Network Scanning Report

Introduction

Network scanning is a fundamental aspect of security assessments, providing insights into network topology, open ports, and potential vulnerabilities. This report summarizes the results of various scanning techniques conducted on the target network.

Objective

The objective of these scans is to identify open ports, services running on those ports, and any potential security risks.

Scan Details

Scanned Host

- **IP Address**: 10.129.2.28

Scanned Ports

- **Port Range**: All ports

Scanning Tools Used

- Nmap (Network Mapper)

Results

Normal Output (.nmap)

```
# Nmap 7.80 scan initiated Tue Jun 16 12:14:53 2020 as: nmap -p- -oA target 10.129.2.28

Nmap scan report for 10.129.2.28

Host is up (0.053s latency).

Not shown: 4 closed ports

PORT   STATE SERVICE

22/tcp open  ssh
```

```
25/tcp open  smtp

80/tcp open  http

MAC Address: DE:AD:00:00:BE:EF (Intel Corporate)

# Nmap done at Tue Jun 16 12:15:03 2020 -- 1 IP address (1 host up)
scanned in 10.22 seconds
```

Grepable Output (.gnmap)

```
# Nmap 7.80 scan initiated Tue Jun 16 12:14:53 2020 as: nmap -p- -oA
target 10.129.2.28

Host: 10.129.2.28 ()  Status: Up

Host: 10.129.2.28 ()  Ports: 22/open/tcp//ssh///,
25/open/tcp//smtp///, 80/open/tcp//http///  Ignored State: closed
(4)

# Nmap done at Tue Jun 16 12:14:53 2020 -- 1 IP address (1 host up)
scanned in 10.22 seconds
```

XML Output (.xml)

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE nmaprun>

<?xml-stylesheet href="file:///usr/local/bin/../share/nmap/nmap.xsl"
type="text/xsl"?>

<!-- Nmap 7.80 scan initiated Tue Jun 16 12:14:53 2020 as: nmap -p-
-oA target 10.129.2.28 -->

<nmaprun scanner="nmap" args="nmap -p- -oA target 10.129.2.28"
start="12145301719" startstr="Tue Jun 16 12:15:03 2020"
version="7.80" xmloutputversion="1.04">

<scaninfo type="syn" protocol="tcp" numservices="65535"
services="1-65535"/>
```

```
<verbose level="0"/>

<debugging level="0"/>

<host starttime="12145301719" endtime="12150323493"><status
state="up" reason="arp-response" reason_ttl="0"/>

<address addr="10.129.2.28" addrtype="ipv4"/>

<address addr="DE:AD:00:00:BE:EF" addrtype="mac" vendor="Intel
Corporate"/>

<hostnames>

</hostnames>

<ports><extraports state="closed" count="4">

<extrareasons reason="resets" count="4"/>

</extraports>

<port protocol="tcp" portid="22"><state state="open"
reason="syn-ack" reason_ttl="64"/><service name="ssh" method="table"
conf="3"/></port>

<port protocol="tcp" portid="25"><state state="open"
reason="syn-ack" reason_ttl="64"/><service name="smtp"
method="table" conf="3"/></port>

<port protocol="tcp" portid="80"><state state="open"
reason="syn-ack" reason_ttl="64"/><service name="http"
method="table" conf="3"/></port>

</ports>

<times srtt="52614" rttvar="75640" to="355174"/>

</host>

<runstats><finished time="12150323493" timestr="Tue Jun 16 12:14:53
2020" elapsed="10.22" summary="Nmap done at Tue Jun 16 12:15:03
2020; 1 IP address (1 host up) scanned in 10.22 seconds"
exit="success"/><hosts up="1" down="0" total="1"/>

</runstats>
```

Conclusion

The network scan revealed the following open ports on the target:

- Port 22 (SSH)
- Port 25 (SMTP)
- Port 80 (HTTP)

Further analysis and vulnerability assessment are recommended based on these findings.

Additional Information

- **Full Report**: [Attached Files]
- **More information**: Nmap Output Documentation