

TASK-1

No.	Time	Source	Destination	Protocol	Length	Info
3753	35.484932	192.168.1.215	192.168.1.251	HTTP/X	756	POST /ctl/IPConn HTTP/1.1
3755	35.488944	192.168.1.251	192.168.1.215	HTTP/X	716	HTTP/1.1 200 OK
3763	35.490997	192.168.1.215	192.168.1.251	HTTP/X	947	POST /ctl/IPConn HTTP/1.1
3765	35.571804	192.168.1.251	192.168.1.215	HTTP/X	444	HTTP/1.1 200 OK
3772	35.756506	192.168.1.215	44.228.249.3	HTTP	500	GET / HTTP/1.1
3793	36.083780	44.228.249.3	192.168.1.215	HTTP	1157	HTTP/1.1 200 OK (text/html)
3795	36.107832	192.168.1.215	44.228.249.3	HTTP	400	GET /style.css HTTP/1.1
3796	36.113914	192.168.1.215	44.228.249.3	HTTP	452	GET /images/logo.gif HTTP/1.1
3805	36.492971	44.228.249.3	192.168.1.215	HTTP	1160	HTTP/1.1 200 OK (text/css)
3814	36.496345	44.228.249.3	192.168.1.215	HTTP	878	HTTP/1.1 200 OK (GIF89a)
3867	40.228195	192.168.1.215	44.228.249.3	HTTP	547	GET /login.php HTTP/1.1
3888	40.589008	44.228.249.3	192.168.1.215	HTTP	1346	HTTP/1.1 200 OK (text/html)
3982	44.071381	192.168.1.215	192.168.1.251	HTTP	252	GET /rootDesc.xml HTTP/1.1
3985	44.076652	192.168.1.251	192.168.1.215	HTTP/X	1314	HTTP/1.1 200 OK
4024	46.009777	192.168.1.215	44.228.249.3	HTTP	716	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
4082	46.016108	44.228.249.3	192.168.1.215	HTTP	98	HTTP/1.1 200 OK (text/html)
4088	46.020144	192.168.1.215	192.168.1.251	HTTP	252	GET /rootDesc.xml HTTP/1.1
4091	46.023598	192.168.1.251	192.168.1.215	HTTP/X	1314	HTTP/1.1 200 OK
4408	58.916215	192.168.1.215	44.228.249.3	HTTP	587	GET /logout.php HTTP/1.1
4494	59.225836	44.228.249.3	192.168.1.215	HTTP	1176	HTTP/1.1 200 OK (text/html)
Frame 4024: 711 bytes on wire (5688 bits), 711 bytes captured (5688 bits) on interface \Device\NPF_{4C2039...}						
Ethernet II, Src: IntelAc:11:4d:38:05:05:4c:11:4d, Dst: BelkinIntern:cd:44:28 (cd:41:1e:cd:44:28)						
Internet Protocol Version 4, Src: 192.168.1.215, Dst: 44.228.249.3						
Transmission Control Protocol, Src Port: 80, Seq: 892, Ack: 9649, Len: 657						
Hypertext Transfer Protocol						
POST /userinfo.php HTTP/1.1\r\n						
Request Method: POST						
Request URI: /userinfo.php						
Request Version: HTTP/1.1						
Host: testphp.vulnweb.com\r\n						
Connection: keep-alive\r\n						
Content-Length: 20\r\n						
[Content Length: 20]						
Cache-Control: max-age=0\r\n						
Origin: http://testphp.vulnweb.com\r\n						
Content-Type: application/x-www-form-urlencoded\r\n						
Upgrade-Insecure-Requests: 1\r\n						
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36\r\n						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8\r\n						
Referer: http://testphp.vulnweb.com/login.php\r\n						
Accept-Charset: gzip, deflate\r\n						

TASK-2

Large numbers of SYN packets were detected from different IP addresses without corresponding SYN+ACK replies.

Filter: tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
16068	0.425906	176.232.188.214	10.10.10.10	TCP	60	12608 → 25565 [SYN] Seq=0 Win=0 Len=0
16067	0.425906	139.111.37.67	10.10.10.10	TCP	60	26545 → 25565 [SYN] Seq=0 Win=0 Len=0
16066	0.425905	114.153.32.195	10.10.10.10	TCP	60	20886 → 25565 [SYN] Seq=0 Win=0 Len=0
16065	0.425904	185.26.176.87	10.10.10.10	TCP	60	46903 → 25565 [SYN] Seq=0 Win=0 Len=0
16064	0.425838	79.162.213.102	10.10.10.10	TCP	60	9422 → 25565 [SYN] Seq=0 Win=0 Len=0
16063	0.425837	74.246.255.66	10.10.10.10	TCP	60	56267 → 25565 [SYN] Seq=0 Win=0 Len=0
16062	0.425837	66.207.81.213	10.10.10.10	TCP	60	9537 → 25565 [SYN] Seq=0 Win=0 Len=0
16061	0.425836	66.129.151.94	10.10.10.10	TCP	60	40422 → 25565 [SYN] Seq=0 Win=0 Len=0
16060	0.425835	84.102.177.109	10.10.10.10	TCP	60	5682 → 25565 [SYN] Seq=0 Win=0 Len=0
16059	0.425835	1.4.242.252	10.10.10.10	TCP	60	59176 → 25565 [SYN] Seq=0 Win=0 Len=0
16058	0.425767	61.125.211.155	10.10.10.10	TCP	60	40936 → 25565 [SYN] Seq=0 Win=0 Len=0
16057	0.425767	183.59.70.124	10.10.10.10	TCP	60	63877 → 25565 [SYN] Seq=0 Win=0 Len=0
16056	0.425766	15.213.165.43	10.10.10.10	TCP	60	38085 → 25565 [SYN] Seq=0 Win=0 Len=0
16055	0.425766	69.42.177.232	10.10.10.10	TCP	60	63007 → 25565 [SYN] Seq=0 Win=0 Len=0
16054	0.425687	113.182.96.184	10.10.10.10	TCP	60	23431 → 25565 [SYN] Seq=0 Win=0 Len=0
16053	0.425686	50.42.102.236	10.10.10.10	TCP	60	46007 → 25565 [SYN] Seq=0 Win=0 Len=0
16052	0.425686	29.31.136.80	10.10.10.10	TCP	60	53393 → 25565 [SYN] Seq=0 Win=0 Len=0
16051	0.425685	58.206.27.214	10.10.10.10	TCP	60	61968 → 25565 [SYN] Seq=0 Win=0 Len=0
16050	0.425685	93.101.7.77	10.10.10.10	TCP	60	41226 → 25565 [SYN] Seq=0 Win=0 Len=0
16049	0.425684	135.104.243.250	10.10.10.10	TCP	60	22412 → 25565 [SYN] Seq=0 Win=0 Len=0

TCP anomalies- TCP Retransmission

Filter: tcp.analysis.flags && !(tcp.flags.reset==1)

No.	Time	Source	Destination	Protocol	Length	Info
9960	0.344689	49.148.158.181	10.10.10.10	TCP	60	[TCP Retransmission] 22187 → 25565 [SYN] Seq=0 Win=0 Len=0
6069	0.291089	147.133.37.166	10.10.10.10	TCP	60	[TCP Retransmission] 16455 → 25565 [SYN] Seq=0 Win=0 Len=0
6313	0.285523	190.39.190.290	10.10.10.10	TCP	60	[TCP Retransmission] 61908 → 25565 [SYN] Seq=0 Win=0 Len=0
6289	0.284966	148.187.5.173	10.10.10.10	TCP	60	[TCP Retransmission] 32406 → 25565 [SYN] Seq=0 Win=0 Len=0
6152	0.282562	156.40.157.255	10.10.10.10	TCP	60	[TCP Retransmission] 6305 → 25565 [SYN] Seq=0 Win=0 Len=0
6075	0.281035	1.88.75.218	10.10.10.10	TCP	60	[TCP Retransmission] 6869 → 25565 [SYN] Seq=0 Win=0 Len=0
5882	0.277555	37.93.252.147	10.10.10.10	TCP	60	[TCP Retransmission] 29231 → 25565 [SYN] Seq=0 Win=0 Len=0
5828	0.276671	191.164.207.33	10.10.10.10	TCP	60	[TCP Retransmission] 43149 → 25565 [SYN] Seq=0 Win=0 Len=0
5709	0.274997	65.84.125.16	10.10.10.10	TCP	60	[TCP Retransmission] 28148 → 25565 [SYN] Seq=0 Win=0 Len=0
5357	0.267681	129.135.168.185	10.10.10.10	TCP	60	[TCP Retransmission] 56131 → 25565 [SYN] Seq=0 Win=0 Len=0
5231	0.265446	28.174.107.112	10.10.10.10	TCP	60	[TCP Retransmission] 37009 → 25565 [SYN] Seq=0 Win=0 Len=0
5161	0.263922	141.109.21.24	10.10.10.10	TCP	60	[TCP Retransmission] 21073 → 25565 [SYN] Seq=0 Win=0 Len=0
5146	0.263656	20.234.24.206	10.10.10.10	TCP	60	[TCP Retransmission] 25134 → 25565 [SYN] Seq=0 Win=0 Len=0
4996	0.260702	55.151.182.161	10.10.10.10	TCP	60	[TCP Retransmission] 25041 → 25565 [SYN] Seq=0 Win=0 Len=0
4914	0.258868	61.136.185.224	10.10.10.10	TCP	60	[TCP Retransmission] 50149 → 25565 [SYN] Seq=0 Win=0 Len=0
4563	0.252737	166.227.141.98	10.10.10.10	TCP	60	[TCP Retransmission] 49709 → 25565 [SYN] Seq=0 Win=0 Len=0
4294	0.247175	111.96.198.244	10.10.10.10	TCP	60	[TCP Retransmission] 5414 → 25565 [SYN] Seq=0 Win=0 Len=0
4080	0.242601	114.240.163.131	10.10.10.10	TCP	60	[TCP Retransmission] 32485 → 25565 [SYN] Seq=0 Win=0 Len=0
4070	0.242389	14.73.168.240	10.10.10.10	TCP	60	[TCP Retransmission] 16155 → 25565 [SYN] Seq=0 Win=0 Len=0
4017	0.241194	112.67.114.50	10.10.10.10	TCP	60	[TCP Retransmission] 13057 → 25565 [SYN] Seq=0 Win=0 Len=0

CONCLUSION: Detected possible all the SYN packets are from **different source IPs**, so it' s a **distributed SYN flood** (DDoS) or scanning activity using spoofed source addresses.