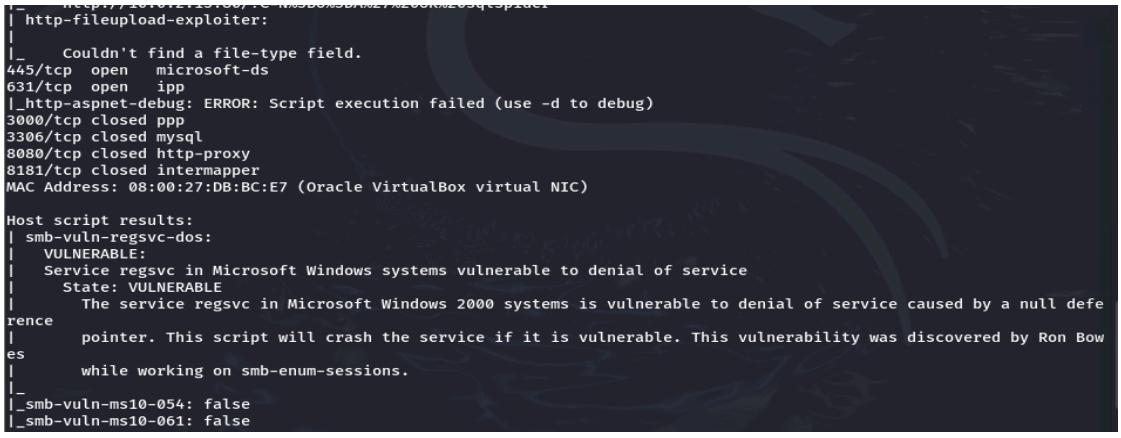
REPORT ON NETWORK VULNERABILITIES

OBJECTIVE:The purpose of this report is to assess the network security based on the provided screenshots and the tools used to identify vulnerabilities. This report includes vulnerabilities found using various tools like Nmap, Nikto, Wireshark, and Netcat,Zenmap,OpenVAS.

NMAP

Nmap is used for port scanning and os detection in this report by running the specific script
Like for scanning of local network use nmap and the targeted ip address
Use **nmap -o** for OS detection of the used by the target network

This screenshot shows the various operating system like LINUX
USE **{nmap -- script vuln}**



Above screenshot shows vulnerability to denial of service.

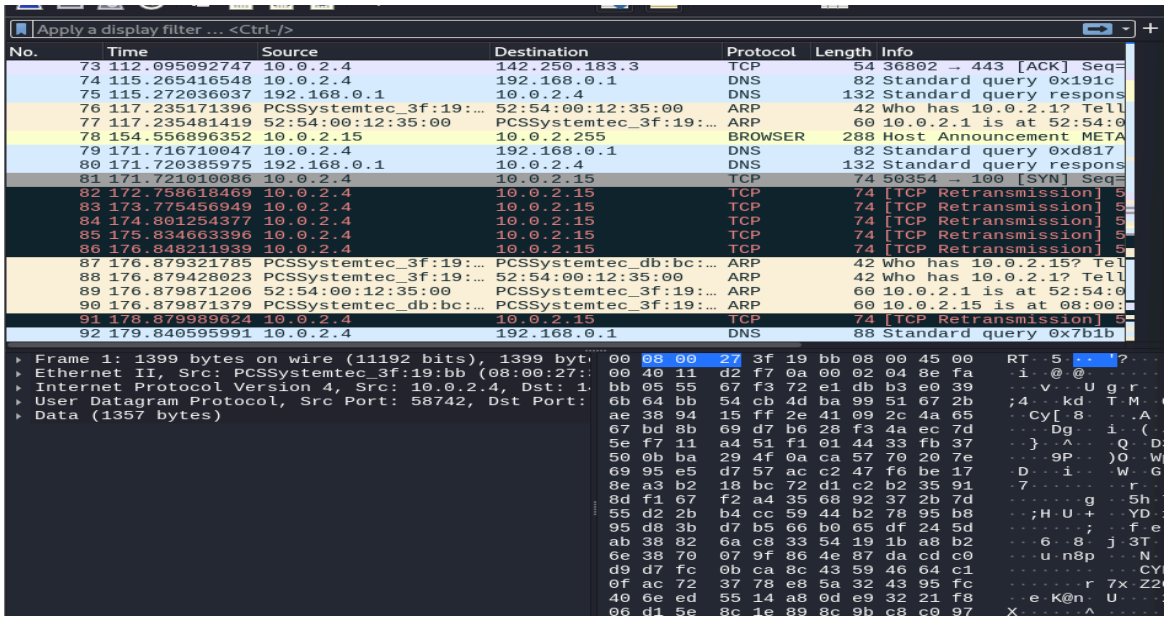
NETCAT

Netcat searches for open ports that are potential entry points for attacker.
Use **nc -zvu** with specify the port E.g 20-100

```
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
┌──(bora㉿kali)-[~]
└─$ nc -zvu 10.0.2.15 20-100
10.0.2.15: inverse host lookup failed: Unknown host
(UNKNOWN) [10.0.2.15] 100 (?) open
(UNKNOWN) [10.0.2.15] 99 (?) open
(UNKNOWN) [10.0.2.15] 98 (?) open
(UNKNOWN) [10.0.2.15] 97 (?) open
(UNKNOWN) [10.0.2.15] 96 (?) open
(UNKNOWN) [10.0.2.15] 95 (?) open
(UNKNOWN) [10.0.2.15] 94 (?) open
(UNKNOWN) [10.0.2.15] 93 (?) open
(UNKNOWN) [10.0.2.15] 92 (?) open
(UNKNOWN) [10.0.2.15] 91 (?) open
(UNKNOWN) [10.0.2.15] 90 (?) open
(UNKNOWN) [10.0.2.15] 89 (?) open
(UNKNOWN) [10.0.2.15] 88 (kerberos) open
```

Ports **20 (FTP)**, **21 (FTP)**, **22 (SSH)**, **80 (HTTP)**, and others between 20-100 were open.

WIRESHARK TRAFFIC ANALYSIS:



TCP Retransmissions: Multiple TCP retransmissions were noted between 10.0.2.4 and 10.0.2.15.Impact: This could indicate network performance issues or even Denial of Service (DoS) attacks.Suspicious UDP Traffic: UDP traffic from 10.0.2.4 to 10.0.2.15.Impact: Could be indicative of UDP flooding or misuse.

NIKTO WEB SERVER SCAN

```
+ Target IP:          10.0.2.15
+ Target Hostname:    10.0.2.15
+ Target Port:        80
+ Start Time:         2024-09-20 20:52:00 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/H
TTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mi
ssing-content-type-header/
+ /: Directory indexing found.
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x bran
ch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing.
+ //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ /%2e/: Directory indexing found.
+ /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfoc
us.com/bid/2513
+ ///: Directory indexing found.
+ /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show
all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.
cgi?name=CVE-1999-0269
+ /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show al
l files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cg
i?name=CVE-1999-0269
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.4.5.
+ /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized
 hosts.
+ ////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
///////////////////////: Directory indexing found.
+ ////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
///////////////////////: Abyss 1.03 reveals directory listing when multiple /'s are requested. See: http://cve.mitre.
org/cgi-bin/cvename.cgi?name=CVE-2002-1078
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to a
uthorized hosts.
+ /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized ho
sts. See: https://typo3.org/
+ 8911 requests: 0 error(s) and 22 item(s) reported on remote host
+ End Time:           2024-09-20 20:52:30 (GMT5.5) (30 seconds)
```

Nikto to scan a selected web server or application **nikto -h <target-IP or domain>**.
Identifies any outdated software, configuration issues, or potential vulnerabilities reported by Nikto.
Outdated Apache Version: Apache/2.4.18 is outdated (current is at least 2.4.54)
X-Frame-Options header is missing, making the site vulnerable to Clickjacking attacks
PHP Version: The web server is running PHP version 5.4.5, which is outdated.

Couldn't use openvas and zenmap due to the issue of it not being installed and showing some packet issue.

RECOMMENDATION

Patch and Update All Services:Upgrade Apache, PHP, and other outdated services to their latest versions to mitigate exposure to known vulnerabilities.

Patch and Update All Services:Upgrade Apache, PHP, and other outdated services to their latest versions to mitigate exposure to known vulnerabilities.

Secure ARP Traffic:Implement measures like static ARP entries or dynamic ARP inspection (DAI) to protect against ARP spoofing.

Implement Strong Authentication and Encryption:Enforce SSH authentication using public key cryptography.

Monitor for TCP Retransmissions and Unusual Traffic:Investigate any anomalies in the network such as TCP retransmissions, frequent ARP requests, and suspicious UDP traffic.

Report by
NIKITA VARMA
nikita.varma25@gmail.com