

Assignment Day 4

Question 1:

Find out the mail servers of the following domain :

Ibm.com

Wipro.com

ans: 1)ibm.com

```

C:\Users\Aayush>nslookup
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Aayush>nslookup
Default Server: UnKnown
Address: 192.168.43.1

> www.ibm.com
Server: UnKnown
Address: 192.168.43.1

Non-authoritative answer:
Name: e2874.dscx.akamaiedge.net
Addresses: 2485:200:1630:991::b3a
           2485:200:1630:9b8::b3a
           104.71.100.25
Aliases: www.ibm.com
          www.ibm.com.cs186.net
          outer-ccdn-dual.ibmcom.edgekey.net
          outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net

> set type=mx
> www.ibm.com
Server: UnKnown
Address: 192.168.43.1

Non-authoritative answer:
www.ibm.com canonical name = www.ibm.com.cs186.net
www.ibm.com.cs186.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net
outer-ccdn-dual.ibmcom.edgekey.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net canonical name = e2874.dscx.akamaiedge.net

dscx.akamaiedge.net
primary name server = n0dscx.akamaiedge.net
responsible mail addr = hostmaster.akamai.com
serial = 1598266139
refresh = 1000 (16 mins 40 secs)
retry = 1000 (16 mins 40 secs)
expire = 1000 (16 mins 40 secs)
default TTL = 1800 (30 mins)
>
```

2)wipro.com

```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Aayush>nslookup
Default Server: UnKnown
Address: 192.168.43.1

> set type=mx
> www.wipro.com
Server: UnKnown
Address: 192.168.43.1




Non-authoritative answer:
www.wipro.com canonical name = d361nqn33s63ex.cloudfront.net

d361nqn33s63ex.cloudfront.net
primary name server = ns-1658.awsdns-15.co.uk
responsible mail addr = awsdns-hostmaster.amazon.com
serial = 1
refresh = 7200 (2 hours)
retry = 900 (15 mins)
expire = 1209600 (14 days)
default TTL = 86400 (1 day)
>
```

Question 2:

Find the locations, where these email servers are hosted.

ans:IBM.com

Pref	Hostname	IP Address	TTL		
5	mx0a-001b2d01.pphosted.com	148.163.156.1 <small>Proofpoint, Inc. (AS26211)</small>	60 min	Blacklist Check	SMTP Test
5	mx0b-001b2d01.pphosted.com	148.163.158.5 <small>Proofpoint, Inc. (AS22843)</small>	60 min	Blacklist Check	SMTP Test
Test		Result			
	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled		 More Info	
	DMARC Record Published	DMARC Record found			
	DNS Record Published	DNS Record found			

Pref	Hostname	IP Address	TTL	
10	mx0-00190b01.gslb.pphosted.com	67.231.149.131 Proofpoint, Inc. (AS26211)	5 min	Blacklist Check SMTP Test
10	mx0-00190b01.gslb.pphosted.com	67.231.157.127 Proofpoint, Inc. (AS22843)	5 min	Blacklist Check SMTP Test
20	mx0a-00190b01.pphosted.com	67.231.149.131 Proofpoint, Inc. (AS26211)	5 min	Blacklist Check SMTP Test
20	mx0a-00190b01.pphosted.com	2620:100:9001:583::1	5 min	Blacklist Check
20	mx0b-00190b01.pphosted.com	67.231.157.127 Proofpoint, Inc. (AS22843)	5 min	Blacklist Check SMTP Test
20	mx0b-00190b01.pphosted.com	2620:100:9005:57f::1	5 min	Blacklist Check

Test	Result
✓ DMARC Record Published	DMARC Record found
✓ DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓ DNS Record Published	DNS Record found

2.WIPRO.com

Pref	Hostname	IP Address	TTL	
0	wipro-com.mail.protection.outlook.com	104.47.124.36 Microsoft Corporation (AS8075)	60 min	Blacklist Check SMTP Test

Test	Result
✓ DMARC Record Published	DMARC Record found
✓ DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓ DNS Record Published	DNS Record found

Pref	Hostname	IP Address	TTL	
5	amazon-smtp.amazon.com	52.94.124.7 Amazon.com, Inc. (AS16509)	15 min	Blacklist Check SMTP Test

Test	Result
✓ DMARC Record Published	DMARC Record found
✓ DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓ DNS Record Published	DNS Record found

Question 3:

Scan and find out port numbers open
203.163.246.23

ANS:

Back to Scan Templates

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

TENABLE

- Community
- Research

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: ktech-scanning

Description: Scanning for vulnerabilities

Folder: My Scans

Targets: 192.168.43.150

Upload Targets [Add File](#)

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

TENABLE

Community

Research

ktech-scanning

Back to All Scans

Configure

Launch

Report

Export

Hosts

Vulnerabilities

History

Search History

1 History

Start Time	Last Modified	Status
Current	Today at 2:03 PM	Completed

Scan Details

Policy:

Status:

Scanner:

Start:

End:

Elapsed:

Basic Network Scan

Completed

Local Scanner

Today at 2:03 PM

Today at 2:03 PM

a few seconds

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

TENABLE

Community

Research

ktech-scanning

Back to All Scans

Configure

Hosts

Vulnerabilities

History

Filter

Search Vulnerabilities

6 Vulnerabilities

Sev	Name	Family	Count
INFO	SMB (Multiple Issues)	Windows	8
INFO	DCE Services Enumeration	Windows	7
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	Nessus Windows Scan Not Performed with Admin Privil...	Settings	1
INFO	Server Message Block (SMB) Protocol Version 1 Enabled...	Misc.	1
INFO	Universal Plug and Play (UPnP) Protocol Detection	Service detection	1

Scan Details

Policy:

Status:

Scanner:

Start:

Basic Network Scan

Running

Local Scanner

Today at 2:04 PM

Vulnerabilities

Critical

High

Medium

Low

Info

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

TENABLE

Community

Research

ktech-scanning

Back to All Scans

Configure

Hosts

Vulnerabilities

History

Filter

Search Hosts

1 Host

Host	Vulnerabilities	%
192.168.43.156	19	4%

Scan Details

Policy:

Status:

Scanner:

Start:

Basic Network Scan

Running

Local Scanner

Today at 2:04 PM

Vulnerabilities

Critical

High

Medium

Low

Info

FOLDERS

My Scans

All Scans

Trash

RESOURCES

★ Policies

🔧 Plugin Rules

🔍 Scanners

TENABLE

👤 Community

💡 Research

INFO

Microsoft Windows SMB Service Detection

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Output

A CIFS server is running on this port.	
Port -	Hosts
445 / tcp / cifs	192.168.43.156

An SMB server is running on this port.	
Port -	Hosts
139 / tcp / smb	192.168.43.156

Plugin Details

Severity:	Info
ID:	11011
Version:	\$Revision: 1.39 \$
Type:	remote
Family:	Windows
Published:	June 5, 2002
Modified:	June 2, 2015

Risk Information

Risk Factor: None

FOLDERS

My Scans

All Scans

Trash

RESOURCES

★ Policies

🔧 Plugin Rules

🔍 Scanners

TENABLE

👤 Community

💡 Research

ktech-scanning / Plugin #10736

Configure

Hosts 1

Vulnerabilities 6

History 2

INFO

DCE Services Enumeration

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Output

```
The following DCE RPC services are available locally :  
Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91  
UUID : d98afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0  
Description : Unknown RPC service  
Type : Local RPC service  
Named pipe : WindowsShutdown  
  
Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91  
UUID : d98afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0  
MORE...
```

Plugin Details

Severity:	Info
ID:	10736
Version:	1.53
Type:	combined
Family:	Windows
Published:	August 26, 2001
Modified:	May 31, 2019

Risk Information

Risk Factor: None

