Assignment On N-map

Submitted To

Mr. Mohammad Zainal Abedin
Assistant Professor
Department of CSE, IIUC

Submitted By

Mohammad Forkan
Id: MC-231106

Objectives

The objectives of the network mapping assessment included:

- Identify open ports and services on the web server.
- Discover active hosts within the website's network.
- Assess the network topology to understand the overall architecture.
- Identify potential vulnerabilities that could pose security risks.

Nmap:

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Scanning Website: puc.ac.bd

Port address: 101.2.163.134

Scanned Features:

Types of Scan:

There are three types of scanning occurs

Ping Scan: During this scan Parallel DNS resolution is initiated and completed

SYN Stealth Scan: During this scanning various tcp open port are discovered such as 139/tcp,8080/tcp, 3306/tcp, 443/tcp, 3389/tcp etc.

Service scan : During this scanning 21 services on puc.ac.bd are scanned.

Nmap scan report for puc.ac.bd (101.2.163.134)

PORT	STATE	SERVICE	VERSION
25/tcp	filtered	smtp	
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
443/tcp	open	ssl/http	Microsoft IIS httpd 10.0
445/tcp	filtered	microsoft-ds	
1433/tcp	open	ms-sql-s	Microsoft SQLServer2014 12.00.2000RTM
3306/tcp	open	mysql	MySQL 8.0.32
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services
8010/tcp	open	http	Microsoft IIS httpd 10.0
8093/tcp	open	http	Microsoft IIS httpd 10.0

http-server-header: Microsoft-IIS/10.0

Public Key type: rsa

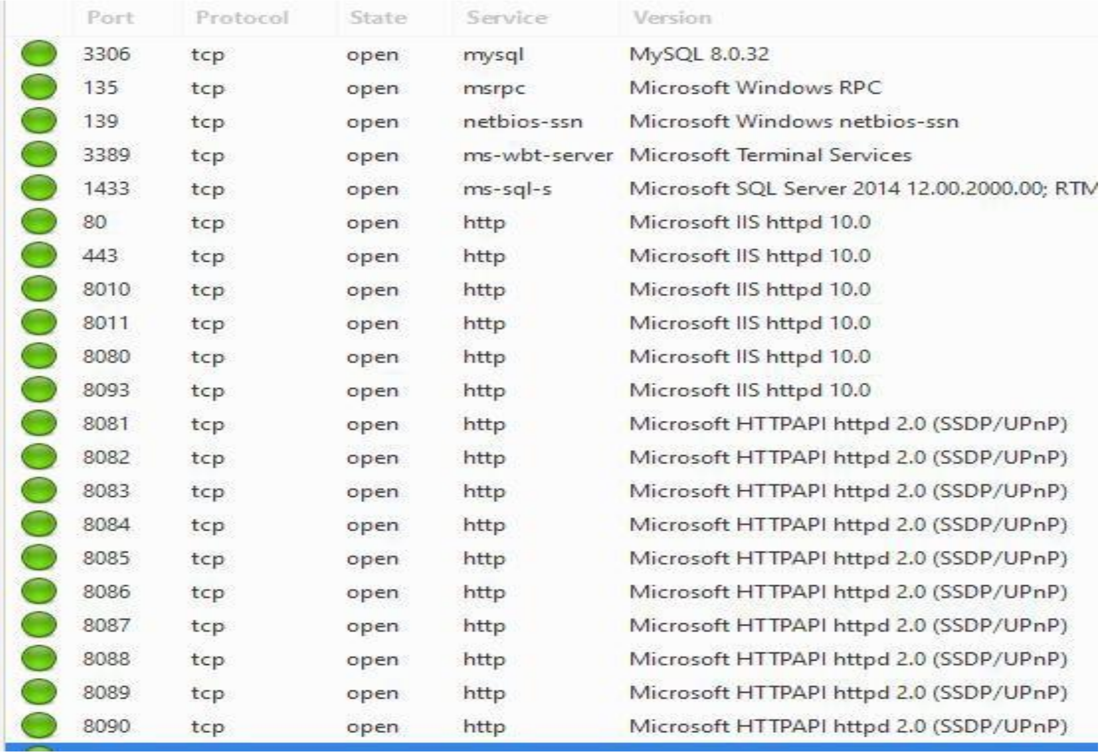
Public Key bits: 2048

Signature Algorithm: sha256WithRSAEncryption

Supported Methods: GET HEAD POST OPTIONS

http-title: Premier University | Center of Exellence for Quality Learning.

Discovered Port and Host:



	Port	Protocol	State	Service	Version
●	3306	tcp	open	mysql	MySQL 8.0.32
●	135	tcp	open	msrpc	Microsoft Windows RPC
●	139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
●	3389	tcp	open	ms-wbt-server	Microsoft Terminal Services
●	1433	tcp	open	ms-sql-s	Microsoft SQL Server 2014 12.00.2000.00; RTM
●	80	tcp	open	http	Microsoft IIS httpd 10.0
●	443	tcp	open	http	Microsoft IIS httpd 10.0
●	8010	tcp	open	http	Microsoft IIS httpd 10.0
●	8011	tcp	open	http	Microsoft IIS httpd 10.0
●	8080	tcp	open	http	Microsoft IIS httpd 10.0
●	8093	tcp	open	http	Microsoft IIS httpd 10.0
●	8081	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	8082	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	8083	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	8084	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	8085	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	8086	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	8087	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	8088	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	8089	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
●	8090	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Topology:

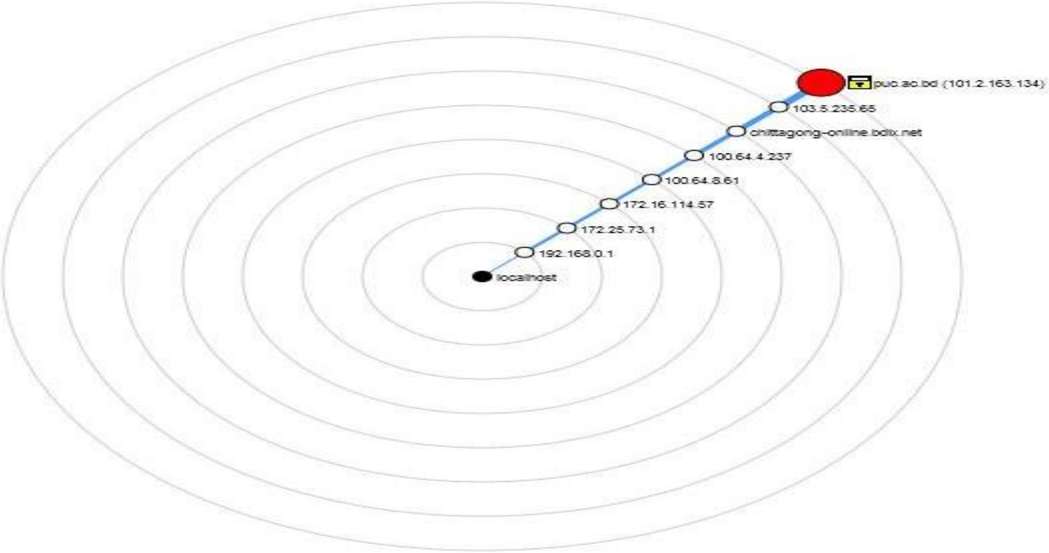


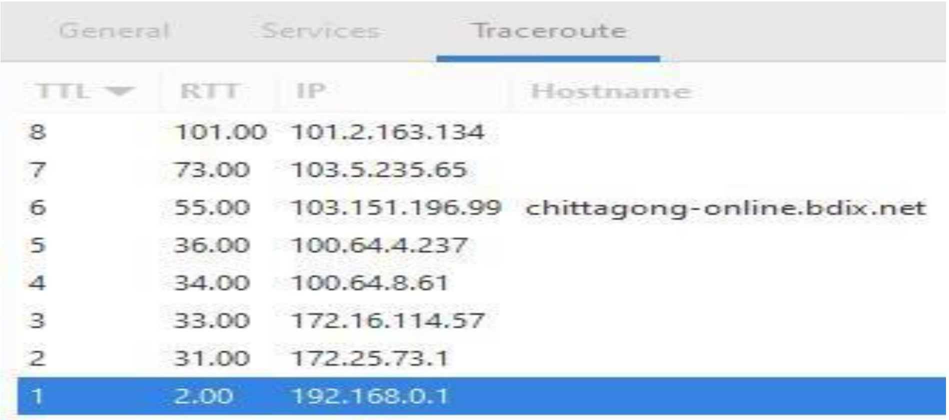
Fig: topological structure of puc.ac.bd

Host Details:

It provided services by 23 ports and 977 extra port

Used Ports in operating system: 80/tcp open

Traceroute:



TTL	RTT	IP	Hostname
8	101.00	101.2.163.134	
7	73.00	103.5.235.65	
6	55.00	103.151.196.99	chittagong-online.bdix.net
5	36.00	100.64.4.237	
4	34.00	100.64.8.61	
3	33.00	172.16.114.57	
2	31.00	172.25.73.1	
1	2.00	192.168.0.1	

Host status:

Open Port: 22

Filtered Port:1

Closed Port: 977

Scanned Port: 1000

Address:

IPV4: 101.2.163.134

IPV6: Not Available

MAC: Not Available

Host Names:

Name:puc.ac.bd

Types: User

TCP Sequences:

Difficulty:Good Luck

Index:260

Vulnerability Assessment:

No specific vulnerabilities were identified during the initial scan. Further analysis and targeted assessments may be needed for a comprehensive evaluation.

Conclusion

The initial network mapping assessment provides a snapshot of the current security state of puc.ac.bd.The purpose of this network mapping assessment on puc.ac.bd was to identify potential security vulnerabilities, map the network topology.There are three types of scanning occurred.Ping Scan , SYN Stealth Scan and service scan.It provided services by 23 ports and 977 extra port.