response_headers.X-Content-Type-Options.0	nosniff
response_headers.Cross-Origin-Embedder-Policy.0	require-corp
response_headers.Cross-Origin-Opener-Policy.0	same-origin
response_headers.X-Permitted-Cross-Domain-Policies.0	none
response_headers.X-Xss-Protection.0	0
response_headers.X-Dns-Prefetch-Control.0	off
response_headers.Cross-Origin-Resource-Policy.0	same-origin
response_headers.Date.0	Tue, 01 Sep 2026 16:04:18 GMT
response_headers.Location.0	/login
response_headers.X-Download-Options.0	noopen
response_headers.Origin-Agent-Cluster.0	?1

5. ZGrab2 Analysis

Field	Value
ip	192.168.1.254
port	443
protocol_service	
protocol	https

Field	Value
ip	192.168.1.50
port	8443
protocol_service	
protocol	https

Field	Value
ip	192.168.1.58
port	22
protocol_service	
protocol	ssh

6. TLSX Analysis

Field	Value
port	443
protocol	https
self-signed	true
timestamp	2026-09-01T16:09:22Z
tls-version	tls13
cipher	TLS_AES_256_GCM_SHA384
ip	192.168.1.254
key-exchange	X25519

Field	Value
tls-version	tls12
cipher	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ip	192.168.1.50
key-exchange	X25519
port	8443
protocol	https
self-signed	true
timestamp	2026-09-01T16:00:14Z