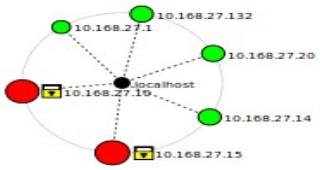
Scanning the Network with Nmap

```
Initiating SYN Stealth Scan at 17:46
Scanning 5 hosts [1000 ports/host]
Discovered open port 139/tcp on 10.168.27.15
Discovered open port 139/tcp on 10.168.27.10
Discovered open port 445/tcp on 10.168.27.15
Discovered open port 445/tcp on 10.168.27.10
Discovered open port 21/tcp on 10.168.27.15
Discovered open port 135/tcp on 10.168.27.10
Discovered open port 135/tcp on 10.168.27.15
Discovered open port 22/tcp on 10.168.27.20
Discovered open port 22/tcp on 10.168.27.14
Discovered open port 22/tcp on 10.168.27.132
Discovered open port 9090/tcp on 10.168.27.14
Discovered open port 9090/tcp on 10.168.27.132
Completed SYN Stealth Scan against 10.168.27.14 in 0.17s (4 hosts left)
Completed SYN Stealth Scan against 10.168.27.132 in 0.17s (3 hosts left)
Completed SYN Stealth Scan against 10.168.27.20 in 0.17s (2 hosts left)
Discovered open port 80/tcp on 10.168.27.15
Discovered open port 49154/tcp on 10.168.27.15
Discovered open port 49154/tcp on 10.168.27.10
Discovered open port 636/tcp on 10.168.27.10
Discovered open port 49155/tcp on 10.168.27.10
Discovered open port 13/tcp on 10.168.27.15
Discovered open port 49158/tcp on 10.168.27.15
Discovered open port 49161/tcp on 10.168.27.10
Discovered open port 389/tcp on 10.168.27.10
Discovered open port 17/tcp on 10.168.27.15
Discovered open port 19/tcp on 10.168.27.15
Discovered open port 49155/tcp on 10.168.27.15
Discovered open port 49157/tcp on 10.168.27.10
Discovered open port 7/tcp on 10.168.27.15
Discovered open port 49152/tcp on 10.168.27.10
Discovered open port 9/tcp on 10.168.27.15
Completed SYN Stealth Scan against 10.168.27.10 in 4.76s (1 host left)
Completed SYN Stealth Scan at 17:46, 4.98s elapsed (5000 total ports)
```

Zenmap Network Topology:



The network is using a logical star topology. The hosts connect back to a single point/router and are logically arranged in a star shape.

Summary of Vulnerabilities and Implications

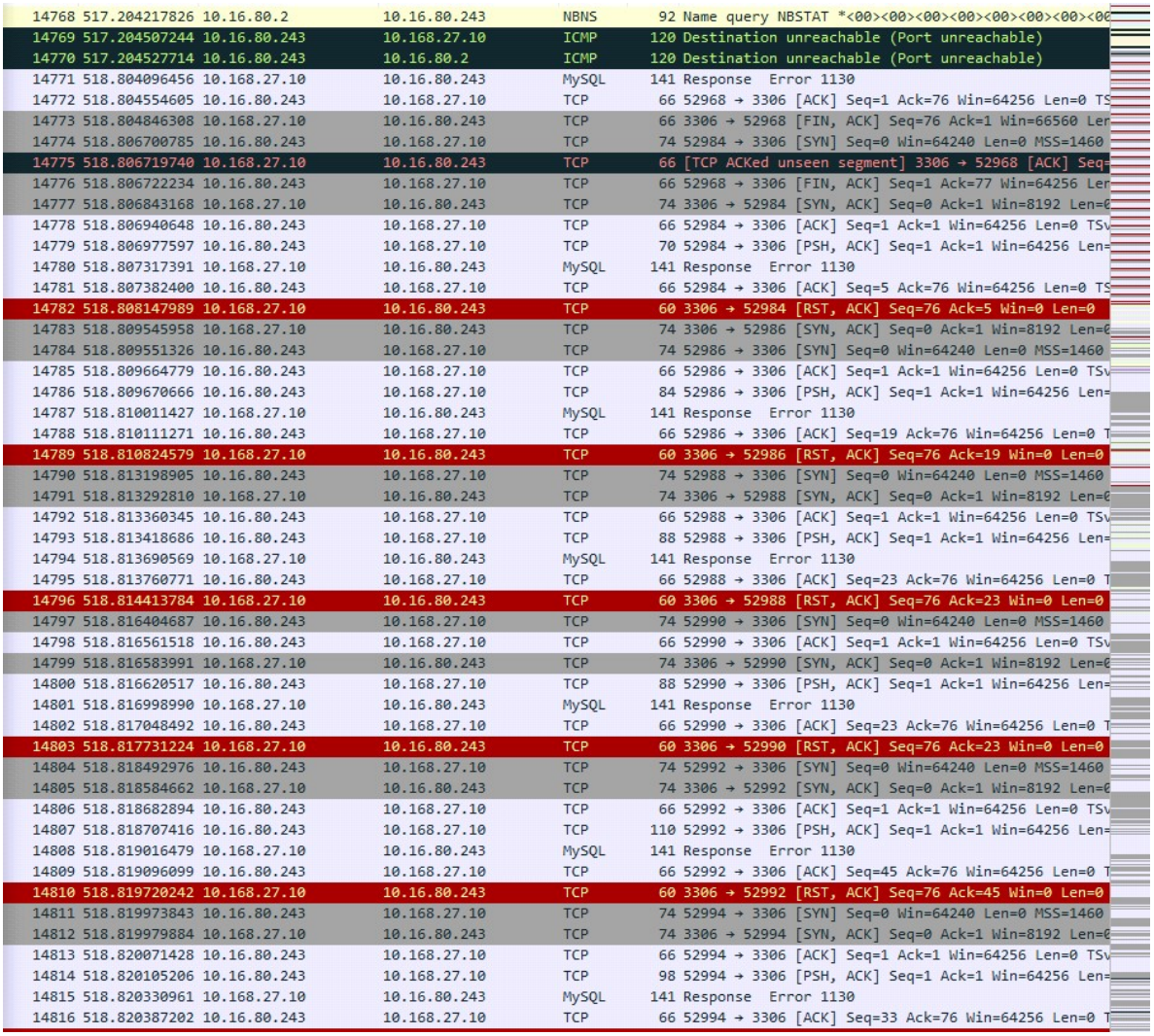
CVE-2017-0174(Windows NetBIOS of Service Vulnerability): The host computer 10.168.27.10 using Windows Server 2012 R2 allows a dos vulnerability because of improper handling of NetBIOS packets. Allowing the continued use of this version of windows server opens the network to a potential DOS attack where a hacker could leave this machine in a permanent DOS state. MITRE (2017).

CVE-2023-48795(Terrapin Attack): OpenSSH 9.6 and below is vulnerable. Two hosts are using versions of ssh that are vulnerable to this exploit (OpenSSH 5.5). This vulnerability allows attackers to bypass certain security checks by not sending certain packets involved in the handshake process. A client-server connection may end up with security features that are either downgraded or disabled. MITRE (2023).

CVE-2016-3213(WPAD Elevation of Privilege Vulnerability): Host 10.168.27.15 is using a version of windows 8 that is vulnerable to this type of attack. In this version of windows, the web proxy auto discovery protocol (WPAD) is vulnerable due to a failback mechanism that allows attackers to abuse NetBIOS name responses to bypass security and elevate their privileges. MITRE (2016).

Wireshark Anomalies

MySQL ERROR 1130 (PCAP1): A computer is trying to access a MySQL server that it cannot or should not connect to indicated by the error code 1130. (Packets 14700 - 219186)



14768	517.204217826	10.16.80.2	10.16.80.243	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00>
14769	517.204507244	10.16.80.243	10.168.27.10	ICMP	120 Destination unreachable (Port unreachable)
14770	517.204527714	10.16.80.243	10.16.80.2	ICMP	120 Destination unreachable (Port unreachable)
14771	518.804096456	10.168.27.10	10.16.80.243	MySQL	141 Response Error 1130
14772	518.804554605	10.16.80.243	10.168.27.10	TCP	66 52968 → 3306 [ACK] Seq=1 Ack=76 Win=64256 Len=0 TS
14773	518.804846308	10.168.27.10	10.16.80.243	TCP	66 3306 → 52968 [FIN, ACK] Seq=76 Ack=1 Win=66560 Len
14774	518.806700785	10.16.80.243	10.168.27.10	TCP	74 52984 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
14775	518.806719740	10.168.27.10	10.16.80.243	TCP	66 [TCP ACKed unseen segment] 3306 → 52968 [ACK] Seq=
14776	518.806722234	10.16.80.243	10.168.27.10	TCP	66 52968 → 3306 [FIN, ACK] Seq=1 Ack=77 Win=64256 Len
14777	518.806843168	10.168.27.10	10.16.80.243	TCP	74 3306 → 52984 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
14778	518.806940648	10.16.80.243	10.168.27.10	TCP	66 52984 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
14779	518.806977597	10.16.80.243	10.168.27.10	TCP	70 52984 → 3306 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=
14780	518.807317391	10.168.27.10	10.16.80.243	MySQL	141 Response Error 1130
14781	518.807382400	10.16.80.243	10.168.27.10	TCP	66 52984 → 3306 [ACK] Seq=5 Ack=76 Win=64256 Len=0 TS
14782	518.808147989	10.168.27.10	10.16.80.243	TCP	60 3306 → 52984 [RST, ACK] Seq=76 Ack=5 Win=0 Len=0
14783	518.809545958	10.168.27.10	10.16.80.243	TCP	74 3306 → 52986 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
14784	518.809551326	10.16.80.243	10.168.27.10	TCP	74 52986 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
14785	518.809664779	10.16.80.243	10.168.27.10	TCP	66 52986 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
14786	518.809670666	10.16.80.243	10.168.27.10	TCP	84 52986 → 3306 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=
14787	518.810011427	10.168.27.10	10.16.80.243	MySQL	141 Response Error 1130
14788	518.810111271	10.16.80.243	10.168.27.10	TCP	66 52986 → 3306 [ACK] Seq=19 Ack=76 Win=64256 Len=0 T
14789	518.810824579	10.168.27.10	10.16.80.243	TCP	60 3306 → 52986 [RST, ACK] Seq=76 Ack=19 Win=0 Len=0
14790	518.813198905	10.16.80.243	10.168.27.10	TCP	74 52988 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
14791	518.813292810	10.168.27.10	10.16.80.243	TCP	74 3306 → 52988 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
14792	518.813360345	10.16.80.243	10.168.27.10	TCP	66 52988 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
14793	518.813418686	10.16.80.243	10.168.27.10	TCP	88 52988 → 3306 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=
14794	518.813690569	10.168.27.10	10.16.80.243	MySQL	141 Response Error 1130
14795	518.813760771	10.16.80.243	10.168.27.10	TCP	66 52988 → 3306 [ACK] Seq=23 Ack=76 Win=64256 Len=0 T
14796	518.814413784	10.168.27.10	10.16.80.243	TCP	60 3306 → 52988 [RST, ACK] Seq=76 Ack=23 Win=0 Len=0
14797	518.816404687	10.16.80.243	10.168.27.10	TCP	74 52990 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
14798	518.816561518	10.16.80.243	10.168.27.10	TCP	66 52990 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
14799	518.816583991	10.168.27.10	10.16.80.243	TCP	74 3306 → 52990 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
14800	518.816620517	10.16.80.243	10.168.27.10	TCP	88 52990 → 3306 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=
14801	518.816998990	10.168.27.10	10.16.80.243	MySQL	141 Response Error 1130
14802	518.817048492	10.16.80.243	10.168.27.10	TCP	66 52990 → 3306 [ACK] Seq=23 Ack=76 Win=64256 Len=0 T
14803	518.817731224	10.168.27.10	10.16.80.243	TCP	60 3306 → 52990 [RST, ACK] Seq=76 Ack=23 Win=0 Len=0
14804	518.818492976	10.16.80.243	10.168.27.10	TCP	74 52992 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
14805	518.818584662	10.168.27.10	10.16.80.243	TCP	74 3306 → 52992 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
14806	518.818682894	10.16.80.243	10.168.27.10	TCP	66 52992 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
14807	518.818707416	10.16.80.243	10.168.27.10	TCP	110 52992 → 3306 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=
14808	518.819016479	10.168.27.10	10.16.80.243	MySQL	141 Response Error 1130
14809	518.819096099	10.16.80.243	10.168.27.10	TCP	66 52992 → 3306 [ACK] Seq=45 Ack=76 Win=64256 Len=0 T
14810	518.819720242	10.168.27.10	10.16.80.243	TCP	60 3306 → 52992 [RST, ACK] Seq=76 Ack=45 Win=0 Len=0
14811	518.819973843	10.16.80.243	10.168.27.10	TCP	74 52994 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
14812	518.819979884	10.168.27.10	10.16.80.243	TCP	74 3306 → 52994 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
14813	518.820071428	10.16.80.243	10.168.27.10	TCP	66 52994 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
14814	518.820105206	10.16.80.243	10.168.27.10	TCP	98 52994 → 3306 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=
14815	518.820330961	10.168.27.10	10.16.80.243	MySQL	141 Response Error 1130
14816	518.820387202	10.16.80.243	10.168.27.10	TCP	66 52994 → 3306 [ACK] Seq=33 Ack=76 Win=64256 Len=0 T

Plain Text HTTP Requests (PCAP1): Some http traffic in pcap1 is unencrypted. This could lead to someone snooping and being able to see passwords and other sensitive information. (Packets 21928-21923)

```
219280 1886.7637435… 10.168.27.10   10.16.80.243    TCP      74 80 → 43910 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=
219281 1886.7637846… 10.16.80.243   10.168.27.10    TCP      66 43910 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
219282 1886.7640076… 10.16.80.243   10.168.27.10    HTTP    182 POST /example?p1=p1val&p2=p2val HTTP/1.0
219283 1886.7652795… 10.168.27.10   10.16.80.243    HTTP    567 HTTP/1.1 404 Not Found  (text/html)
219284 1886.7653655… 10.16.80.243   10.168.27.10    TCP      66 43910 → 80 [ACK] Seq=117 Ack=502 Win=64128 Len=
219285 1886.7654034… 10.168.27.10   10.16.80.243    TCP      66 80 → 43910 [FIN, ACK] Seq=502 Ack=117 Win=66560
219286 1886.7662494… 10.16.80.243   10.168.27.10    TCP      66 43910 → 80 [FIN, ACK] Seq=117 Ack=503 Win=64128
219287 1886.7663047… 10.168.27.10   10.16.80.243    TCP      66 80 → 43910 [ACK] Seq=503 Ack=118 Win=66560 Len=
```

DDOS/ Multiple Same HTTP Requests (PCAP2): Pcap2 shows evidence of DOS/DDOS by http request.

```
10.16.80.243    10.168.27.10    HTTP     485 GET /dvwa/login.php HTTP/1.1
10.168.27.10    10.16.80.243    HTTP    1800 HTTP/1.1 200 OK  (text/html)
10.168.27.10    10.16.80.243    TCP       66 80 → 44054 [FIN, ACK] Seq=1735
10.16.80.243    10.168.27.10    TCP       66 44054 → 80 [ACK] Seq=420 Ack=14
10.16.80.243    10.168.27.10    TCP       66 44054 → 80 [ACK] Seq=420 Ack=17
10.16.80.243    10.168.27.10    TCP       66 44054 → 80 [FIN, ACK] Seq=420 A
10.168.27.10    10.16.80.243    TCP       66 80 → 44054 [ACK] Seq=1736 Ack=4
10.16.80.243    10.168.27.10    TCP       74 44056 → 80 [SYN] Seq=0 Win=6424
10.168.27.10    10.16.80.243    TCP       74 80 → 44056 [SYN, ACK] Seq=0 Ack
10.16.80.243    10.168.27.10    TCP       66 44056 → 80 [ACK] Seq=1 Ack=1 Wi
10.16.80.243    10.168.27.10    HTTP     479 GET /dvwa/login.php HTTP/1.1
10.168.27.10    10.16.80.243    HTTP    1911 HTTP/1.1 200 OK  (text/html)
10.168.27.10    10.16.80.243    TCP       66 80 → 44056 [FIN, ACK] Seq=1846
10.16.80.243    10.168.27.10    TCP       66 44056 → 80 [ACK] Seq=414 Ack=14
10.16.80.243    10.168.27.10    TCP       66 44056 → 80 [ACK] Seq=414 Ack=18
10.16.80.243    10.168.27.10    TCP       66 44056 → 80 [FIN, ACK] Seq=414 A
10.168.27.10    10.16.80.243    TCP       66 80 → 44056 [ACK] Seq=1847 Ack=4
10.16.80.243    10.168.27.10    TCP       74 44058 → 80 [SYN] Seq=0 Win=6424
10.168.27.10    10.16.80.243    TCP       74 80 → 44058 [SYN, ACK] Seq=0 Ack
10.16.80.243    10.168.27.10    TCP       66 44058 → 80 [ACK] Seq=1 Ack=1 Wi
10.16.80.243    10.168.27.10    HTTP     479 GET /dvwa/login.php HTTP/1.1
10.168.27.10    10.16.80.243    HTTP    1911 HTTP/1.1 200 OK  (text/html)
10.168.27.10    10.16.80.243    TCP       66 80 → 44058 [FIN, ACK] Seq=1846
10.16.80.243    10.168.27.10    TCP       66 44058 → 80 [ACK] Seq=414 Ack=14
10.16.80.243    10.168.27.10    TCP       66 44058 → 80 [ACK] Seq=414 Ack=18
```

Shown here we have GET requests followed by an OK Response. This suggests to me that someone is continually sending a GET request to slow down the receiving webserver. (Packet 1500-2000)

Brute force Logon Attempts (PCAP3): Someone is attempting to brute force login to the server as evidence I have screen captures of multiple login attempts with different password values. This html was taken from the http response sent from the web server. This behavior spans from the start of the PCAP at packet 1 and continues until packet 12000+

```
</html>POST /dvwa/login.php HTTP/1.1
Host: 10.168.27.10
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Wfuzz/2.4.5
Content-Length: 27

log=admin@example.com&pwd=3HTTP/1.1 200 OK
Date: Tue, 14 Sep 2021 03:04:15 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1l PHP/8.0.10
X-Powered-By: PHP/8.0.10
Set-Cookie: PHPSESSID=7r5kerjh185ovjiqjgj5a18jd1; path=/
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=7r5kerjh185ovjiqjgj5a18jd1; path=/; HttpOnly
Set-Cookie: security=impossible; HttpOnly
Content-Length: 1415
Content-Type: text/html;charset=utf-8
```

Here the pwd value has been changed to "access granted".

```
</html>POST /dvwa/login.php HTTP/1.1
Host: 10.168.27.10
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Wfuzz/2.4.5
Content-Length: 39

log=admin@example.com&pwd=accessgrantedHTTP/1.1 200 OK
Date: Tue, 14 Sep 2021 03:04:27 GMT
```

Plaintext HTTP PCAP3: The http requests in pcap3 are unencrypted. This leaves passwords and usernames open to sniffing/packet capture. Above you can see that the traffic is unencrypted.

RST/ACK DOS PCAP4: RST/ACK packets are being sent at an alarming rate. Sending these in succession will cause the server to slow due to the RST packets resetting the handshake process before it is completed causing unnecessary system usage.

16	2.150758909	10.168.27.10	10.16.80.243	TCP	60 5900 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
17	2.150760667	10.168.27.10	10.16.80.243	TCP	60 256 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
18	2.150760817	10.168.27.10	10.16.80.243	TCP	60 143 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
19	2.150762602	10.168.27.10	10.16.80.243	TCP	60 21 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
20	2.150762033	10.168.27.10	10.16.80.243	TCP	60 3389 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
21	2.150768379	10.168.27.10	10.16.80.243	TCP	60 1025 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
22	2.150817200	10.168.27.10	10.16.80.243	TCP	60 587 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
23	2.150852165	10.168.27.10	10.16.80.243	TCP	60 1723 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
24	2.150907340	10.168.27.10	10.16.80.243	TCP	60 53 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
25	2.150973148	10.168.27.10	10.16.80.243	TCP	60 139 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
26	2.150992683	10.16.80.243	10.168.27.10	TCP	60 33701 → 110 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
27	2.151040029	10.16.80.243	10.168.27.10	TCP	60 33701 → 995 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
28	2.151042162	10.16.80.243	10.168.27.10	TCP	60 33701 → 554 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
29	2.151057399	10.168.27.10	10.16.80.243	TCP	60 110 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
30	2.151059075	10.16.80.243	10.168.27.10	TCP	60 33701 → 199 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
31	2.151107976	10.168.27.10	10.16.80.243	TCP	60 995 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
32	2.151121967	10.16.80.243	10.168.27.10	TCP	60 33701 → 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
33	2.151166758	10.16.80.243	10.168.27.10	TCP	60 33701 → 3306 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
34	2.151171903	10.168.27.10	10.16.80.243	TCP	60 554 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
35	2.151173802	10.168.27.10	10.16.80.243	TCP	60 199 → 33701 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

Implications of Wireshark Anomalies

(PCAP1 Implications): The host in question will not be able to communicate with the MySQL server. Traffic between the server may be intercepted and read due to the lack of encryption.

(PCAP2 Implications): If no action is taken to remediate the DOS attack the server will slow down and system usage and requirements will be used up / exhausted.

(PCAP3 Implications): Here action needs to be taken to stop the brute force login attempts. If no action is taken user accounts, usernames, and passwords may end up compromised. HTTP traffic needs to be encrypted to stop sensitive data being intercepted by attackers.

(PCAP4 Implications): If no action is taken to stop the dos attack system resources will end up diminished then exhausted.

Recommended Actions Taken

CVE-2017-0174(Windows NetBIOS of Service Vulnerability)

One solution to this vulnerability is to block TCP port 139 on the firewall. Doing so will help block attempted exploiters from attacking hosts that are behind the firewall. However, this may impact other services that use TCP port 139 so using an updated version of windows server may be advisable. Microsoft (2017).

CVE-2023-48795(Terrapin Attack):

Suggested action to remedy this vulnerability would be to update the version of OpenSSH to one that supports strict key-exchange. Strict key-exchange ensures that an attacker cannot inject packets into the handshake process by changing the SSH handshake in a way that is not backwards compatible. Bäumer, F., Brinkmann, M., & Schwenk, J. (2023).

CVE-2016-3213(WPAD Elevation of Privilege Vulnerability):

Microsoft's solution to this vulnerability was released as a patch to the WPAD protocol. Patching this protocol to an updated version should mitigate the risk of attack. Microsoft (2023).

MySQL ERROR 1130 (PCAP1):

The admin must connect to the MySQL server and allow access privileges to the Host in question. Kumar (2023).

HTTP GET DOS (PCAP2):

Adding a challenge or security question can help stop unsophisticated DOS attempts. Another solution would be to block the offending IP address via a firewall. Cloudflare (n.d.).

Brute force Login Attempts (PCAP3):

Locking out accounts after a certain number of failed attempts should help stop this issue. This helps by stopping the login process entirely after a certain number of attempts has been reached. Esheridan (n.d.).

Lack of Encryption / Plaintext HTTP (PCAP1, PCAP3): The lack of encryption can be fixed by installing an SSL certificate on the webserver. This will encrypt the traffic so that plain text will not be displayed if someone is intercepting the traffic. Cloudflare (n.d.).

RST/ACK DOS (PCAP4):

This type of attack is commonly mitigated by assigning a cookie to the RST packets on the network so that the receiving host can differentiate between valid and non-valid RST packets. Beschokov (2021).

References

Bäumer, F., Brinkmann, M., & Schwenk, J. (2023). Terrapin attack. Terrapin Attack. https://terrapin-attack.com/

Beschokov, M. (2021, May 19). What is TCP Reset Attack (RST)? https://www.wallarm.com/what/what-is-syn-spoofing-or-tcp-reset-attack

Cloudflare. (n.d.). HTTP flood attack. HTTP flood ddos attack | cloudflare. https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/

Cloudflare. (n.d.). What is an SSL certificate? | how to get a free SSL certificate ... https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/

Esheridan. (n.d.). Blocking brute force attacks. Blocking Brute Force Attacks | OWASP Foundation. https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

Kumar, R. (2023, September 23). (fixed) error 1130 (HY000): Host is not allowed to connect to this mysql server. TecAdmin. https://tecadmin.net/error-1130-hy000-host-is-not-allowed-to-connect-to-this-mysql-server/

Microsoft. (2017, August 8). Windows NetBIOS Denial of Service Vulnerability. Security Update Guide - Microsoft Security Response Center. https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0174

Microsoft. (2023, January 3). Microsoft Security bulletin MS16-077 - important. Microsoft Learn. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-077

MITRE. (2016). CVE-2016-3213. CVE. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3213

MITRE. (2017). CVE-2017-0174. CVE. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0174

MITRE. (2023). CVE-2023-48795. CVE. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-48795