***Syn-Flood Attack Detection and Prevention***

**Abstract**

**A DDOS attack that targets a vulnerability in TCP connection (i.e. 3-way hand shake) to overload the resources of a target sever or website. It thus prevents legitimate host from connecting to the server or in some cases may takedown the server or website.**

**syn flood attack is a type of DDOS attack in which a hostile host sends many simultaneous syn packets from various fake IPs or from bot networks.**

**The server in response sends syn-ack packets to those fake IPs. However, the fake IPs don’t respond, leaving the connection incomplete (half open connection). Such connections exhaust resources on sever thus prevents other legitimate hosts from connecting.**

**In this project, our team will demonstrate the above mentioned syn flood attacks and detect it on the victim’s machine using Wireshark.**

**We will also study prevention methods and implement them.**

**Key words**

**1 DDOS attack-** **DDoS is short for Distributed Denial of Service. DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.**

**2 TCP/IP- IP is the network layer protocol that acts as a packet delivery service. TCP enables reliable delivery of data packets in order without any repetition and errors.**

**3 Three way handshake­-The method used in TCP/IP network to create connection between client and server where a three-step method that requires both the client and server to exchange SYN and ACK (acknowledgment) packets before actual data communication begins is used**

**4 syn-ack packets-SYNchronize and ACKnowledge messages are indicated by a either the SYN bit, or the ACK bit inside the TCP header, and the SYN-ACK message has both the SYN and the ACK bits turned on (set to 1) in the TCP header.**

**5 Half open connections-** **The term half-open refers to TCP connections whose state is out of synchronization between the two communicating hosts, possibly due to a crash of one side**

**6 SYN flood attack- A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.**

**Introduction**

**Denial of Service attacks**

**In these attacks, the main aim of the attacker is to stop the victim’s machine from doing it’s required job. Thus, the server is unable to provide its service to the legitimate clients. The damage done by these attacks can vary from a minor inconvenience to major financial losses. Some companies like ebay, amazon etc depend on the online services for their business. If their websites are attacked, it affects their transactions and they lose millions of dollars. The attacks are broadly classified into three major categories:**

**1) Bandwidth Consumption: All available bandwidth is used by the attacker leaving no bandwidth for the actual clients. E.g., ICMP ECHO attack**

**2) Other Resource consumption: In this type of attack, resources like web server, print or mail server if flooded with useless requests, prevent the actual serving software from handling the traffic. E.g., mail bomb**

**3) Network Connectivity: The attacker forces the server to stop communicating on the network.**

**E.g., SYN Flooding. [2]**

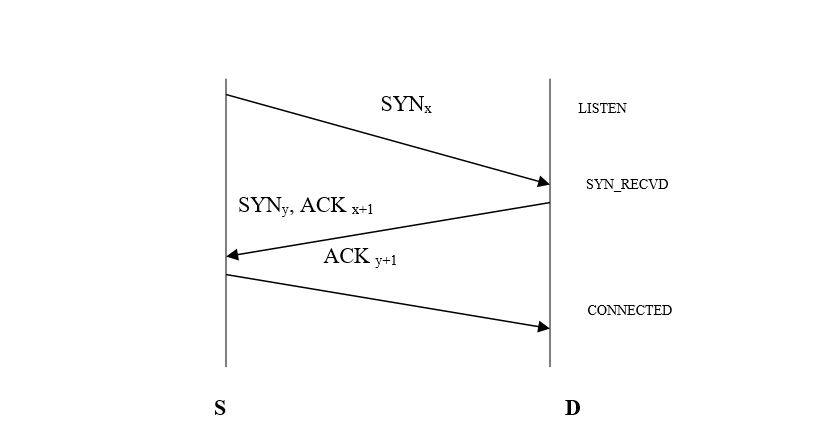
**SYN Flooding attack is one of the most common network-based denial of service attack that exploits the limitations in the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. It requires a little amount of work on the part of the attacker and is very difficult to trace it back to the attacker. I will briefly describe some of the features of TCP/IP protocol that make this attack possible.**

**TCP/IP**

**IP is the network layer protocol that acts as a packet delivery service. It is unreliable (delivery of packets is not guaranteed) and connection-less (each packet can take its own path independent of other packets). TCP is flanked by the application layer on one side and IP on the other side. It ensures that a reliable communication takes place between the applications and the different services. TCP enables reliable delivery of data packets in order without any repetition and errors.**

**Three-way Handshake**

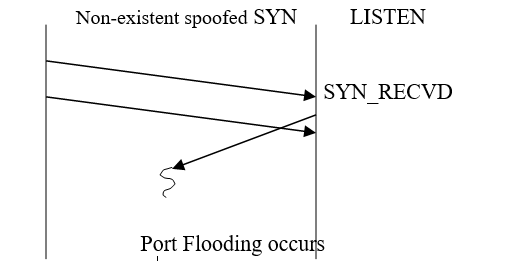
**As we know, a connection needs to be established between the source S and destination D to facilitate the communication between them. This process is referred as the three-way handshake. The process starts with the source sending a SYN packet (TCP header with SYN bit set) to D who responds by sending back packet with both SYN and ACK bits set. If the source finally responds with ACK bit set, connection is established else D sends RST signal after timeout period. Three-way handshake is also used for initializing the sequence numbers, which are needed to provide reliable delivery of packets. Three memory structures namely socket structure (socket), internet protocol control block structure (inpcb) and the TCP control block structure (tcpcb) are allocated by both S and D for every connection. These structures contain all the information required for the connection like state information, buffers, address information, flags, timer information, port numbers, sequence number information etc.**

****

**The three-way handshake can be explained by the figure 1.**

**SYN FLOODING ATTACK**

**As it is explained above, whenever a SYN message arrives at the server that is in LISTEN state, the three memory structures are allocated by the server. It goes in SYN\_RECVD state and sends back SYN, ACK message to the source. This is called half open connection state. There is limit on the number of half-open connections per port that any system can have concurrently. When the limit has reached, the machine will no longer accept any new connection until its queue goes below the limit. It is this limitation the attacker takes advantage to attack the victim. An attacker A starts the attack by sending different connection requests with spoofed/illegitimate source addresses to the victim D. D not knowing it is an attack, allocates its memory resources to these connections and sends SYN, ACK to these requests. D is now in the state of half open connections. The attacker does not send any ACK messages back. When the limit of half-open connections is reached, the victim no longer accepts any more connection requests. So all the legitimate connection requests are also denied. This denial of service to its actual clients exists until timer expires (usually 75s) or if some connections are reset or completed.**

****

**Figure 2: System under attack**

**The attacker has to continuously keep sending SYN packets to the victim requesting new connections. This is important if he wants the denial of service condition to exist for longer period than the timeout period. After timeout period, the connections are reset and resources are reallocated enabling the new connection requests to be accepted. It is necessary for the attacker to use source addresses that are not accessible from victim D. If this is not done, then when the victim sends SYN, ACK to the actual source address S. S does not expect this message so it sends RST packet to D and the connection is reset. This will be a loss for the attacker.**

**Different Attack Modes**

**Usually there are different parameters by which the SYN flood attack can vary. These include batch-size (number of packets sent from the source address in a batch), delay (time interval between two batches of packets) and mode of source address. There are mainly three modes of source address allocation:**

**Single address: A single forged source address is used as the source for all packets.**

**Short list: An attacker uses a small list to pick the source address. These source addresses are then used to send the SYN packets**

**No list: An attacker can use a different, randomly created source address for sending out the packets every time he sends a new batch of packets.**

**Related works**

**All the effective solutions of countering SYN flooding attacks can be roughly classified into four categories: firewallbased, server-based, agent-based and router-based. As firewalls have been installed at almost all sites, several SYN flooding protection systems are available at these firewalls, such as SynDefender and Syn proxying . The firewall before the protected server plays a key role in protection mechanisms, which acts on behalf of the server before the connection is actually established. It intercepts the TCP traffic between clients and the server, and maintains state for each TCP connection. The drawbacks of this approach are delays on every packet for additional processing. Syn cache and Syn cookies belong to the serverbased mechanism. Syn cache still maintains states for each SYN request, but the allocated state structure is much smaller scheme, this requires the coordination between the two FDSs. The first-mile FDS maintains the count of outgoing SYNs and the last-mile FDS keeps track of incoming SYN/ACK packets. At the end of each observation period, the count information must be exchanged between the two FDSs. Since SYN/ACK packets are generated by the other side (i.e., the victim of flooding attacks), it is harder for the flooding sources to evade the detection. Moreover, as compared to the SYN-FIN pair, the interval between SYN and SYN/ACK is bounded by a RTT, instead of the duration of a TCP session that has a much larger variation. Note that the SYN–SYN/ACK pair detection scheme itself is not immune to counter-measures. If the spoofed source address is in the same stub network as a flooding source, it cannot detect the ongoing flooding attack. Recently, Multihomed ASs become necessary to improve availability, reliability and load-balancing. In such a case, the stub network is connected to the Internet by multiple leaf routers. However, as long as the packets that belong to the same TCP session go through the same leaf router, our detection scheme still works.**

**Proposed work**

**The work to be done by our team are as mentioned below:-**

1. **Install all required software and ready a setup to implement our project.**

**Software’s used:**

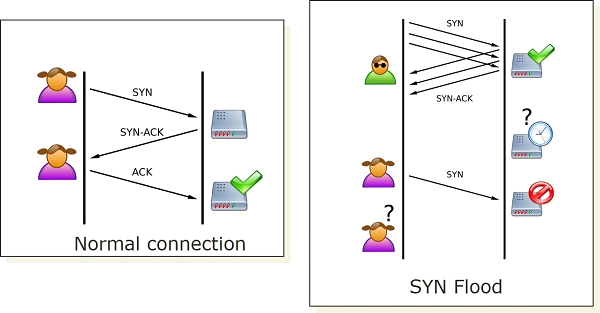
* **Hping3**
* **Wireshark**
* **VMware**
* **PRTG**

1. **initialize syn-flood attack on a virtual machine using hping3.**
2. **Capture and analysis above syn packs in Wireshark in the victim’s machine.**
3. **Analysis network traffic and other data using PRTG tool.**
4. **Setup a notification function in PRTG to alert users of syn flood attacks**
5. **Use firewall to search and block such attacks.**

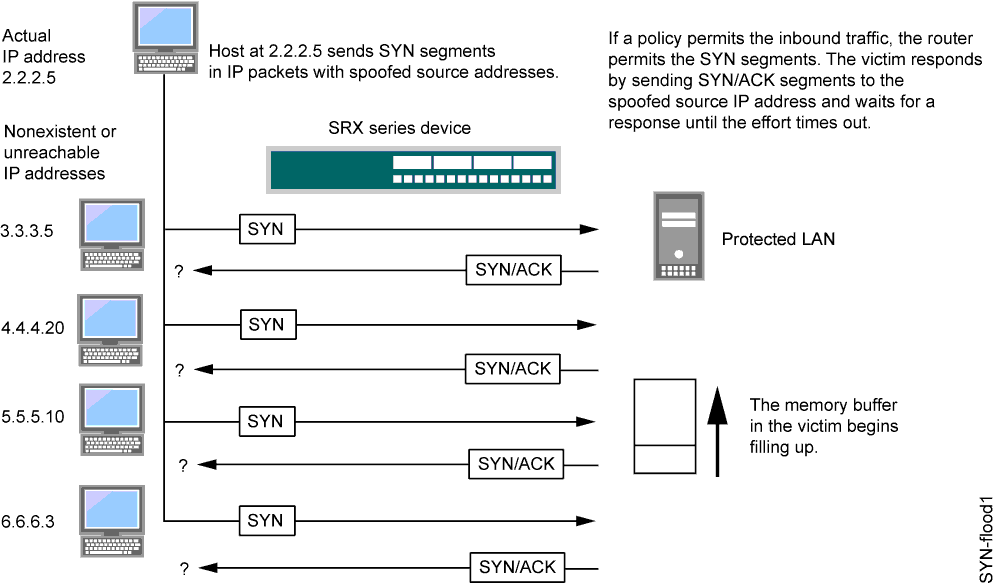
**Architecture**

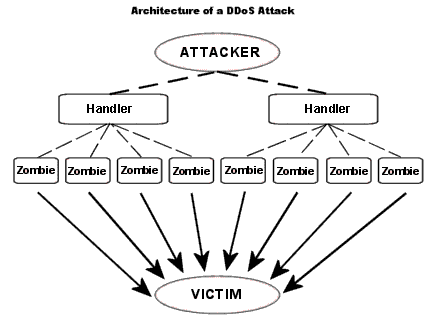
**To conduct the experiment the same machine will act as source as well as destination for the attack. The attack will be conducted from hping on virtual machine(ubuntu) through VMware adapter on host computer which will act as a receiver of the TCP SYN packets. The host is the victim. There are two sections, first is performing denial of service attack from ubuntu host using hping. The second section shows the effect of TCP SYN flood on the victim through Wireshark.**

**TCP 3 WAY HANDSHAKE**

****

**BLOCK DIAGRAMS-**

****

****

**Module description**

* **Attack:**
  + - **Module 1:**

**Attack through hping3**

**hping3 -S 192.168.56.2 -a 192.168.1.1 -p 80 --flood**

**192.168.56.2 is your target IP address. -p 80 is the port to be attacked.  
You can even spoof the ip address fo the source.**

**The IP 192.168.1.1 is the spoofed IP. The victim will think the traffic is coming from 192.168.1.1.**

* **Detection:**
  + - **Module 2:**

**Detection through Wireshark:**

**The Wireshark is used to detect the tcp packets going in and out of the system. The packets without the ack would be red in colour. The huge number of packets without acknowledgement show that the system is under attack. [ refer the screenshots below]**

* + - **Module 3:**

**Detection of traffic through PRTG tool**

**The exponential increase in the number of tcp/udp packets under the heading Various and in the top connections would show the 2 ip address of the attacher and both this would fill up nearly 100% of the pie chart.**

* **Prevention:**
  + - **Module 4:**

**Setting up alarm in PRTG tool.**

**The PRTG tool the sensor we have set up for this particular experiment would go down if the traffic exceeds a certain limit. When the sensor goes down the PRTG tool triggers a alarm and it would also send an email to the user. The user will be notified and would take counter measures regarding it**

* + - **Module 5:**

**Setting up protocols in Firewall setting**

**We would set new rule and block the IP from where the particular attack is being carried out. Thus preventing further attacks from that ip.**

**Implementation details**

## **Procedure**

**Initializing SYN flood attack:-**

**1. Install VMware on victim’s computer and create a virtual machine in VMware with a Linux operating system.**

**2. Install hping3 on the virtual machine**

**3. Now note the ipv4 address of the VM in communication information menu and the ipv4 address of the VM network adapter on victim’s PC.**

**4. Type {sudo -S “attackers IP” -a “victims IP” -p 135 –flood} in the terminal of the VM.**

**Here -S sets hping3 in syn packet generation mode, -p sets port used by these packets, --flood set hping3 in flood mode.**

**5. enter admin password of the VM to initialize attack.**

**Detecting syn flood attack manually using Wireshark:**

**1. open Wireshark and start capturing packets for the ethernet connection of the VMware network adapter.**

**2. you will notice large number of incoming packets that are color coded red because these packets are incomplete and Wireshark doesn’t know how to handle these packets.**

**3. you will also notice that all the packets are from the same source and are labelled ACK.**

**4. these are the SYN flood packets being received by your PC.**

**Detecting syn flood attack automatically using PRTG tool:**

**1. open PRTG tool and click on the “add sensor “button in the sensors tab on the navigation panel at the top of the screen.**

**2. click and select probe device.**

**3. search for “Packet Sniffer” in the search bar displayed on the new screen.**

**4. Select packet sniffer sensor.**

**5. in the settings for the sensor, give a name for your sensor; e.g.: syn1.**

**6. select all adapters in the list displayed after include and exclude filter and save settings.**

**7. The probe device details should be displayed on screen now, in the list of devices attached to probe device find and click on your sensor.**

**8. sensor details are now displayed.**

**9. click in various column displayed in the list on the sensor overview and enable limits.**

**10. set upper limit as 5000 Kbits/sec and save or apply settings.**

**11. now click on the notifications tab on the sensors navigation panel.**

**12 click on “add state notification”, set sensor down time as 0 and notification dropdown as send notification to email and push notification for admin. Set the same setting for sensor up status (on situation resolved). Save settings.**

**Now your PRTG tool will monitor Various protocols section (includes TCP) and will alert you automatically if your sensor goes down.**

**Blocking attackers IP:**

**1. using PRTG and Wireshark you can identify attackers IP.**

**2. once you identify the attackers IP, open windows firewall.**

**3. click on inbound rules in the left panel of the window. Now click on new rule displayed in the right panel of the window.**

**4. in the pop up window click on custom radio button and then press next.**

**5. click on all programs and press next.**

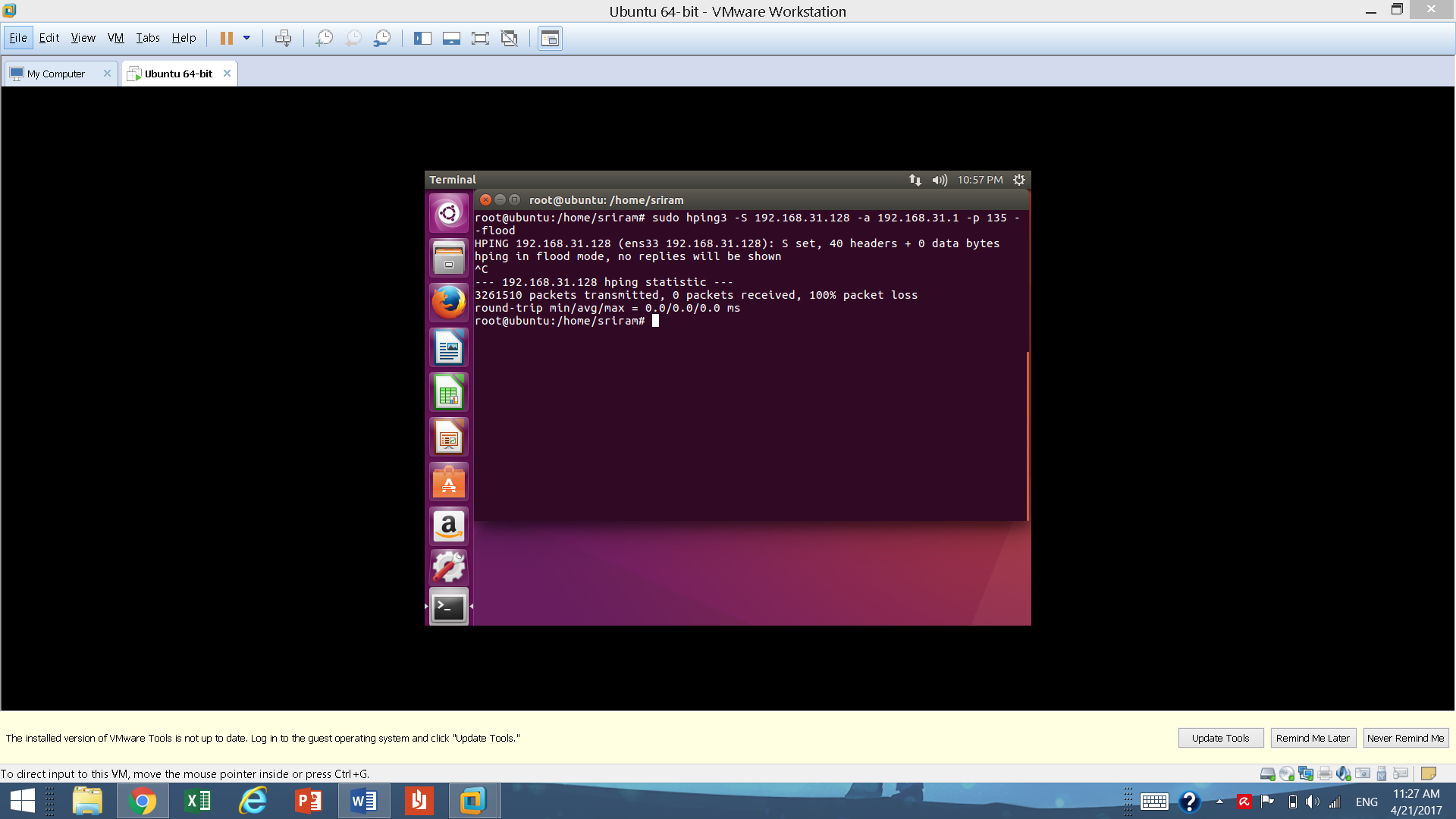
**6. select protocol type TCP and press next.**

**7. enter attackers IP in both local and remote IP addresses then press next.**

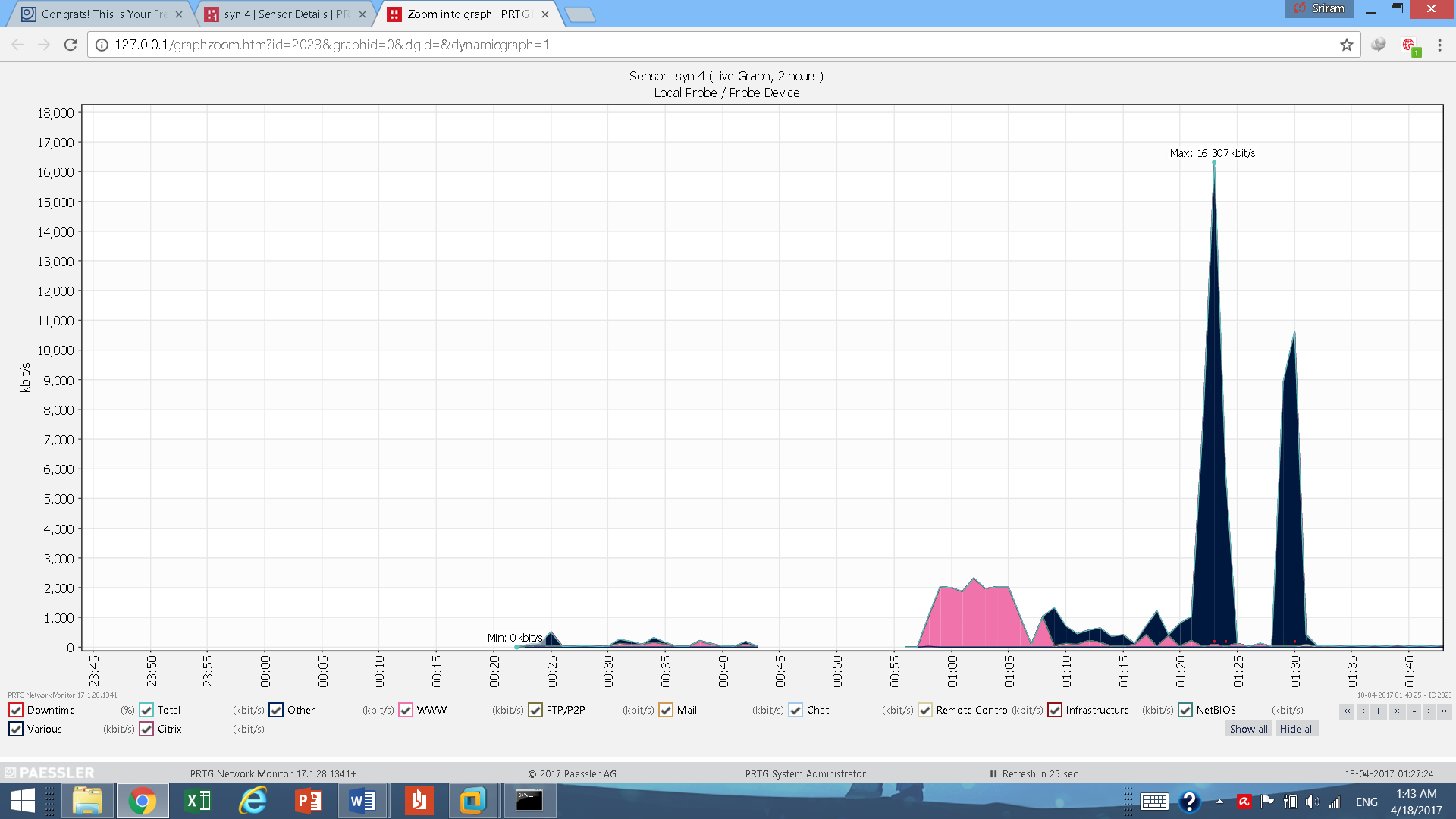
**8. click on block connection and press next twice.**

**9. name your rule and describe it before pressing on finish.**

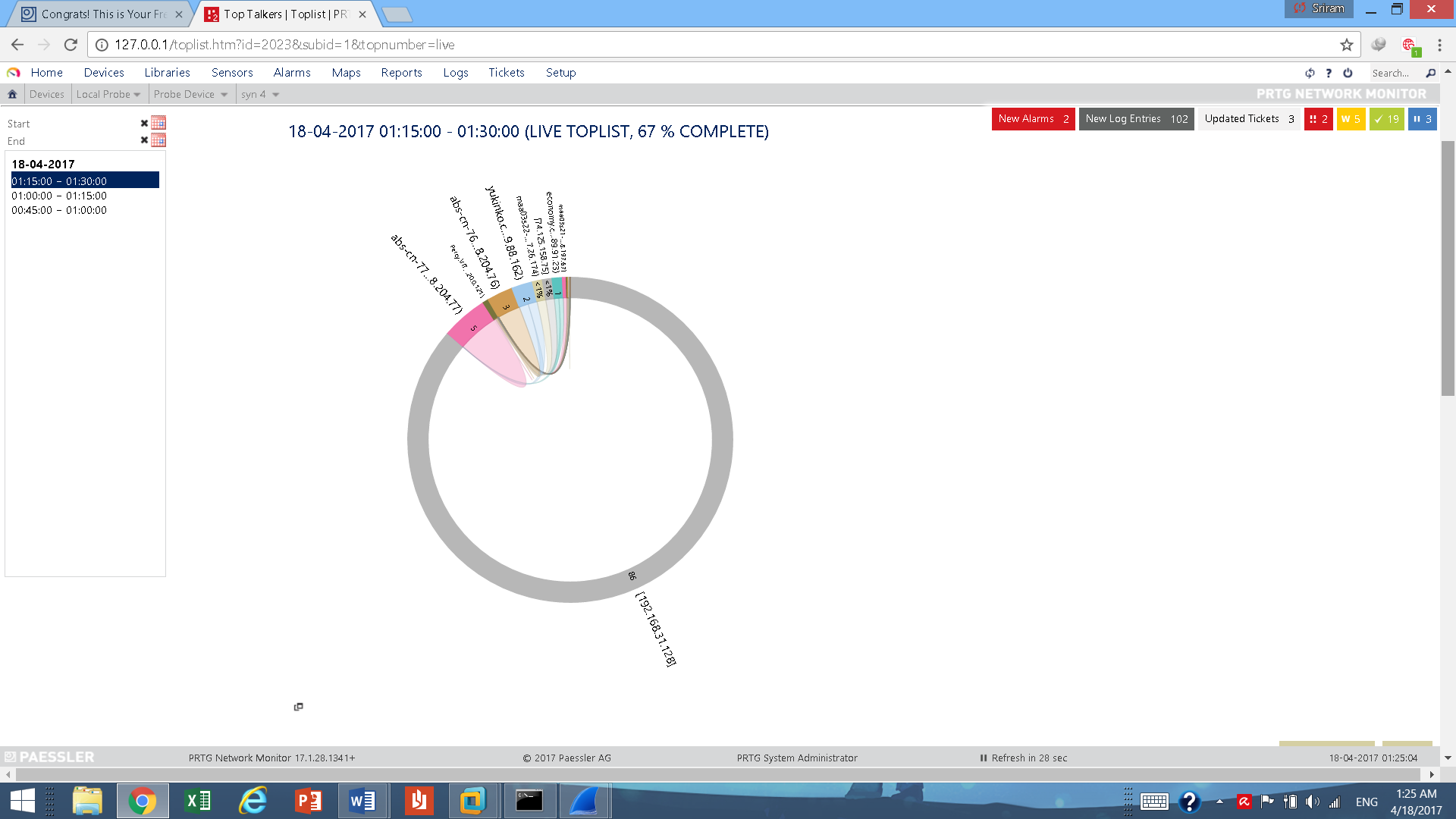
**10. now you have successfully blocked the attacker and prevented any further SYN flood attacks form that IP.**

**Results and analysis**

**Here is an implementation of a syn flood attack in a virtual machine with ipv4 address of 192.168.31.128. this machine Is sending syn packets to the host machine whose IP is 192.168.31.1.**

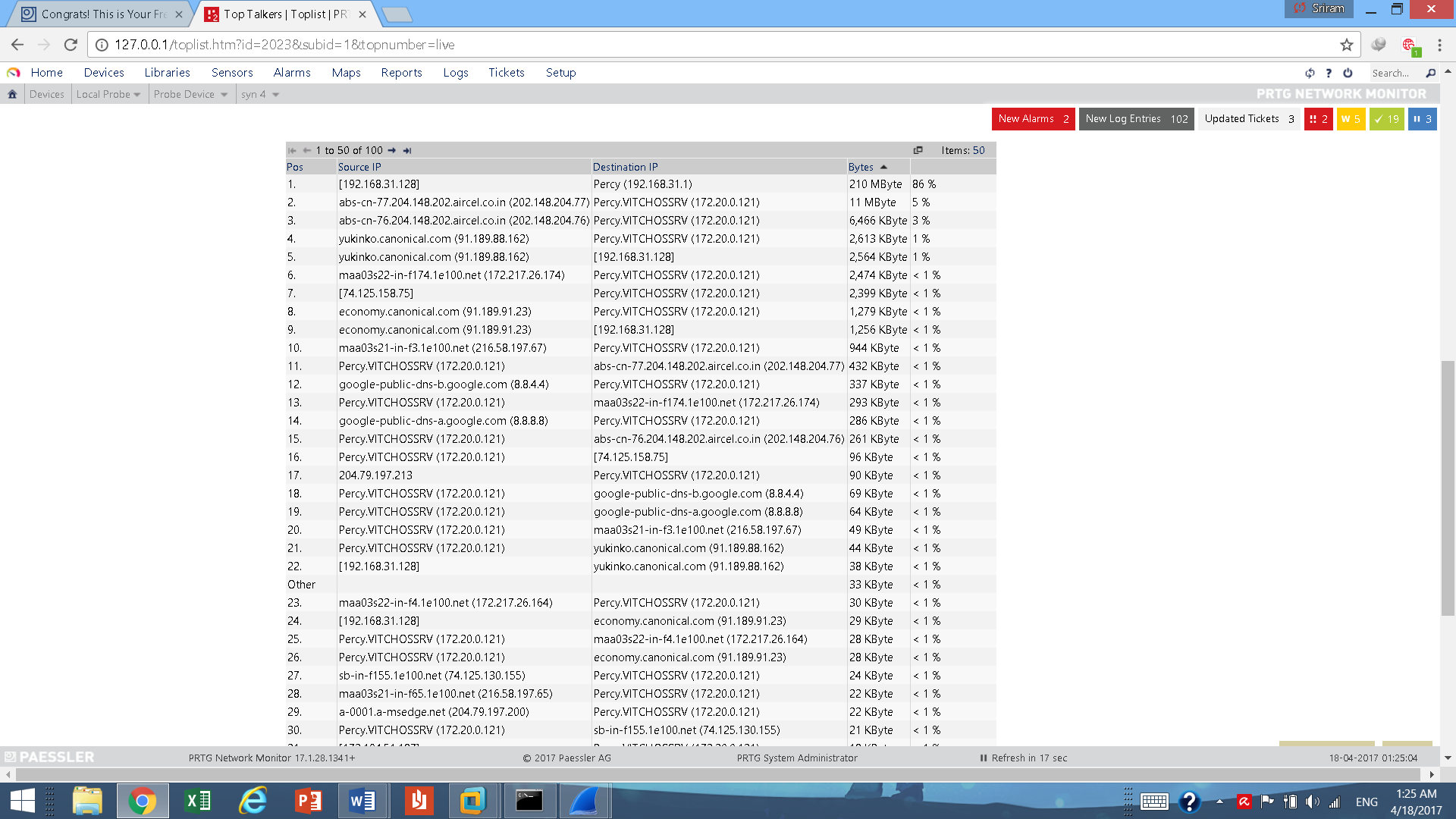
****

**This graph shows various packets received by host in Kbits/s on y axis and the time of recording on x axis. In the graph the 2 tallest sharp peaks are the syn packs received from the attacker. The steep drop after sometime from the initiation is due to the sensor shutting down due to exceeded packet receiving limit.**

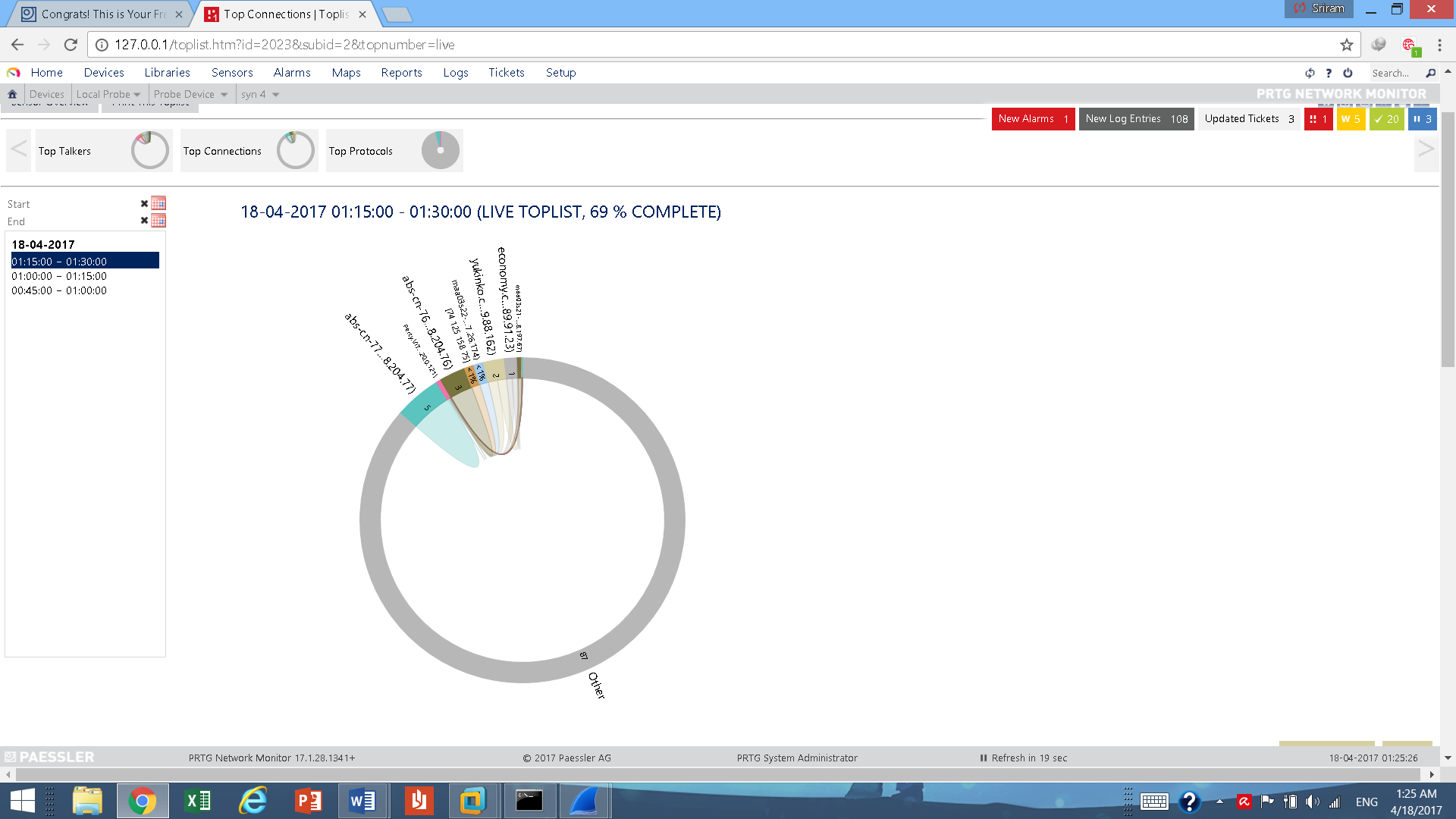
****

**TOP TALKERS CHART**

**This pie chart shows the connections or pair of users that has the highest amount of data transfer between them. Here as shown by the chart the attacker whose IP is 192.168.31.128 has transmitted about 86% of data throughout the session in which this data was recorded. This graph shows the excessive amount of data flow from the attacker to the victim caused by the syn flood attack.**

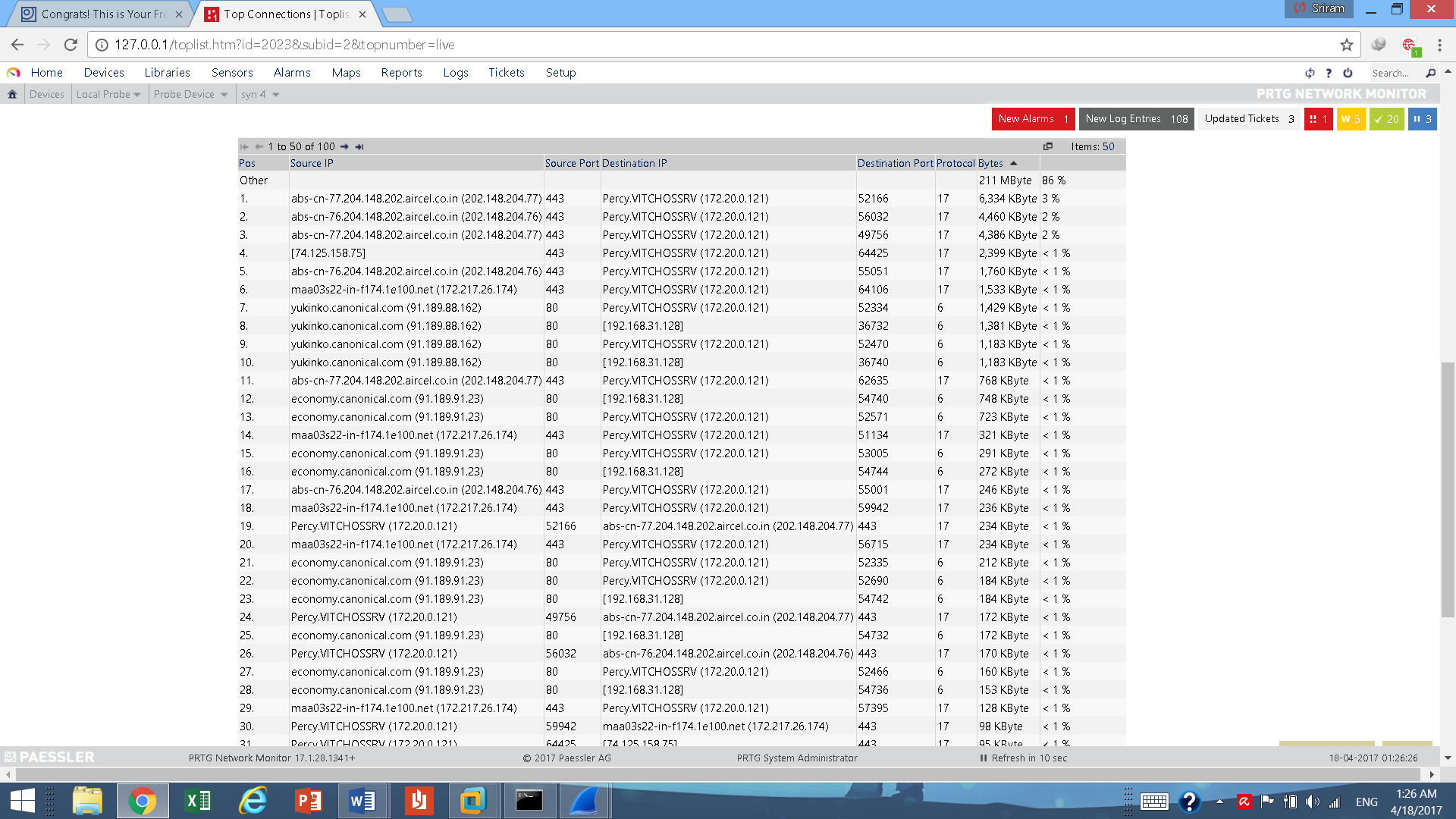
****

**This table represents the data in the above top talkers chart in a more detailed table format. As the first row of the table shows about 210Mb of data was transferred from attacker to the victim which accounts to about 86% of the total data transfer recorded in this session.**

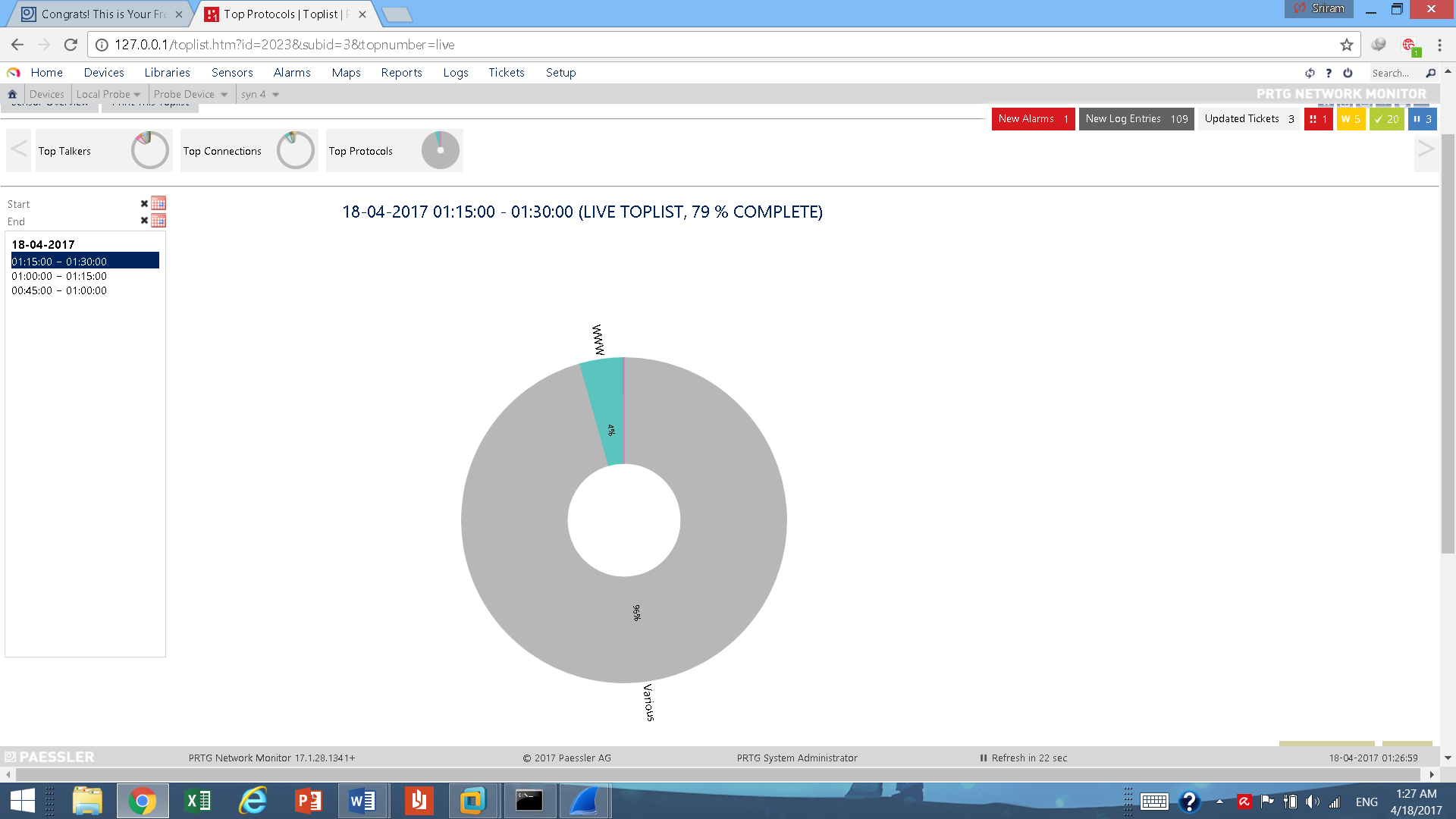
****

**TOP CONNECTIONS CHART**

**This chart shows the different connections made while the session was being recorded The top connections list is a toplist type that displays the connections using most of the bandwidth within the network. It delivers information on the destination IP and port, the period during which this connection has been in the toplist, and much more**

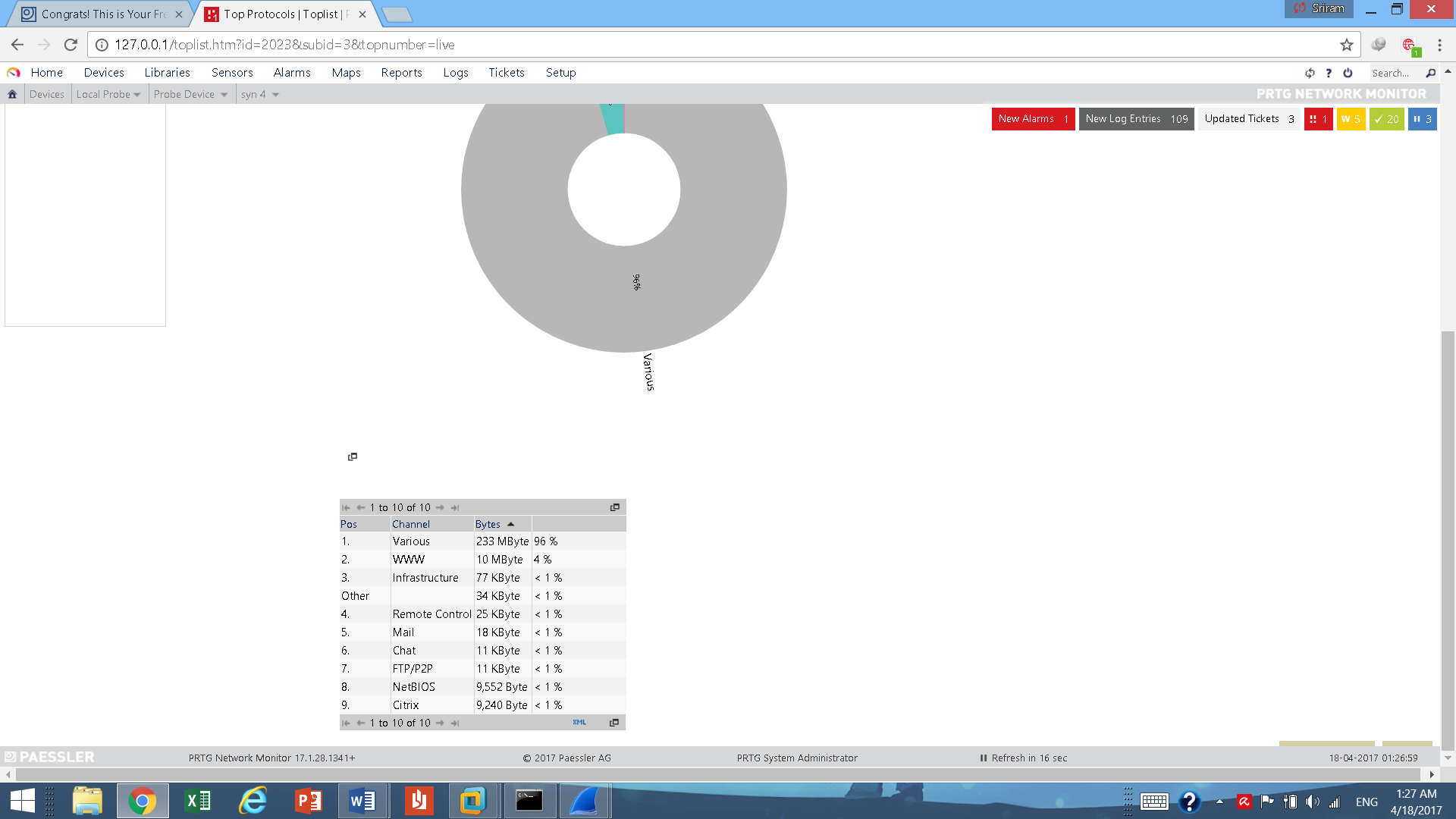
****

**Here is the table format of the above chart. As you can see there are many small tcp connections from the same source i.e. the attacker. All these connections are small and transfer a very small portion of data. However, there are numerous such connection being received simultaneously by the Victim. Note: protocol 6 stands for a TCP protocol.**

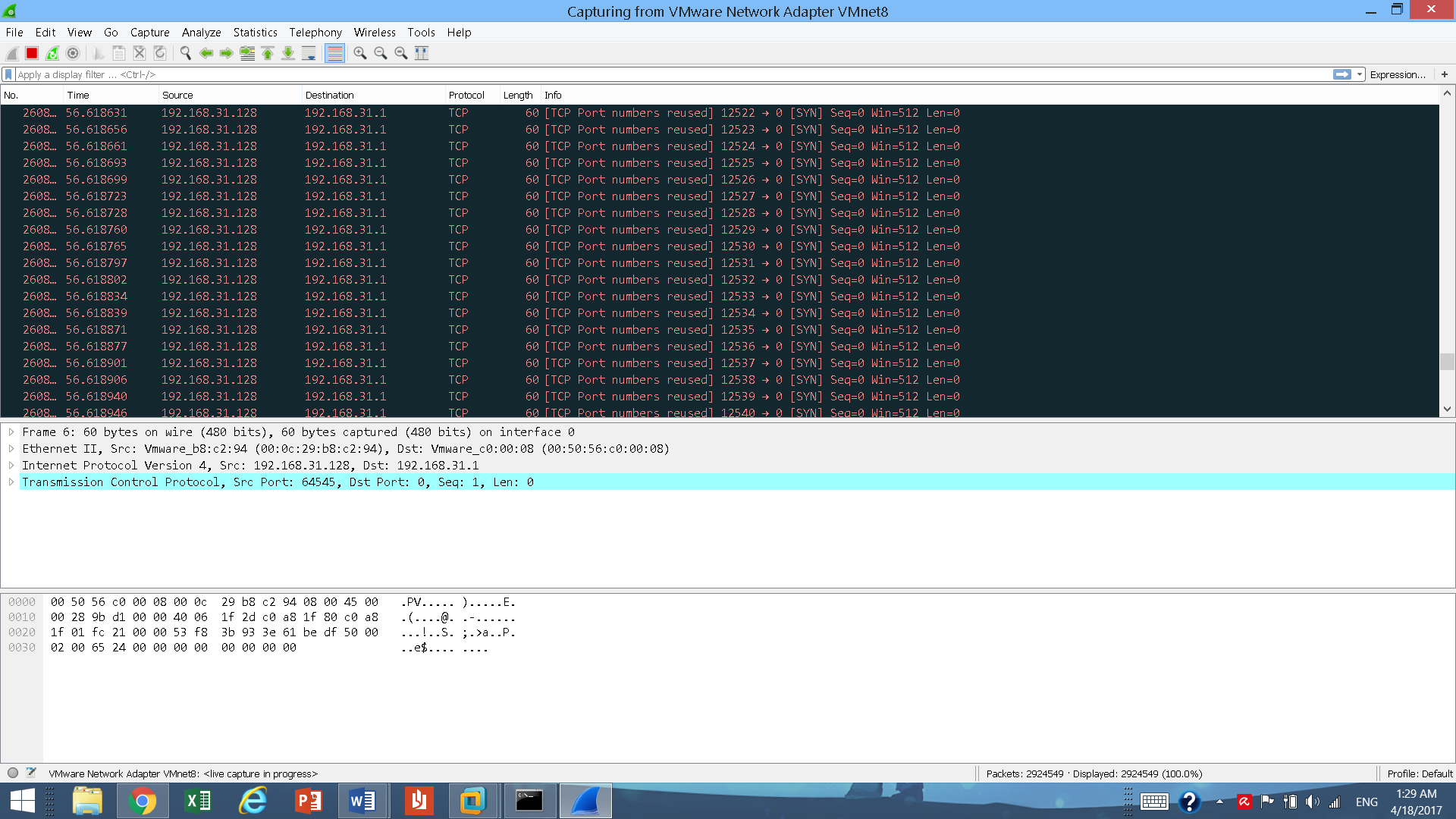
****

**TOP PROTOCOLS**

**This chart shows which protocols are being used and are consuming the band width. Here we see that the category Various occupies 96% of bandwidth. Note that TCP, UDP ,etc come under this category. Hence we can deduce from this and the previous charts that this the syn flood is causing this enormous consumption of bandwidth in the victim’s pc.**

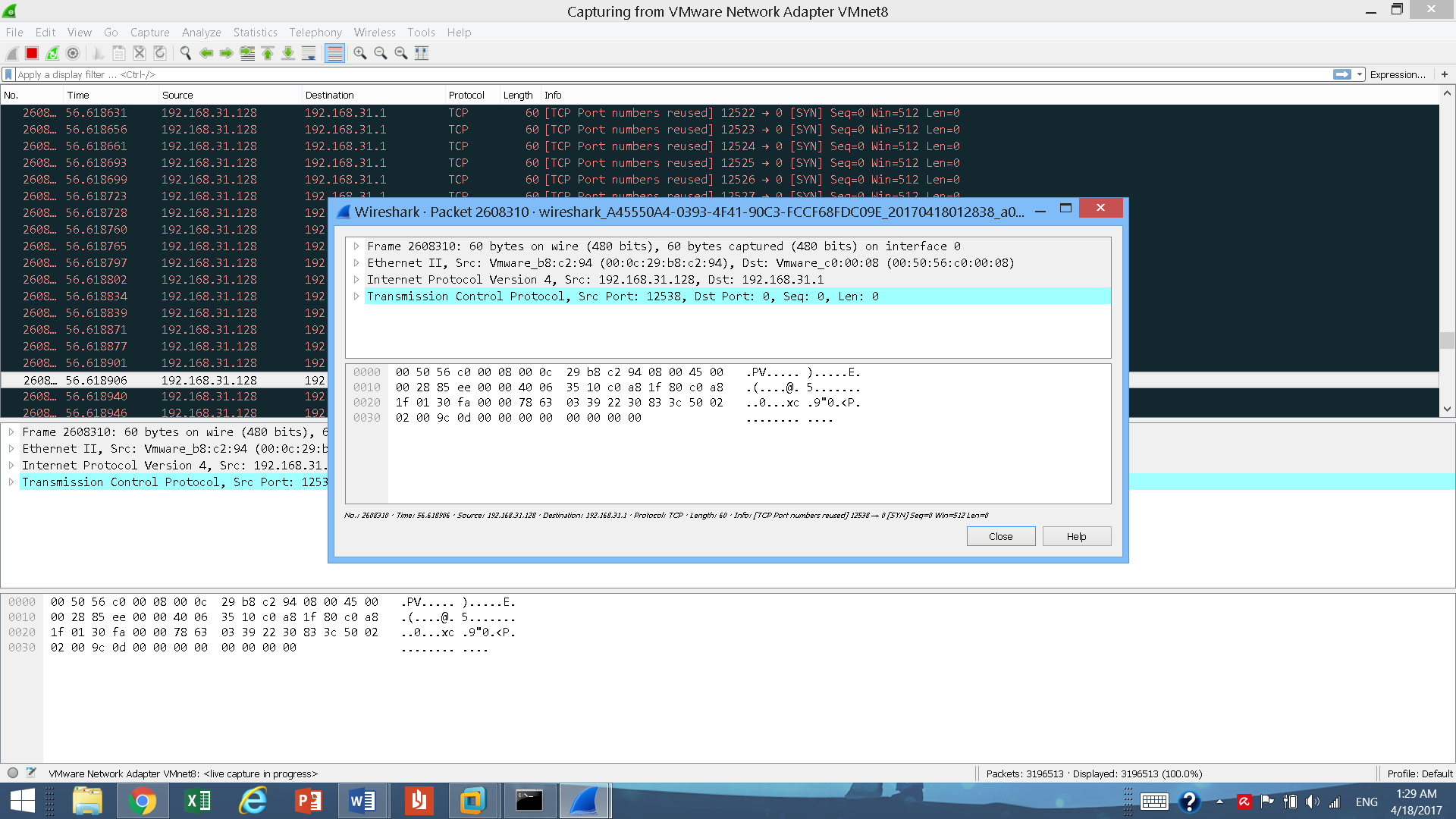
****

**Table form of above chart. As mentioned before in the 1st row we can see how the category various occupies about 96% of usage.**

****

**Wireshark screenshots**

**Each of the above rows represents a corrupt or ill-formed packet (corrupt packages are colored in red by wire shark). As you can see all packets are from the same source and are using TCP protocol indicating a syn flood attack.**

****

**Here is the definition and content of a packet from the TCP packs received.**

**Uniqueness of this research**

* **Allows user to identify and prevent SYN attacks, thus providing a better sense of security.**
* **Notifications would be sent to user via email.**

**Conclusion and future work**

**A denial of service attack is to prevent the legitimate user from gaining access to a certain resources or even complete failure of the server by sending too many requests. The TCP DDOS attack can be implemented by an attacker that may lead to damage to computer network. . Responding, defeating these attacks in an effective manner is the primary challenge of today‟s network security. The demonstration of a Denial of Service attack in this paper is a way to show how a Denial of Service attack can be implemented by the malicious attacker in a LAN and prepare the server to respond and defeat these attacks because if you are not prepared for the worst you will suffer when the worst happens. To detect attack, Network Traffic is analyzed at the victim and the results showed that the arrival rates of normal TCP SYN packets and attacked SYN Flood attack varies with large difference. On the basis of daily network behavior a SYN Packet arrival rate is decided. At the victim side the attack is detected by considering different parameters.**

**Syn flooding attack is one of the most common denial of service attack. It can cause lot of damages. While it is not possible to eliminate this attack, by taking above described measures properly, we can definitely reduce the risk of these attacks.**

**References**

**[1]. D. Nashat , X. Jiang, “Detecting syn flooding agents under any type of ip spoofing,” in IEEE International Conference on e-Business Engineering, pp. 499-505, 2008.**

**[2]. D. Erhan, Anarim, et al., “Effect of DDoS attacks on traffic features,” 21st Conference Signal Processing and Communications Applications, pp. 24-26 April 2013.**

**[3]. Wireshark** [**http://www.wireshark.org/about.html**](http://www.wireshark.org/about.html)

**[4]. T. Nakashima, T. Sueyoshi, “Performance Estimation of TCP under SYN Flood Attacks,” First International Conference on Complex, Intelligent and Software Intensive Systems, pp.10-12 April 2007.**

**[5].Hping** [**http://www.hping.org/**](http://www.hping.org/)

**[6].** [**https://en.wikipedia.org/wiki/SYN\_flood**](https://en.wikipedia.org/wiki/SYN_flood)

**[7].H.Wang,D.Zhang,K.G.Shin, Detecting SYN Flooding attacks, In proceedings of the IEEE infocom,pages 000-001, New York, June 2002,IEEE**

**[8].Che-Fn Yu and virgil D.Gligor. A specification and verification method for preventing denial of service.IEEE Trans.Software Eng.,16(6):581-592,1990.**

**[9]. Zhuang Wei, et al., “TCP DDOS Attack Detection on the Host in the KVM Virtual Machine Environment,” IEEE/ACIS 11th International Conference on Computer and Information Science (ICIS),pp.62-67, June 1 2012.**

**[10]. Z. Gao, et.al. , “Differentiating Malicious DDoS Attack Traffic from Normal TCP Flows by Proactive Tests,”, IEEE Communications Letters, vol.10, pp.793,795, November 2006.**

**[11]. Kavisankar, C. Chellapan ,” A Mitigation model for TCP SYN flooding with IP Spoofing”, IEEE-International Conference on Recent Trends in Information Technology, pp. 251-256, 2011.**

**[12]. L. Limwiwatkul, A. Rungsawang, “Distributed denial of service detection using TCP/IP header and traffic measurement analysis,”, IEEE International Symposium on Communications and Information Technology, pp.26-29 Oct. 2004.**

**[13]. K. Park and H. Lee, “On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack”, Proceedings of IEEE INFOCOM 2001, March 2001.**

**[14].K. Park and H. Lee, “On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack”, Proceedings of IEEE INFOCOM 2001, March 2001.**

**[15].Preventing of SYN Flood Attack with Iptables FirewallSara Mirzaie; Alireza Karimi Elyato; Mehdi Agha Sarram2010 Second International Conference on Communication Software and Networks Year: 2010 Pages: 532 - 535.**