VULNERABILITY ASSSSMENT REPORT

ABC CORPORATION
29TH MAY, 2023

Santa Clara,Ca
Technology,
5,5000 Employees

Report details

Title	ABC VULNERABILITY ASSESSMENT
Version	V1.0
Author	S.Afrin
Tester(s)	
Classification	Confidential

Recipient

Name	Title	Company
Afrin	ABC VULNERABILITY ASSESSMENT	ABC CORPORATION

Version Control

Version	Date	Author	Description
V1.0	29th Jue	AFRIN	

Table of Contents:

Executive Summary

Security and Thread Prevention

IPS attacks detected: 1,592

Malware & botnet events detected: 73

High risk applications detected: 296

Last year, over 780 enterprises were breached as a result of poor internal security practices and latent vendor content security. The average cost of a corporate security breach is estimated at $3.5 million USD and is rising at 15% year over year. Intrusions, malware/botnets and malicious applications collectively comprise a massive risk to your enterprise network. These attack mechanisms can give attackers access to your most sensitive files and database information. Forti Guard Labs mitigates these risks by providing award-winning content security and is consistently rated among industry leaders by objective third parties such as NSS Labs, VB 100 and AV Comparatives.

User Productivity

Application Categories: Network.Service / Video/Audio / Web.Others

Top 3 Web Categories: Shopping and Auction / Streaming Media and Download / Web-based Email

Top 3 Web Domains: mail.google.com / stream.pandora.com / en.wikipedia.org

User application usage and browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate a lack of proper enforcement of corporate usage policies. Most enterprises recognize that personal use of corporate resources is acceptable. But there are many grey areas that businesses must keep a close eye on including: use of proxy avoidance/peer to peer applications, inappropriate web browsing, phishing websites, and potentially illegal activity. All of which expose the company to undue liability and potential damages. With over 5,800 application control rules and 250 million categorized websites, FortiGuard Labs provides telemetry that FortiOS uses to keep your business running effectively.

Network Utilization

Top Hosts/Clients by Bandwidth: 8.1.0.215 / 10.1.82.175 / 8.1.0.222

Average Throughput: 28 Mbps

Unique Hosts Detected: 664

Performance effectiveness is an often undervalued aspect of security devices, but firewalls must keep up with the line speeds that today's next generation switches operate at. A recent survey by Infonetics indicates that 77% of decision-makers at large organizations feel that they must upgrade their network security performance (100+ Gbps aggregate throughput) in the coming year. FortiGates leverage FortiASICs to accelerate CPU intensive functions such as packet forwarding and pattern matching.This offloading typically results in a 5-10X performance increase when measured against competitive solutions.

1.1. Scope Purpose and Duration of Work

The ABC system of cost accounting is based on activities, which are any events, units of work, or tasks with a specific goal, such as setting up machines for production, designing products, distributing finished goods, or operating machines. Activities consume overhead resources and are considered cost objects.

Under the ABC system, an activity can also be considered as any transaction or event that is a cost driver. A cost driver, also known as an activity driver, is used to refer to an allocation base. Examples of cost drivers include machine setups, maintenance requests, consumed power, purchase orders, quality inspections, or production orders.

There are two categories of activity measures: transaction drivers, which involves counting how many times an activity occurs, and duration drivers, which measure how long an activity takes to complete.

Unlike traditional cost measurement systems that depend on volume count, such as machine hours and/or direct labor hours to allocate indirect or overhead costs to products, the ABC system classifies five broad levels of activity that are, to a certain extent, unrelated to how many units are produced. These levels include batch-level activity, unit-level activity, customer-level activity, organization-sustaining activity, and product-level activity.

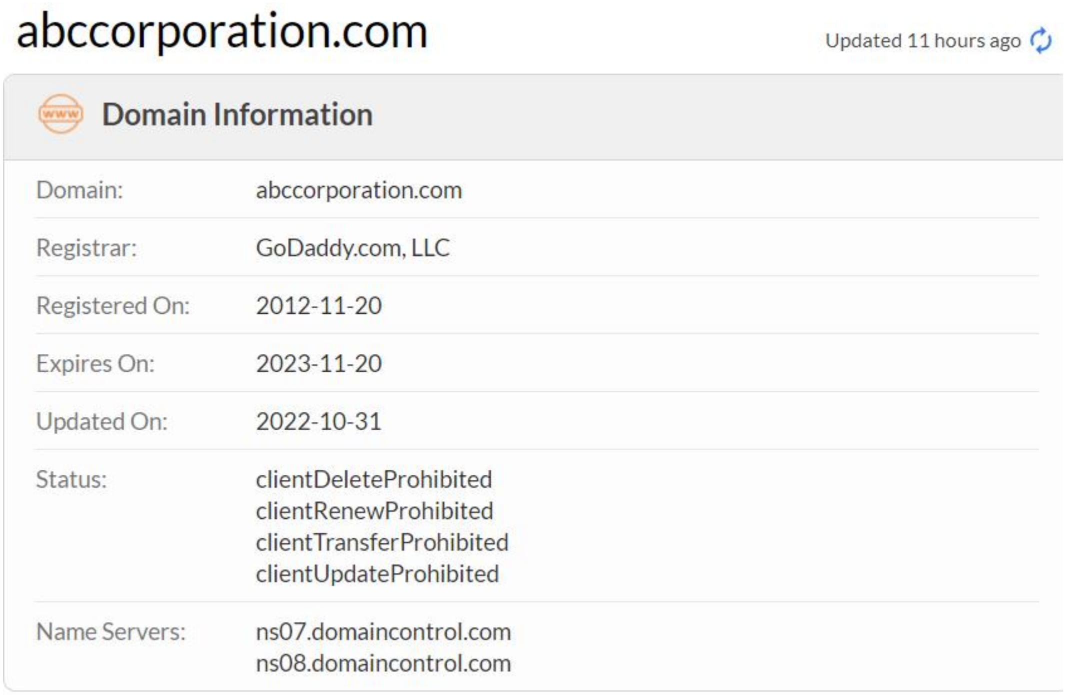
1.1. Scope Purpose and Duration of Work

Scope

This Risk Assessment Applies To the systems,Data,and Networks of ABC Company.

Purpose

The document provides ABC Company with an explanation of assets, threats,and vulnerabilities to systems,data and networks. In addition, this document outlines recommendations for remediation to lower risks for ABC Company



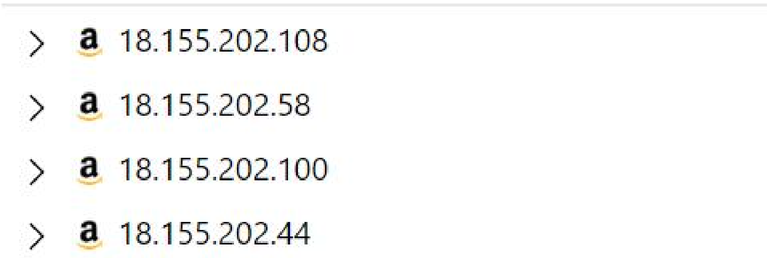
abccorporation.com

Updated 11 hours ago

Domain Information

Domain:	abccorporation.com
Registrar:	GoDaddy.com, LLC
Registered On:	2012-11-20
Expires On:	2023-11-20
Updated On:	2022-10-31
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns07.domaincontrol.com ns08.domaincontrol.com

IP ADDRESSS

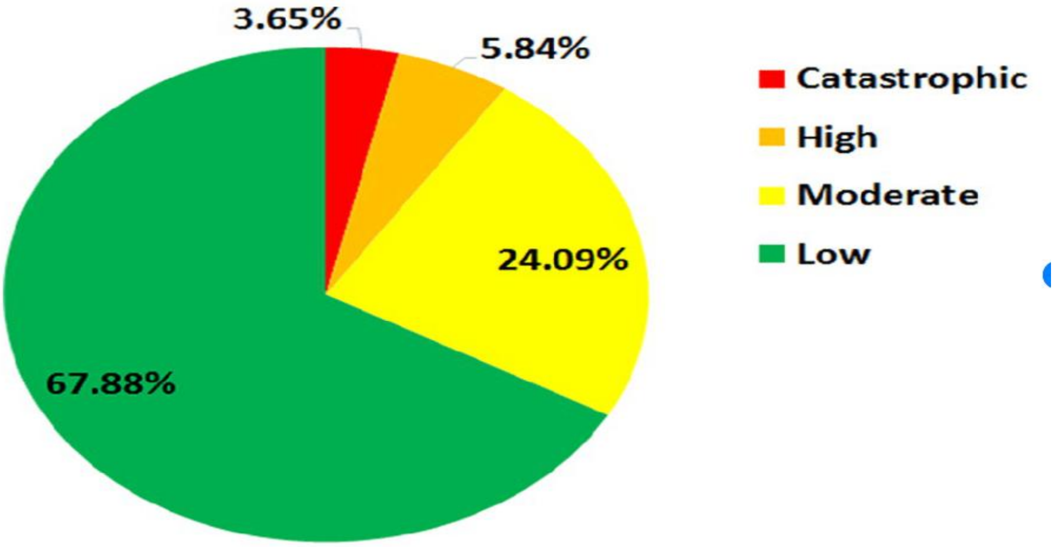


- 18.155.202.108
- 18.155.202.58
- 18.155.202.100
- 18.155.202.44

1.2. Findings

1. High
2. Low
3. Moderate
4. Catastrophic

1.3. Risk Distributions



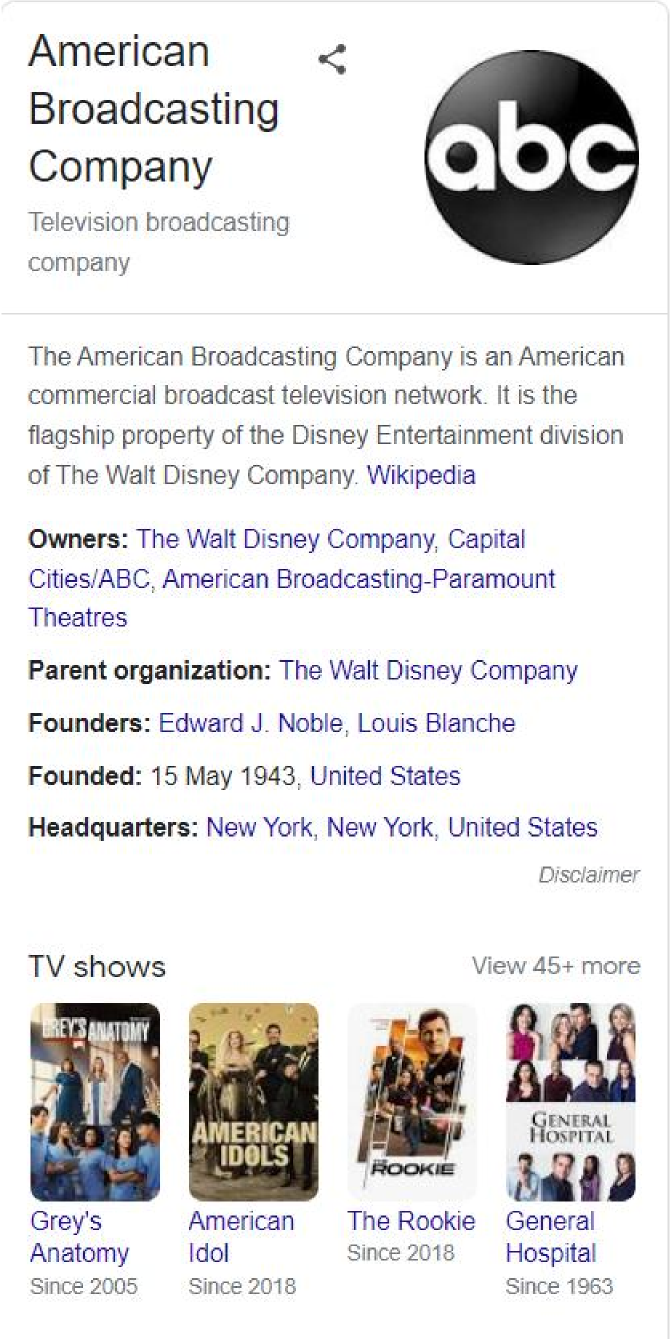
2. Methodology

The methodology consisted of # of steps beginning with the determination of test scope, and ending with reporting. These tests were performed by security experts using potential attackers' modes of operation while controlling execution to prevent harm to the systems being tested. The approach included but is not limited to manual and automated vulnerability scans, verification of findings (automated and otherwise). This verification step and manual scanning process eliminated false positives and erroneous outputs, resulting in more efficient tests.

- Information Gathering
- Determining scope
- Scanning
- Vulnerability Analysis

2.1. Information Gathering

Before directly accessing the target we researched everything we could locate from third party resources. This included DNS records, previous hacking attempts, job listings, email addresses, etc. This information was used in later tests.



American Broadcasting Company

Television broadcasting company

The American Broadcasting Company is an American commercial broadcast television network. It is the flagship property of the Disney Entertainment division of The Walt Disney Company. Wikipedia

Owners: The Walt Disney Company, Capital Cities/ABC, American Broadcasting-Paramount Theatres

Parent organization: The Walt Disney Company

Founders: Edward J. Noble, Louis Blanche

Founded: 15 May 1943, United States

Headquarters: New York, New York, United States

Disclaimer

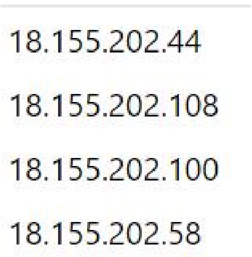
TV shows

View 45+ more

Grey's Anatomy Since 2005	American Idol Since 2018	The Rookie Since 2018	General Hospital Since 1963

Fig : About ABC corporation

2.1.1. IP Addresses and Domains



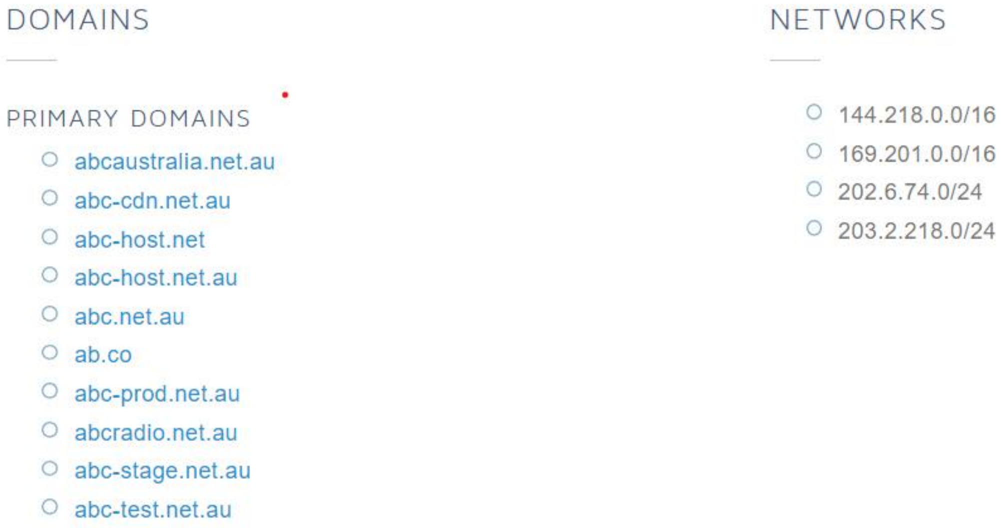
18.155.202.44

18.155.202.108

18.155.202.100

18.155.202.58

Fig : IP ADDRESSES



DOMAINS

PRIMARY DOMAINS

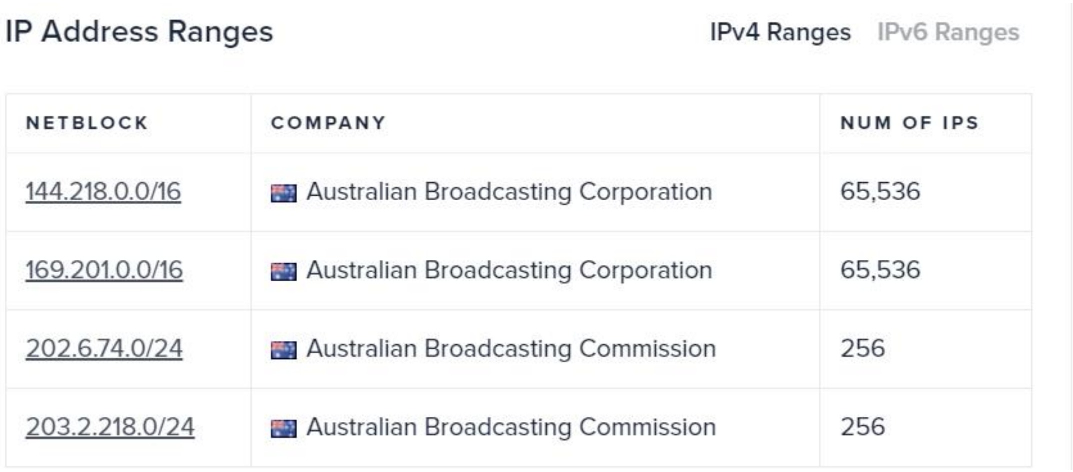
- abcaustralia.net.au
- abc-cdn.net.au
- abc-host.net
- abc-host.net.au
- abc.net.au
- ab.co
- abc-prod.net.au
- abcradio.net.au
- abc-stage.net.au
- abc-test.net.au

NETWORKS

- 144.218.0.0/16
- 169.201.0.0/16
- 202.6.74.0/24
- 203.2.218.0/24

Fig : DOMAINS

2.1.2. IP Range Information



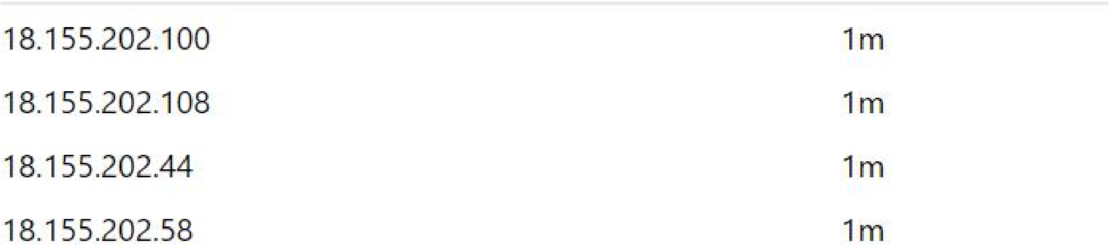
IP Address Ranges

IPv4 Ranges IPv6 Ranges

NETBLOCK	COMPANY	NUM OF IPS
144.218.0.0/16	Australian Broadcasting Corporation	65,536
169.201.0.0/16	Australian Broadcasting Corporation	65,536
202.6.74.0/24	Australian Broadcasting Commission	256
203.2.218.0/24	Australian Broadcasting Commission	256

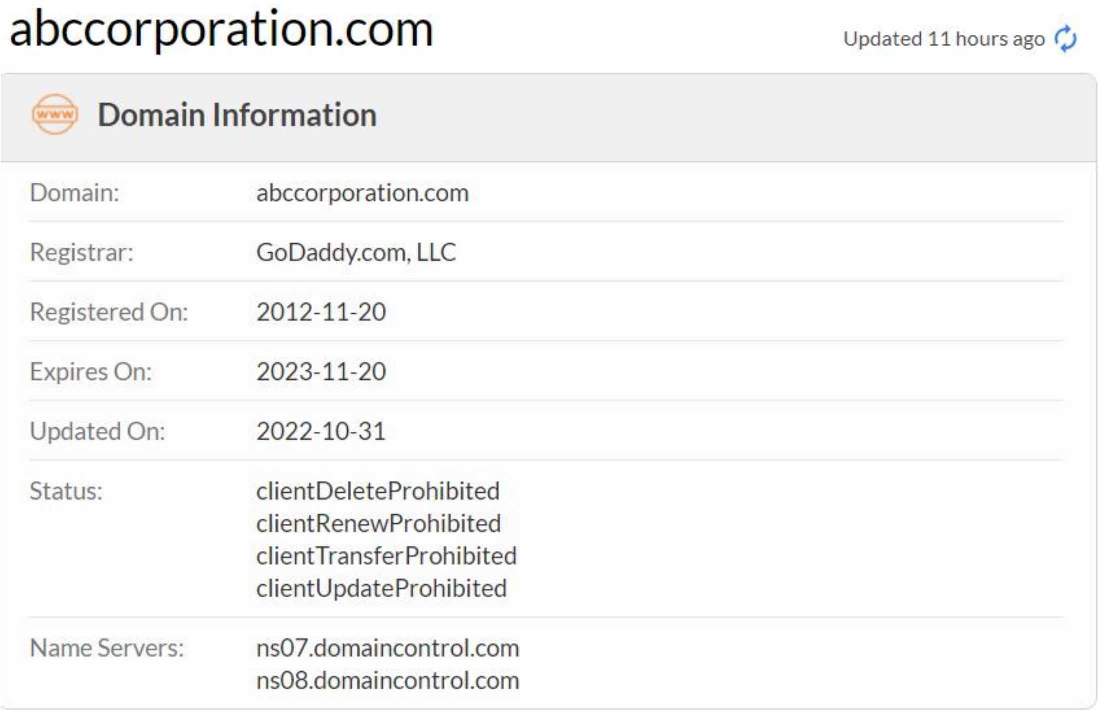
2.1.3. DNS RECORDS

DNS records identify URL/IP pairs. DNS servers connect the organization website to outside world. Exploitation of these servers may lead to malicious usage of the organization web and mail servers.



18.155.202.100	1m
18.155.202.108	1m
18.155.202.44	1m
18.155.202.58	1m

2.1.4. WHO IS LOOK UP



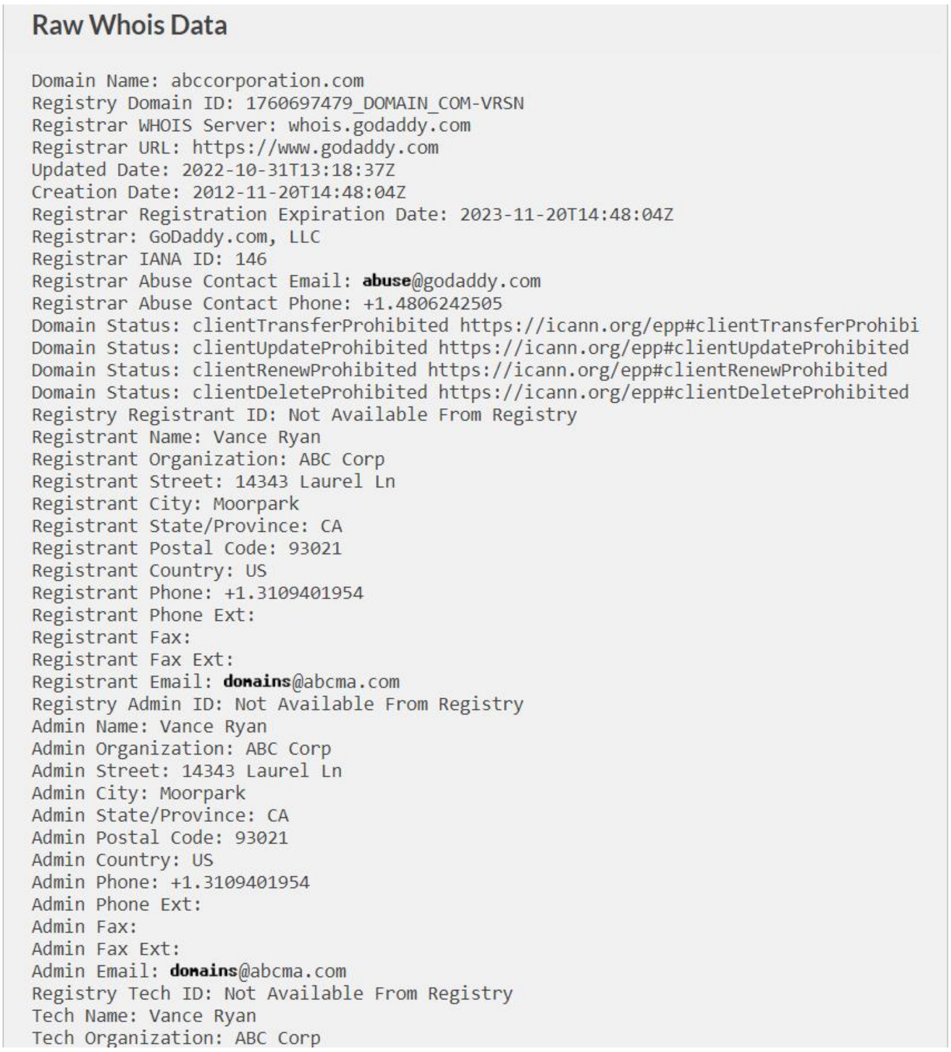
abccorporation.com

Updated 11 hours ago

Domain Information

Domain:	abccorporation.com
Registrar:	GoDaddy.com, LLC
Registered On:	2012-11-20
Expires On:	2023-11-20
Updated On:	2022-10-31
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns07.domaincontrol.com ns08.domaincontrol.com

FIG : DOMAIN INFORMATION

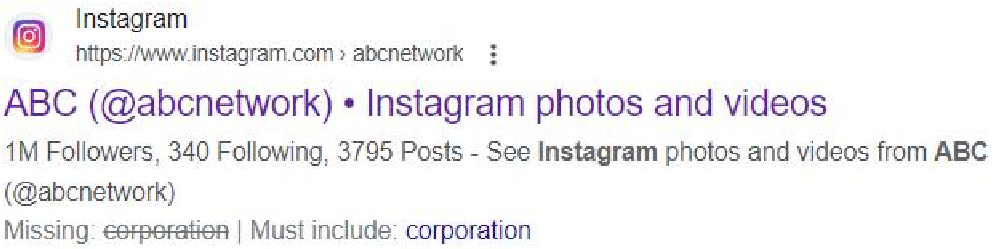


Raw Whois Data

```
Domain Name: abccorporation.com
Registry Domain ID: 1760697479_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2022-10-31T13:18:37Z
Creation Date: 2012-11-20T14:48:04Z
Registrar Registration Expiration Date: 2023-11-20T14:48:04Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibi
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Vance Ryan
Registrant Organization: ABC Corp
Registrant Street: 14343 Laurel Ln
Registrant City: Moorpark
Registrant State/Province: CA
Registrant Postal Code: 93021
Registrant Country: US
Registrant Phone: +1.3109401954
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domains@abcma.com
Registry Admin ID: Not Available From Registry
Admin Name: Vance Ryan
Admin Organization: ABC Corp
Admin Street: 14343 Laurel Ln
Admin City: Moorpark
Admin State/Province: CA
Admin Postal Code: 93021
Admin Country: US
Admin Phone: +1.3109401954
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domains@abcma.com
Registry Tech ID: Not Available From Registry
Tech Name: Vance Ryan
Tech Organization: ABC Corp
```

2.2. Determining the Scope

The **American Broadcasting Company** (**ABC**) is an American commercial broadcast television network. It is the flagship property of the Disney Entertainment division of The Walt Disney Company. The network is headquartered in Burbank, California, on Riverside Drive, directly across the street from Walt Disney Studios and adjacent to the Roy E. Disney Animation Building. The network's secondary offices, and headquarters of its news division, are in New York City, at its broadcast center at 77 West 66th Street on the Upper West Side of Manhattan.



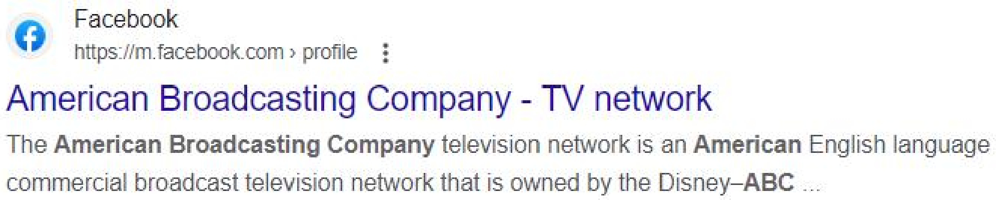
Instagram
https://www.instagram.com › abcnetwork

ABC (@abcnetwork) • Instagram photos and videos

1M Followers, 340 Following, 3795 Posts - See **Instagram** photos and videos from **ABC** (@abcnetwork)

Missing: ~~corporation~~ | Must include: corporation

Fig : Instagram profile

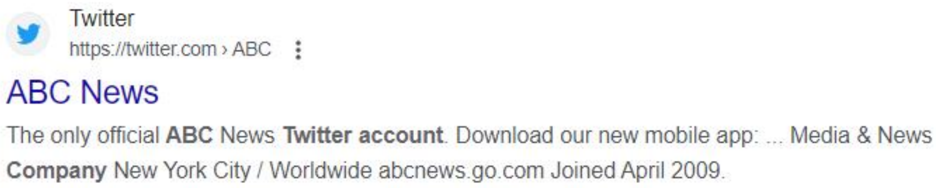


Facebook
https://m.facebook.com › profile

American Broadcasting Company - TV network

The **American Broadcasting Company** television network is an **American** English language commercial broadcast television network that is owned by the Disney–**ABC** ...

Fig : Facebook profile

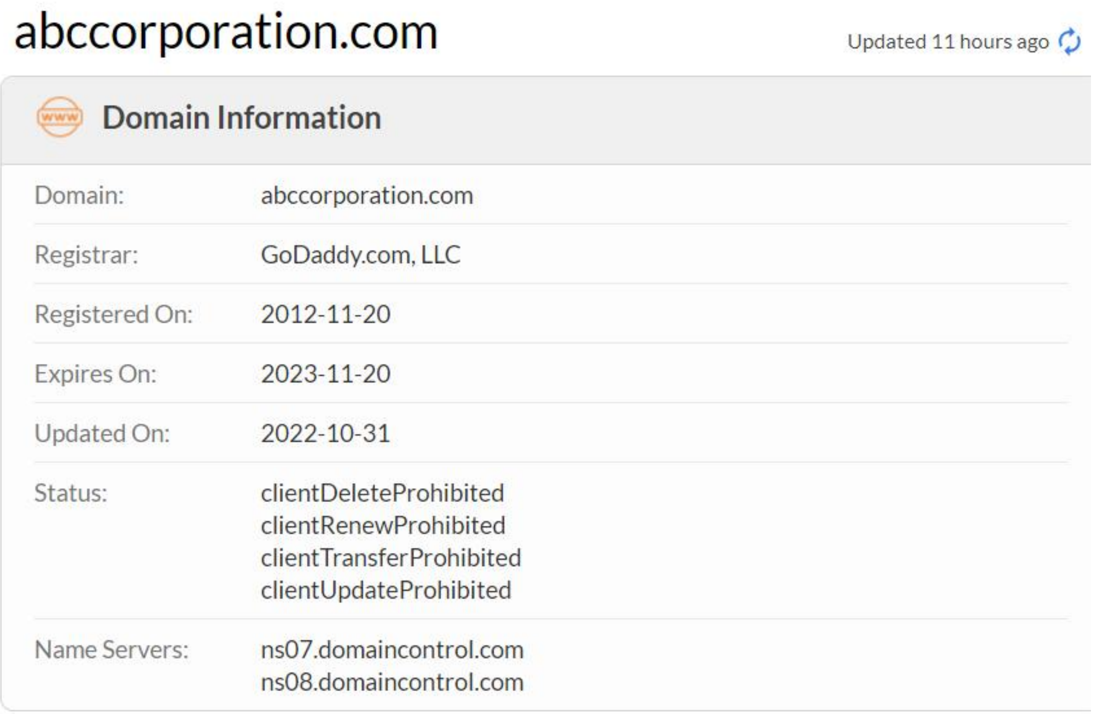


Twitter
https://twitter.com › ABC

ABC News

The only official **ABC** News **Twitter account**. Download our new mobile app: ... Media & News **Company** New York City / Worldwide abcnews.go.com Joined April 2009.

Fig : twitter profile



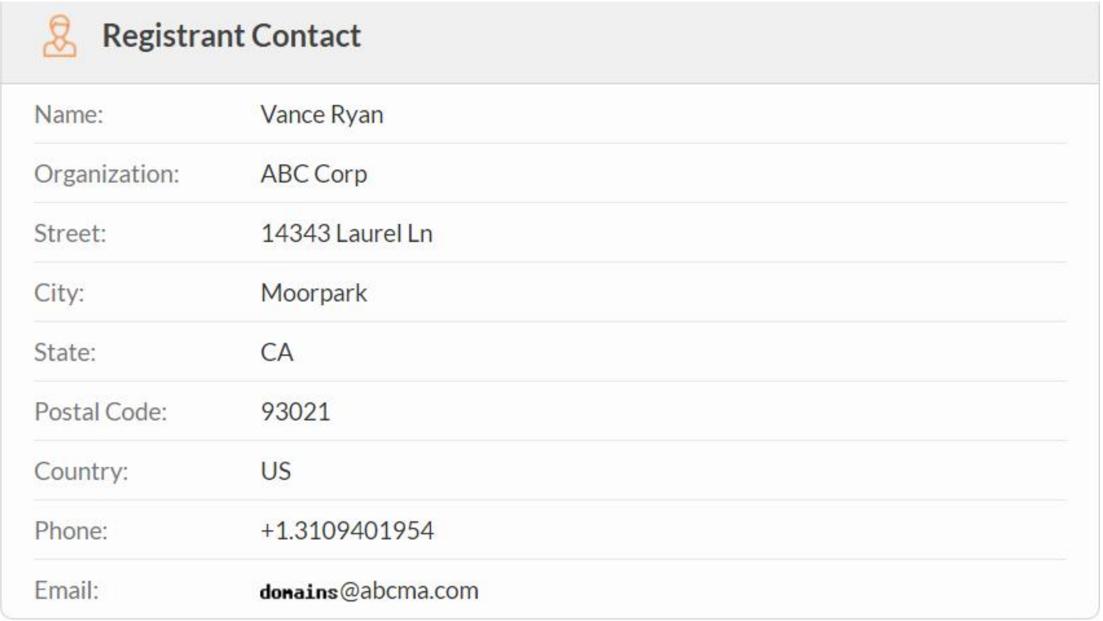
abccorporation.com

Updated 11 hours ago

Domain Information

Domain:	abccorporation.com
Registrar:	GoDaddy.com, LLC
Registered On:	2012-11-20
Expires On:	2023-11-20
Updated On:	2022-10-31
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns07.domaincontrol.com ns08.domaincontrol.com

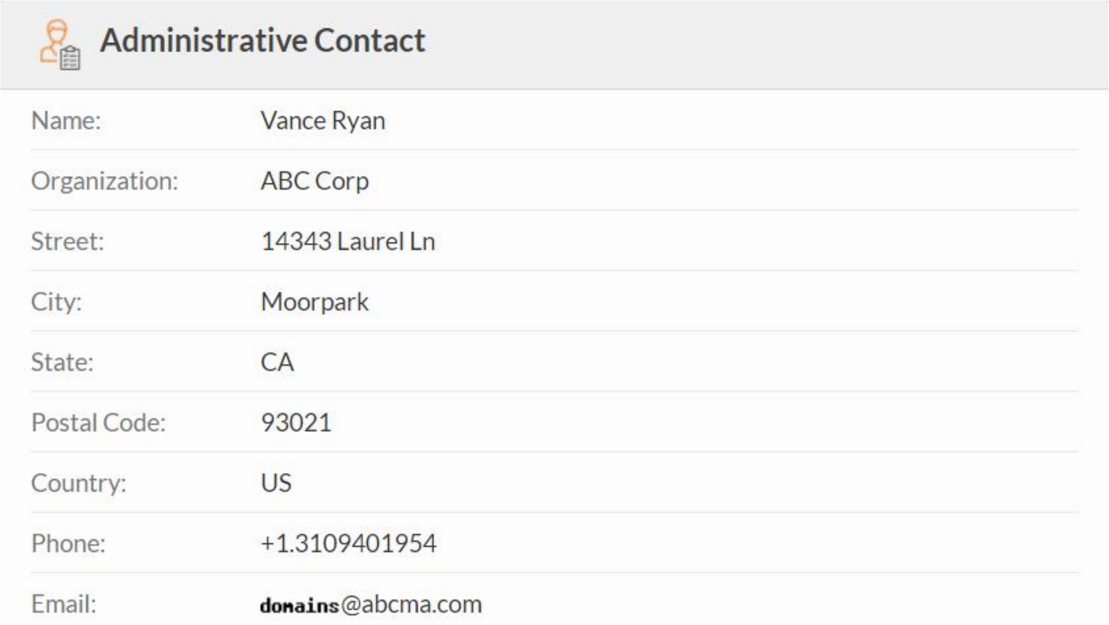
Fig : Domain



Registrant Contact

Name:	Vance Ryan
Organization:	ABC Corp
Street:	14343 Laurel Ln
City:	Moorpark
State:	CA
Postal Code:	93021
Country:	US
Phone:	+1.3109401954
Email:	domains@abcma.com

Fig : Registrant Contact



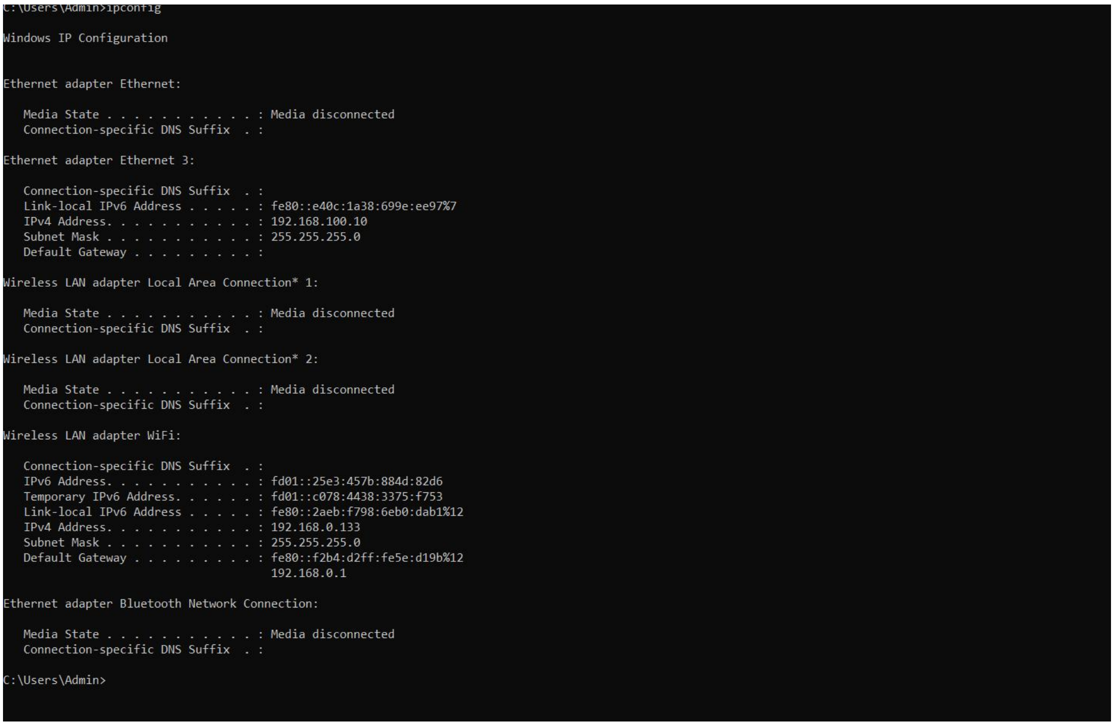
Administrative Contact

Name:	Vance Ryan
Organization:	ABC Corp
Street:	14343 Laurel Ln
City:	Moorpark
State:	CA
Postal Code:	93021
Country:	US
Phone:	+1.3109401954
Email:	domains@abcma.com

Fig : Administrative Contact

2.3. Scanning

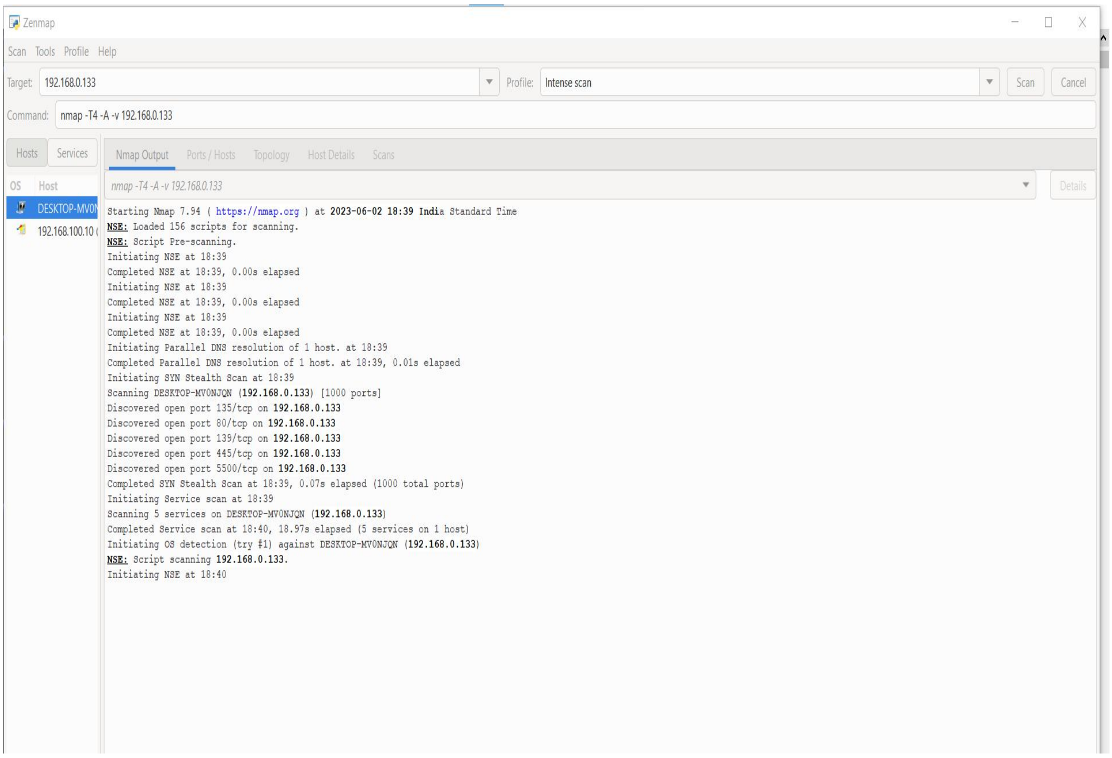
The below fig is a command prompt of my system I am using command prompt and using my own systems IP addresses to make a scanning.



```
C:\Users\Admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e40c:1a38:699e:ee97%7
   IPv4 Address. . . . . . . . . . . : 192.168.100.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : fd01::25e3:457b:884d:82d6
   Temporary IPv6 Address. . . . . . : fd01::c078:4438:3375:f753
   Link-local IPv6 Address . . . . . : fe80::2aeb:f798:6eb0:dab1%12
   IPv4 Address. . . . . . . . . . . : 192.168.0.133
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::f2b4:d2ff:fe5e:d19b%12
                                       192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Admin>
```

By using Nmap I am finding the scanning process to make understand and make understand how to use scanning

The below figure is about the intense scanning of IP address 192.168.0.133



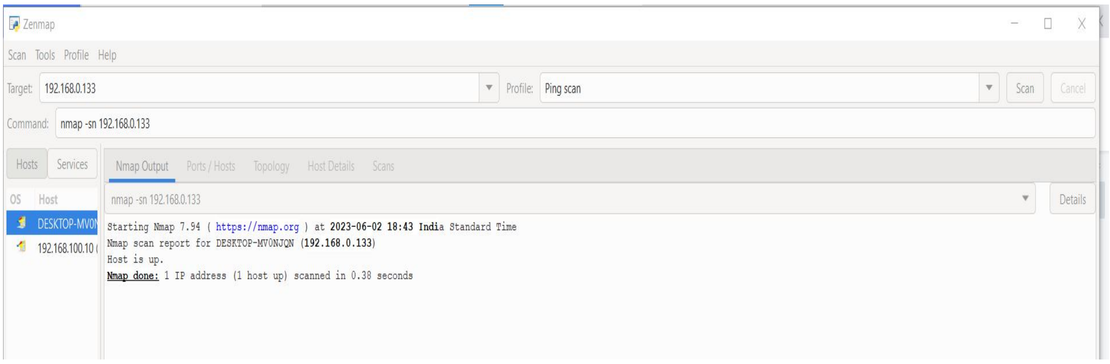
Target: 192.168.0.133

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.133

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-02 18:39 India Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:39
Completed NSE at 18:39, 0.00s elapsed
Initiating NSE at 18:39
Completed NSE at 18:39, 0.00s elapsed
Initiating NSE at 18:39
Completed NSE at 18:39, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 18:39
Completed Parallel DNS resolution of 1 host. at 18:39, 0.01s elapsed
Initiating SYN Stealth Scan at 18:39
Scanning DESKTOP-MV0NJQN (192.168.0.133) [1000 ports]
Discovered open port 135/tcp on 192.168.0.133
Discovered open port 80/tcp on 192.168.0.133
Discovered open port 139/tcp on 192.168.0.133
Discovered open port 445/tcp on 192.168.0.133
Discovered open port 5500/tcp on 192.168.0.133
Completed SYN Stealth Scan at 18:39, 0.07s elapsed (1000 total ports)
Initiating Service scan at 18:39
Scanning 5 services on DESKTOP-MV0NJQN (192.168.0.133)
Completed Service scan at 18:40, 18.97s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against DESKTOP-MV0NJQN (192.168.0.133)
NSE: Script scanning 192.168.0.133.
Initiating NSE at 18:40
```

By using ping scan



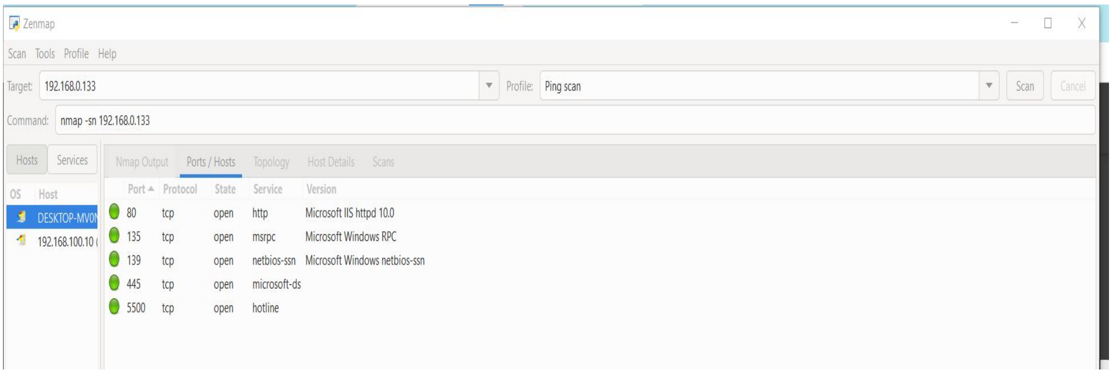
Target: 192.168.0.133

Profile: Ping scan

Command: nmap -sn 192.168.0.133

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-02 18:43 India Standard Time
Nmap scan report for DESKTOP-MV0NJQN (192.168.0.133)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

2.3.1. Port scan



Target: 192.168.0.133
Profile: Ping scan
Command: nmap -sn 192.168.0.133

OS	Host
	DESKTOP-MV0N
	192.168.100.10 (

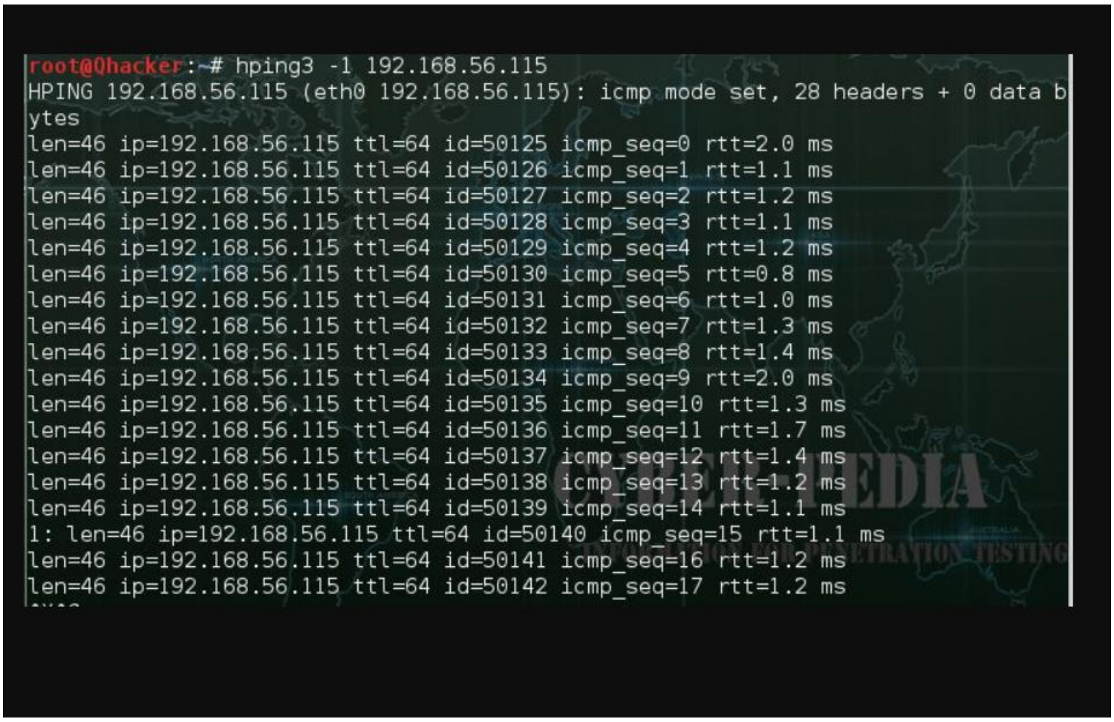
Port	Protocol	State	Service	Version
80	tcp	open	http	Microsoft IIS httpd 10.0
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	
5500	tcp	open	hotline	

Primarily nmap is used to scan the targets. Besides nmap, tools like strobe, x probe, a map are used to determine which ports are open, which operating systems are working on targets, and which services are used.

2.3.2. Route Scan

Using tools like hping, scanrand, traceroute, the network mapping of targets can be determined. It is also useful for detecting defensive measures like IDS, IPS, UTM, and firewalls.

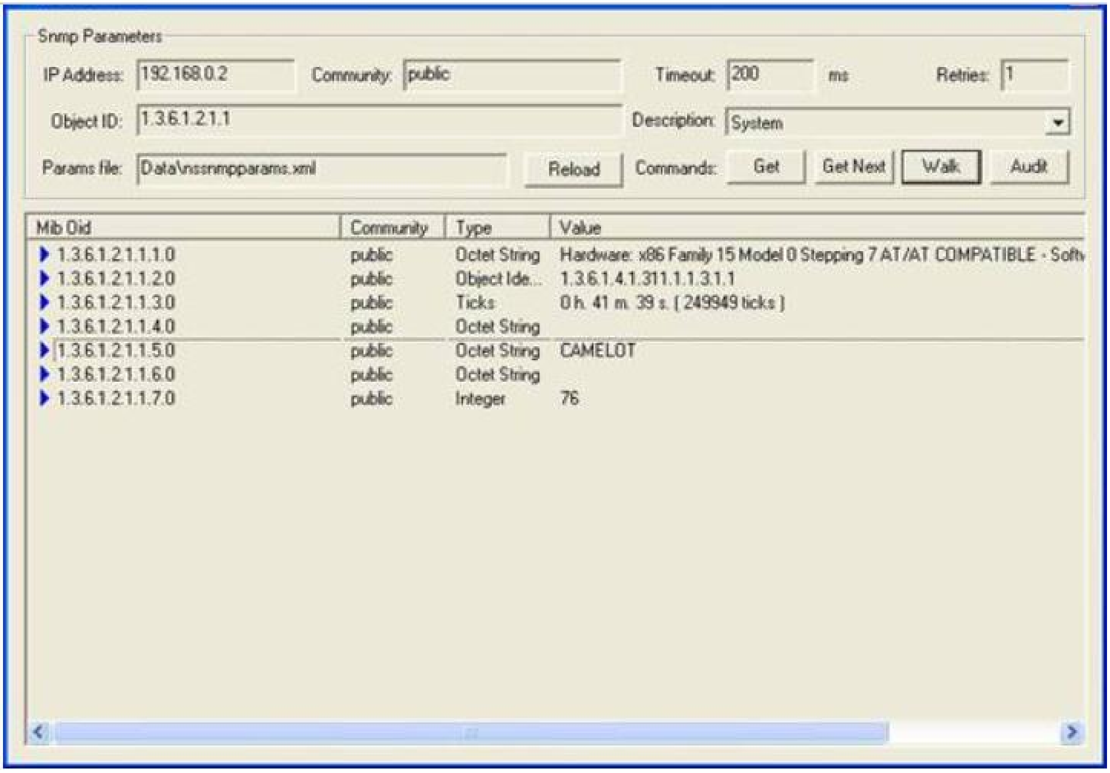
I haved used hping tool to find an analyzer for tcp/ip protocol



```
root@Qhacker:~# hping3 -1 192.168.56.115
HPING 192.168.56.115 (eth0 192.168.56.115): icmp mode set, 28 headers + 0 data b
ytes
len=46 ip=192.168.56.115 ttl=64 id=50125 icmp_seq=0 rtt=2.0 ms
len=46 ip=192.168.56.115 ttl=64 id=50126 icmp_seq=1 rtt=1.1 ms
len=46 ip=192.168.56.115 ttl=64 id=50127 icmp_seq=2 rtt=1.2 ms
len=46 ip=192.168.56.115 ttl=64 id=50128 icmp_seq=3 rtt=1.1 ms
len=46 ip=192.168.56.115 ttl=64 id=50129 icmp_seq=4 rtt=1.2 ms
len=46 ip=192.168.56.115 ttl=64 id=50130 icmp_seq=5 rtt=0.8 ms
len=46 ip=192.168.56.115 ttl=64 id=50131 icmp_seq=6 rtt=1.0 ms
len=46 ip=192.168.56.115 ttl=64 id=50132 icmp_seq=7 rtt=1.3 ms
len=46 ip=192.168.56.115 ttl=64 id=50133 icmp_seq=8 rtt=1.4 ms
len=46 ip=192.168.56.115 ttl=64 id=50134 icmp_seq=9 rtt=2.0 ms
len=46 ip=192.168.56.115 ttl=64 id=50135 icmp_seq=10 rtt=1.3 ms
len=46 ip=192.168.56.115 ttl=64 id=50136 icmp_seq=11 rtt=1.7 ms
len=46 ip=192.168.56.115 ttl=64 id=50137 icmp_seq=12 rtt=1.4 ms
len=46 ip=192.168.56.115 ttl=64 id=50138 icmp_seq=13 rtt=1.2 ms
len=46 ip=192.168.56.115 ttl=64 id=50139 icmp_seq=14 rtt=1.1 ms
1: len=46 ip=192.168.56.115 ttl=64 id=50140 icmp_seq=15 rtt=1.1 ms
len=46 ip=192.168.56.115 ttl=64 id=50141 icmp_seq=16 rtt=1.2 ms
len=46 ip=192.168.56.115 ttl=64 id=50142 icmp_seq=17 rtt=1.2 ms
```

2.3.3. SNMP SCAN

Using onesixtyone, SNMP scans were conducted to gain information.
onesixtyone is a simple SNMP scanner which sends SNMP requests for the sys Descr value asynchronously with user-adjustable sending times and then logs the responses which gives the description of the software running on the device.



IP Address: 192.168.0.2 Community: public Timeout: 200 ms Retries: 1

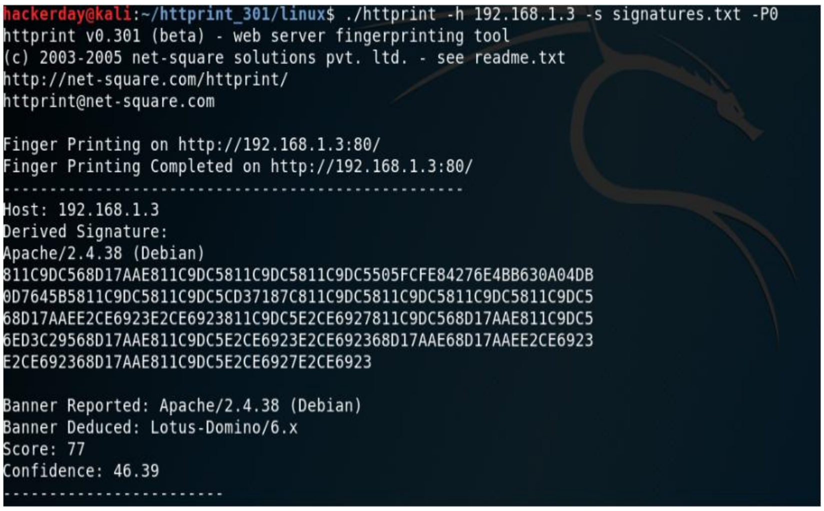
Object ID: 1.3.6.1.2.1.1 Description: System

Params file: Data\nssnmpparams.xml

Mib Oid	Community	Type	Value
1.3.6.1.2.1.1.1.0	public	Octet String	Hardware: x86 Family 15 Model 0 Stepping 7 AT/AT COMPATIBLE - Softw
1.3.6.1.2.1.1.2.0	public	Object Ide...	1.3.6.1.4.1.311.1.1.3.1.1
1.3.6.1.2.1.1.3.0	public	Ticks	0 h. 41 m. 39 s. (249949 ticks)
1.3.6.1.2.1.1.4.0	public	Octet String	
1.3.6.1.2.1.1.5.0	public	Octet String	CAMELOT
1.3.6.1.2.1.1.6.0	public	Octet String	
1.3.6.1.2.1.1.7.0	public	Integer	76

2.3.4. Server Identification

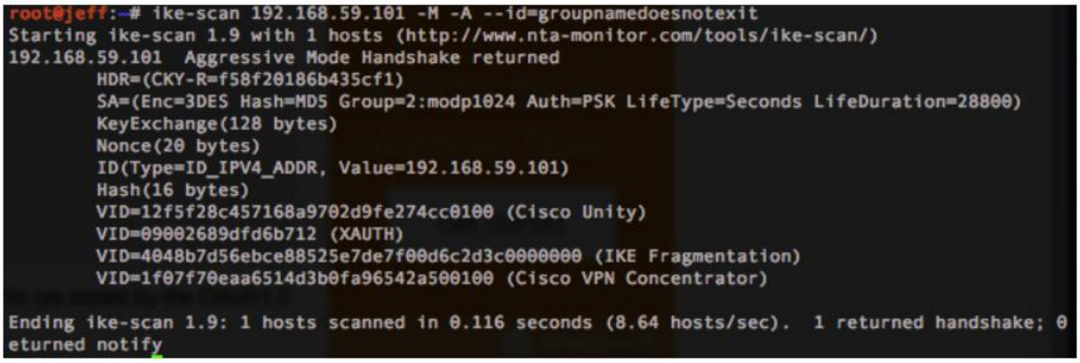
Using tools like httprint, smtpscan, detected servers (HTTP, FTP, SMTP, POP, IMAP, etc) from previous scans are listed and classified by their brand/model/operation systems/version numbers.



```
hackerday@kali:~/httprint_301/linux$ ./httprint -h 192.168.1.3 -s signatures.txt -P0
httprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@net-square.com

Finger Printing on http://192.168.1.3:80/
Finger Printing Completed on http://192.168.1.3:80/
--------------------------------------------------
Host: 192.168.1.3
Derived Signature:
Apache/2.4.38 (Debian)
811C9DC568D17AAE811C9DC5811C9DC5811C9DC5505FCFE84276E4BB630A04DB
0D7645B5811C9DC5811C9DC5CD37187C811C9DC5811C9DC5811C9DC5811C9DC5
68D17AAEE2CE6923E2CE6923811C9DC5E2CE6927811C9DC568D17AAE811C9DC5
6ED3C29568D17AAE811C9DC5E2CE6923E2CE692368D17AAE68D17AAEE2CE6923
E2CE692368D17AAE811C9DC5E2CE6927E2CE6923

Banner Reported: Apache/2.4.38 (Debian)
Banner Deduced: Lotus-Domino/6.x
Score: 77
Confidence: 46.39
------------------------
```

2.3.5. VPN Identification

Using ike-scan, the network was traced for VPN servers.

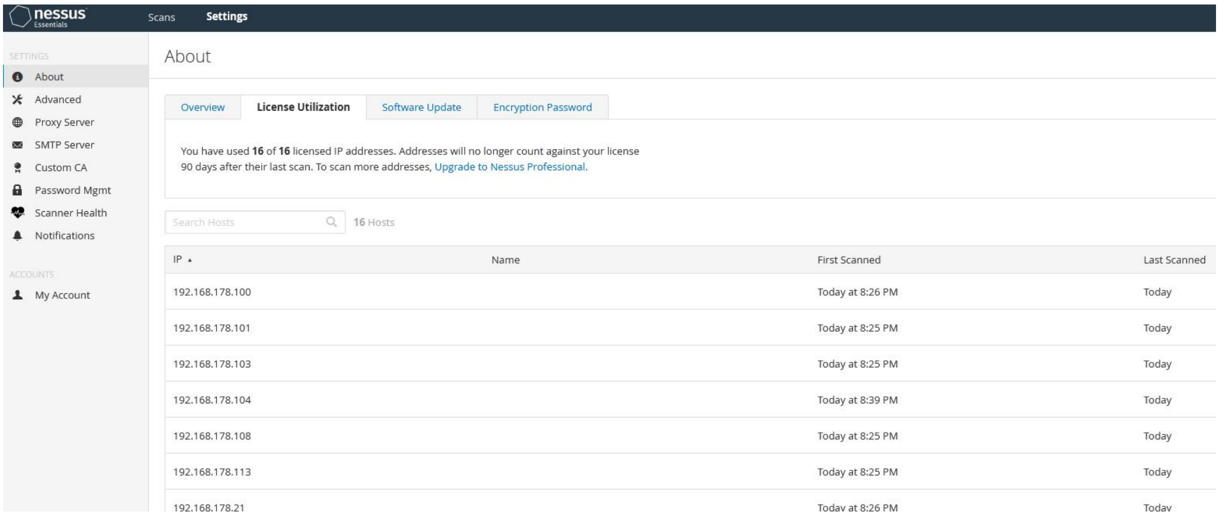


```
root@jeff:~# ike-scan 192.168.59.101 -M -A --id=groupnamedoesnotexit
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.59.101  Aggressive Mode Handshake returned
        HDR=(CKY-R=f58f20186b435cf1)
        SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
        KeyExchange(128 bytes)
        Nonce(20 bytes)
        ID(Type=ID_IPV4_ADDR, Value=192.168.59.101)
        Hash(16 bytes)
        VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity)
        VID=09002689dfd6b712 (XAUTH)
        VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)
        VID=1f07f70eaa6514d3b0fa96542a500100 (Cisco VPN Concentrator)

Ending ike-scan 1.9: 1 hosts scanned in 0.116 seconds (8.64 hosts/sec).  1 returned handshake; 0
eturned notify
```

2.4. Vulnerability Analysis

2.4.1. Scanning Target Systems

Using vulnerability scanners like nessus, acunetix, etc, target systems were crosschecked with up-to-date vulnerability databases.



About

You have used **16** of **16** licensed IP addresses. Addresses will no longer count against your license 90 days after their last scan. To scan more addresses, Upgrade to Nessus Professional.

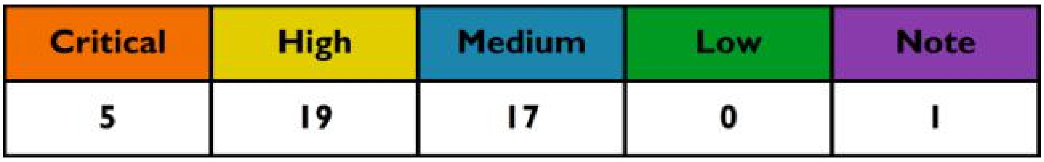
16 Hosts

IP ▲	Name	First Scanned	Last Scanned
192.168.178.100		Today at 8:26 PM	Today
192.168.178.101		Today at 8:25 PM	Today
192.168.178.103		Today at 8:25 PM	Today
192.168.178.104		Today at 8:39 PM	Today
192.168.178.108		Today at 8:25 PM	Today
192.168.178.113		Today at 8:25 PM	Today
192.168.178.21		Today at 8:26 PM	Today

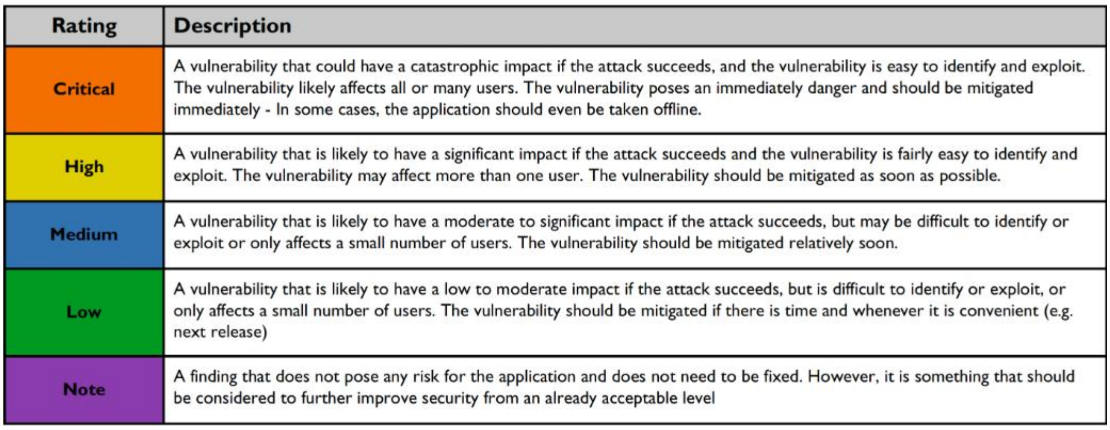
3. Detailed Information on Findings

3.1. Definition of Risk levels

Risk levels are based upon PCI / DSS standard definitions. The risk levels contained in this report are not the same as risk levels reported by the automated tools in general. Risk Level Explanation



Critical	High	Medium	Low	Note
5	19	17	0	1



Rating	Description
Critical	A vulnerability that could have a catastrophic impact if the attack succeeds, and the vulnerability is easy to identify and exploit. The vulnerability likely affects all or many users. The vulnerability poses an immediately danger and should be mitigated immediately - In some cases, the application should even be taken offline.
High	A vulnerability that is likely to have a significant impact if the attack succeeds and the vulnerability is fairly easy to identify and exploit. The vulnerability may affect more than one user. The vulnerability should be mitigated as soon as possible.
Medium	A vulnerability that is likely to have a moderate to significant impact if the attack succeeds, but may be difficult to identify or exploit or only affects a small number of users. The vulnerability should be mitigated relatively soon.
Low	A vulnerability that is likely to have a low to moderate impact if the attack succeeds, but is difficult to identify or exploit, or only affects a small number of users. The vulnerability should be mitigated if there is time and whenever it is convenient (e.g. next release)
Note	A finding that does not pose any risk for the application and does not need to be fixed. However, it is something that should be considered to further improve security from an already acceptable level

3.2.Vulnerability List

Name	Parameter Name	Definition	Parameter Type	Risk Level
SQL Injection	btcAmount	A Critical severity vulnerability means that your website is at risk of being hacked at any time.	JSON	CRITICAL
High Severity	Hello	A High severity vulnerability means that your website can be hacked and can lead hackers to find other vulnerabilities which have a bigger impact	*GET	HIGH
Medium severity	payload	Even though special conditions are required to exploit Medium	GFT	Medium

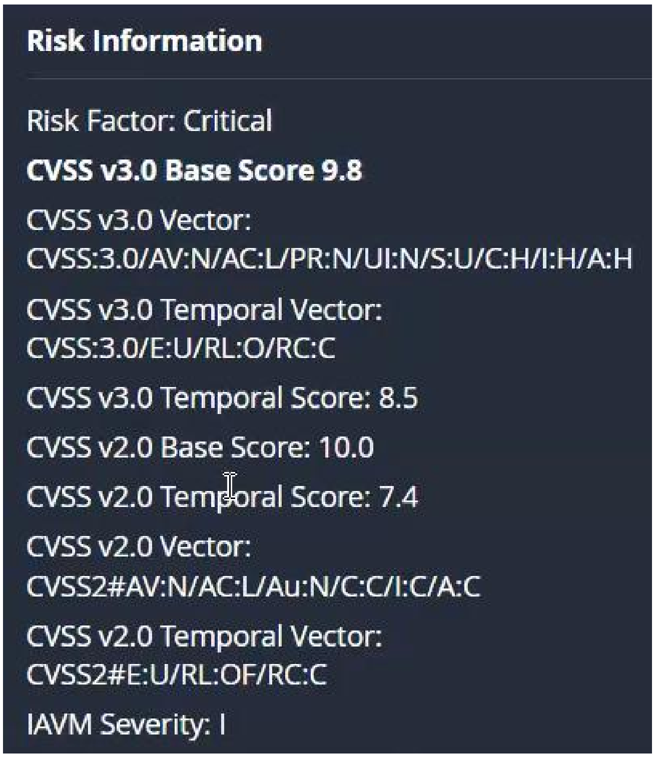
		Severity issues and they don’t directly affect the application or system (in contrast to Critical and High Severities), in order to keep your web application secure and comply with the regulations, they should still be fixed.		
Low severity	Body XML	A decision on whether to fix these issues should be determined by assessing the context in the application, and by considering the business impacts.	Body XML	Low

4.Detected Vulnerabilities and Recommendations

4.1. Apache Vulnerabilities

4.1.1. Apache 2.4.X<2.4.56 Multiple Vulnerabilities

Risk : Critical



Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 8.5

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 7.4

CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C

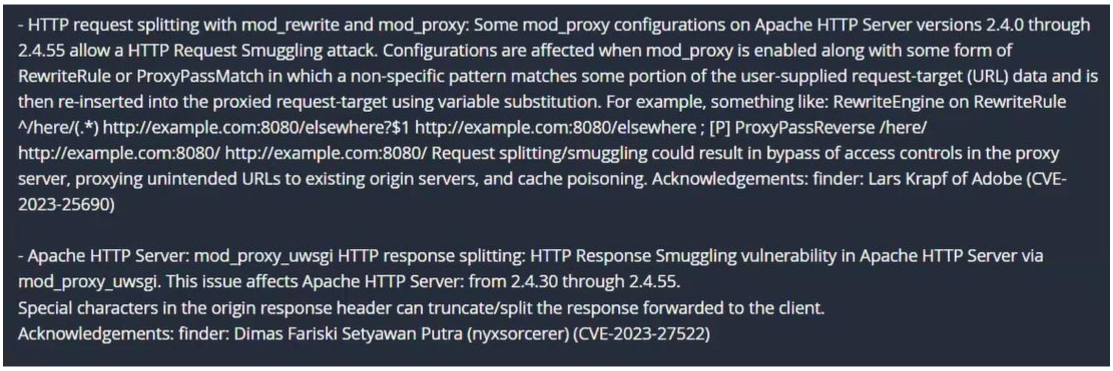
IAVM Severity: I

Source : The version of Apache httpd installed on the remote host is prior to 2.4.56. It is therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory.

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory.

Explanation :

HTTP request splitting with mod_rewrite and mod_proxy:Some mod_proxy configurations on Apache HTTP Server Versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configuration are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied rquest-target(URL) data and is then re-inserted into the proxied request-target using variable substitution.



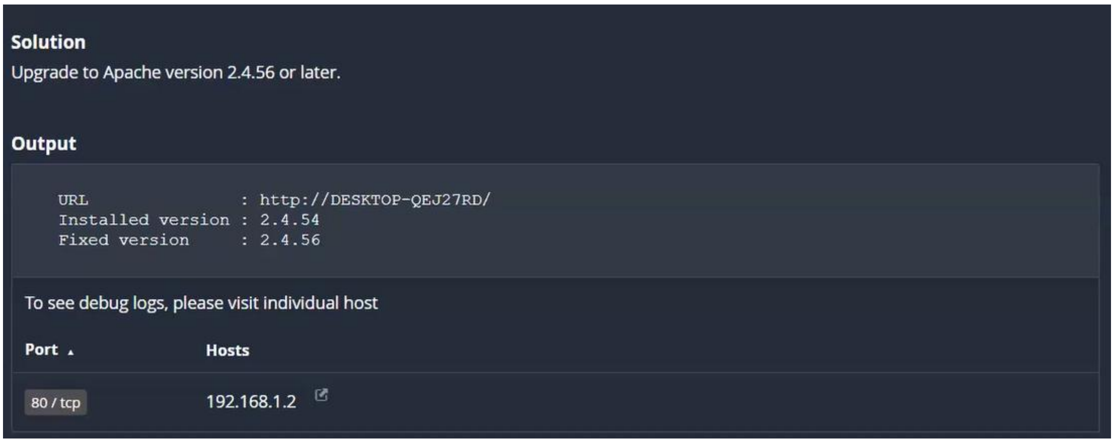
- HTTP request splitting with mod_rewrite and mod_proxy: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule ^/here/(.*) http://example.com:8080/elsewhere?$1 http://example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Acknowledgements: finder: Lars Krapf of Adobe (CVE-2023-25690)

- Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.
Special characters in the origin response header can truncate/split the response forwarded to the client.
Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

Recommendation :

Upgrade to Apache Version 2.4.56 or later

SOLUTION AND RECOMMADATION:



Solution

Upgrade to Apache version 2.4.56 or later.

Output

```
    URL               : http://DESKTOP-QEJ27RD/
    Installed version : 2.4.54
    Fixed version     : 2.4.56
```

To see debug logs, please visit individual host

Port ▴	Hosts
80 / tcp	192.168.1.2

4.2. vulnerabilities by IP Numbers

Name	**IP Address**	**Vulnerability**
Attacker	129.174.124.122	___
Workstations	129.174.124.184/185/186	HTML objects memory corruption vulnerability (CVE-2009-1918)
Webserver1 product web Service	129.174.124.53:8080	SQL Injection (CWE89)
Webserver2 Product Web Service	129.174.124.53:80	SQL Injection (CWE89)
Administrator	129.174.124.137	Cross-Site Scripting Flaw (XSS)
Database Server	129.174.124.35	___