

ATTACK SURFACE MONITORING (VULNERABILITY ASSESSMENT)

UBONGABASI ETIM

Group members: Hannah Ekpo, Dorcas Oyaniyi, Oyeniyi Oluwatayo James

Chosen assets: www.db.com, campaignmonitor.com, captainfact.io, www.chain.link, www.clario.io

Assets in (this) document(in order): www.db.com, www.clario.io

1. According to **Gartner**, the top three vulnerability management platforms today include:
 - a. Insight VM (by Rapid7) with a total 4.3 star rating from 719 ratings of which 45% were 5 stars.
 - b. Tenable Nessus by Tenable with a 4.6 star overall rating from 603 ratings of which 53% were 5 stars.
 - c. Qualys VDMR by Qualys with a 4.4 star rating from 517 ratings of which 46% were 5 stars.
2. According to **IDC (International Data Corporation)**:
The top three Vulnerability management platforms according to market share are:
 - a. Tenable with 20% (\$678.1 million and 13.6% yoy growth)
 - b. Qualys with 18% (\$442.4 million and 3.6% yoy growth)
 - c. Rapid7 with 13.7% (\$321.2 million and 9.9 yoy growth)
3. According to **Forrester**, based on reports from Q3 of 2023, the top three vulnerability management platforms are:
 - a. Tenable
 - b. Rapid7
 - c. Qualys

Scan Results

May 15, 2025

This report was generated with an evaluation version of Qualys

Report Summary	
User Name:	Chikodili Udeh
Login Name:	magne1cu
Company:	Magnetic Oak
User Role:	Manager
Address:	5, Oakmere Street, Belmont Business Park,
City:	Durham
Zip:	DH1 1TW
Country:	United Kingdom
Created:	05/15/2025 at 12:30:38 PM (GMT+0100)
Launch Date:	05/15/2025 at 11:44:25 AM (GMT+0100)
Active Hosts:	12
Total Hosts:	13
Type:	On demand
Status:	Finished
Reference:	scan/1747305865.63394
External Scanners:	151.104.34.6 (Scanner 14.7.19-1, Vulnerability Signatures 2.6.325-3)
Duration:	00:41:06
Title:	group1 clario scan
Network:	Global Default Network
Asset Groups:	group1 clario ip assetg
IPs:	3.95.93.236, 3.221.200.183, 18.244.140.107, 18.244.140.124, 18.244.164.4, 18.244.164.8, 18.244.164.16, 18.244.164.82, 54.87.125.48, 95.100.153.186, 104.77.161.88, 148.163.157.10, 160.83.59.102
Excluded IPs:	-
FQDNs:	-
Options Profile:	Qualys Recommended Option Profile

Summary of Vulnerabilities

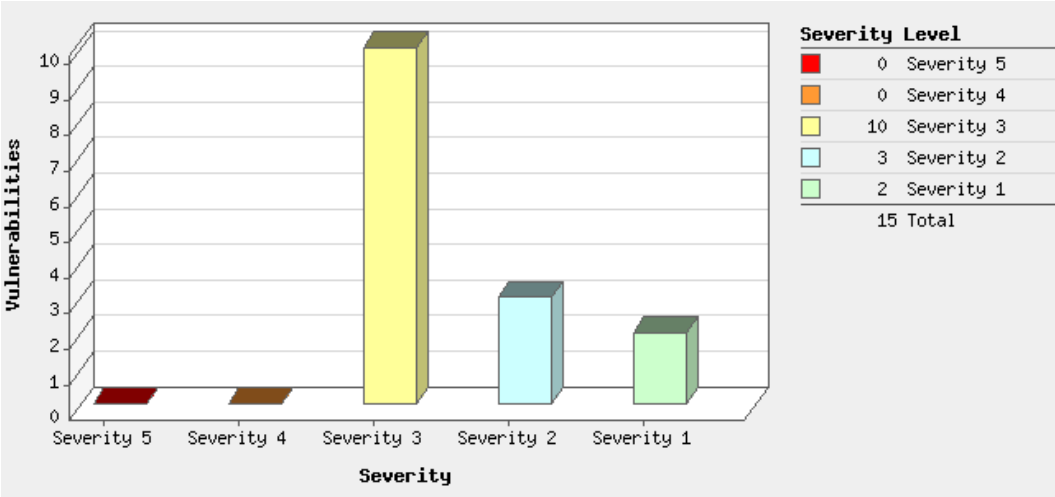
Vulnerabilities Total	313	Security Risk (Avg)	<div><div></div><div></div><div></div><div></div><div></div></div>	1.5
-----------------------	-----	---------------------	--	-----

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	10	3	2	15
2	3	0	35	38
1	2	2	256	260
Total	15	5	293	313

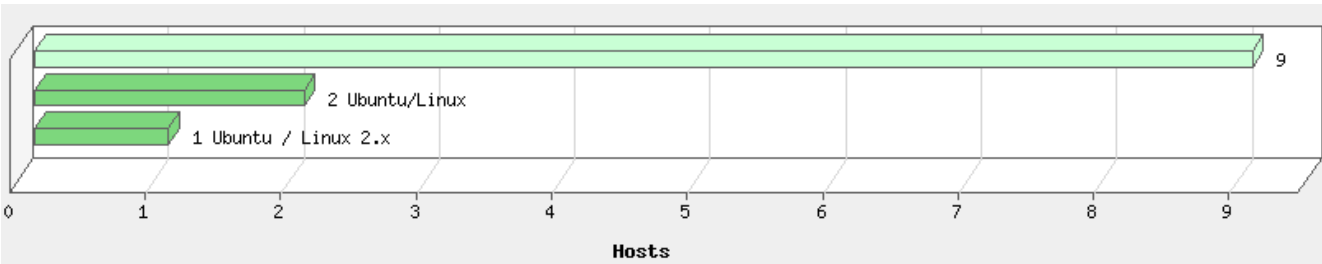
5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	136	136
TCP/IP	2	3	53	58
General remote services	13	2	38	53

Category	Confirmed	Potential	Information Gathered	Total
CGI	0	0	42	42
Firewall	0	0	11	11
Total	15	5	280	300

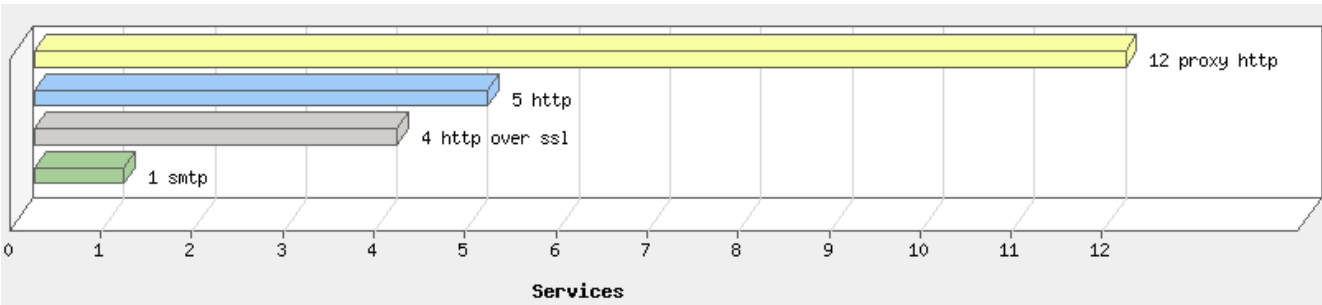
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

Scan Results

May 14, 2025

This report was generated with an evaluation version of Qualys

Report Summary	
User Name:	Chikodili Udeh
Login Name:	magne1cu
Company:	Magnetic Oak
User Role:	Manager
Address:	5, Oakmere Street, Belmont Business Park,
City:	Durham
Zip:	DH1 1TW
Country:	United Kingdom
Created:	05/14/2025 at 09:59:10 PM (GMT+0100)
Launch Date:	05/14/2025 at 09:05:34 PM (GMT+0100)
Active Hosts:	7
Total Hosts:	10
Type:	On demand
Status:	Finished
Reference:	scan/1747253134.61529
External Scanners:	151.104.34.102 (Scanner 14.6.13-1, Vulnerability Signatures 2.6.325-3)
Duration:	00:38:25
Title:	group1 deustche scan
Network:	Global Default Network
Asset Groups:	group1 deustche ip assestg
IPs:	3.84.166.34, 54.82.173.102, 66.77.1.199, 95.100.153.186, 104.77.161.88, 104.77.161.93, 104.77.161.95, 160.83.59.102, 160.83.59.112, 160.83.59.140
Excluded IPs:	-
FQDNs:	-
Options Profile:	Qualys Recommended Option Profile

Summary of Vulnerabilities

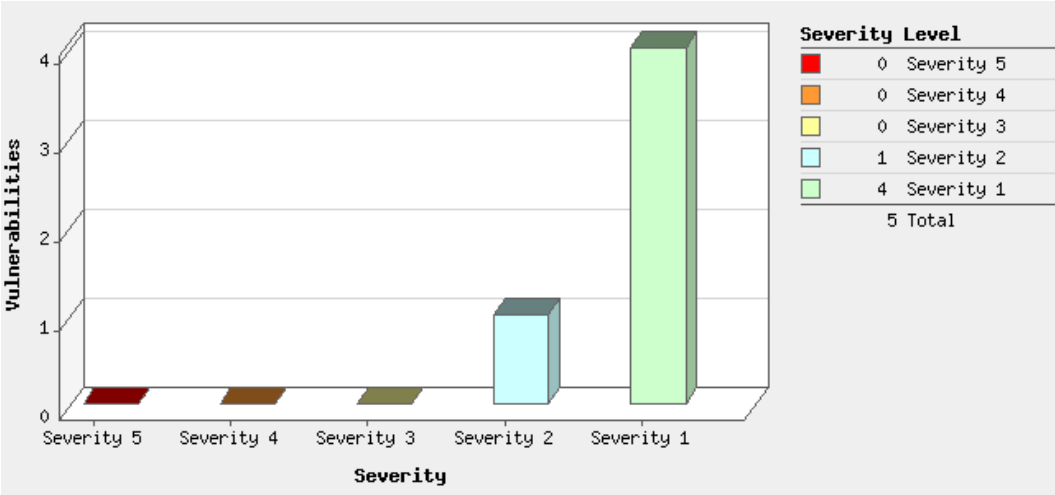
Vulnerabilities Total	174	Security Risk (Avg)	<div><div></div><div></div><div></div><div></div><div></div></div>	2.1
-----------------------	-----	---------------------	--	-----

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	5	5	10
2	1	0	20	21
1	4	4	135	143
Total	5	9	160	174

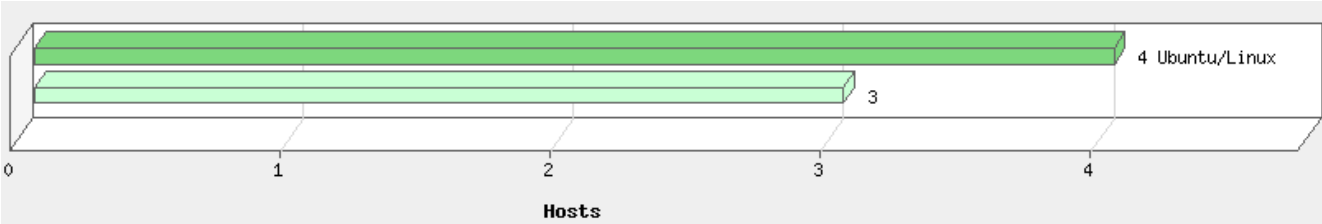
5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	75	75
TCP/IP	4	5	36	45
General remote services	0	4	14	18
CGI	1	0	14	15

Category	Confirmed	Potential	Information Gathered	Total
Web server	0	0	10	10
Total	5	9	149	163

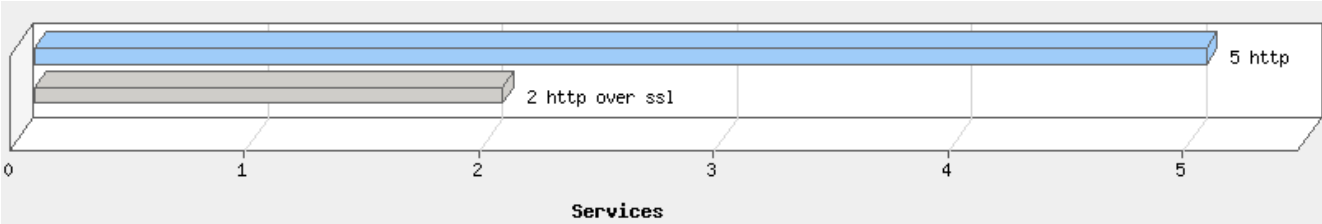
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

3.84.166.34 (ec2-3-84-166-34.compute-1.amazonaws.com, -)
Global Default Network

Information Gathered (28)

- 2 Host Uptime Based on TCP TimeStamp Option
- QID: 82063
- Category: TCP/IP
- Associated CVEs: -