The SNORT Intrusion Prevention System

Ibrahim Tamim

Electrical and Computer Engineering Department

ECE 9609: Introduction to Hacking

Outline

- The Problem Overview
  - What is a Network Intrusion?
  - Network Intrusion Attack Examples
- How to Prevent a Network Intrusion?
  - Intrusion Prevention System
  - How Do IPSs Work?
  - IPS vs IDS vs Firewall
- SNORT
- A Technical Look at SNORT
  - SNORT VS Network Attacks
  - Attacks That SNORT Protect Against
- Conclusion

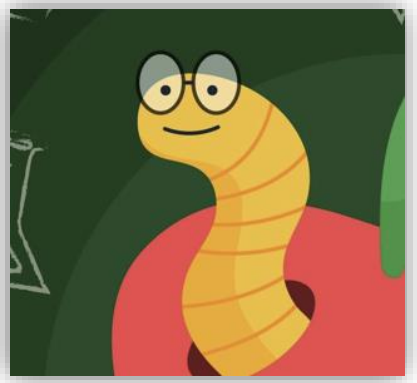
The Problem Overview
Network Intrusion

What is a Network Intrusion?

- It’s an unauthorized penetration of an isolated private/public network, or a penetration of a specific address/machine on that network.
- Intrusion can be of two main types,
  - Passive where the attack on the network is carried without detection. No or minimal modification to the networks are performed.
  - Active: Changes to the network resources or infrastructures are made.

Network Intrusion Attack Examples

- Intrusions are one of the most dangerous attacks on networks. This is due to the wide range of abilities the intruder gains.
- Most critically, information is immediately compromised.
- An intruder **can gain access** for a targeted one-time attack (e.g., injecting malware) or they can "live" in the network for extend periods of time (carrying different attack and staling information).
- **Network Intrusion attack examples:**
  - *Covert CGI Scripts*
  - *Multi-Routing*
  - ***Worms***
  - *Traffic Flooding*



How to Prevent a Network Intrusion?

Intrusion Prevention System

Intrusion Prevention System (IPS)

- IPSs are security tools that are tasked with continuously monitoring the network for any penetration attempts or malicious request/activities.
- IPSs also act against any detected intrusion attempt. These actions include reporting, blocking or dropping the detected requests.
- IPSs can be hardware-based network functions or software-based network functions.

How Do IPSs Work?

- **Signature-Based:** Well-known threats have clearly identified signatures. This methods tries to detect these signatures to identify the threat. A major limitation for such an approach is new threats/attacks *(unknown signatures).*

- **Anomaly-Based:** A baseline standard of the subject network must first be defined. The method will identify any suspicious or anomalous behaviors in the network's traffic. A drawback for such an approach is that it produces false positives.

- **Policy-Based:** Administrators and network engineers have to set-up and define clear network policies that the IPS will execute while monitoring a **specific** network.

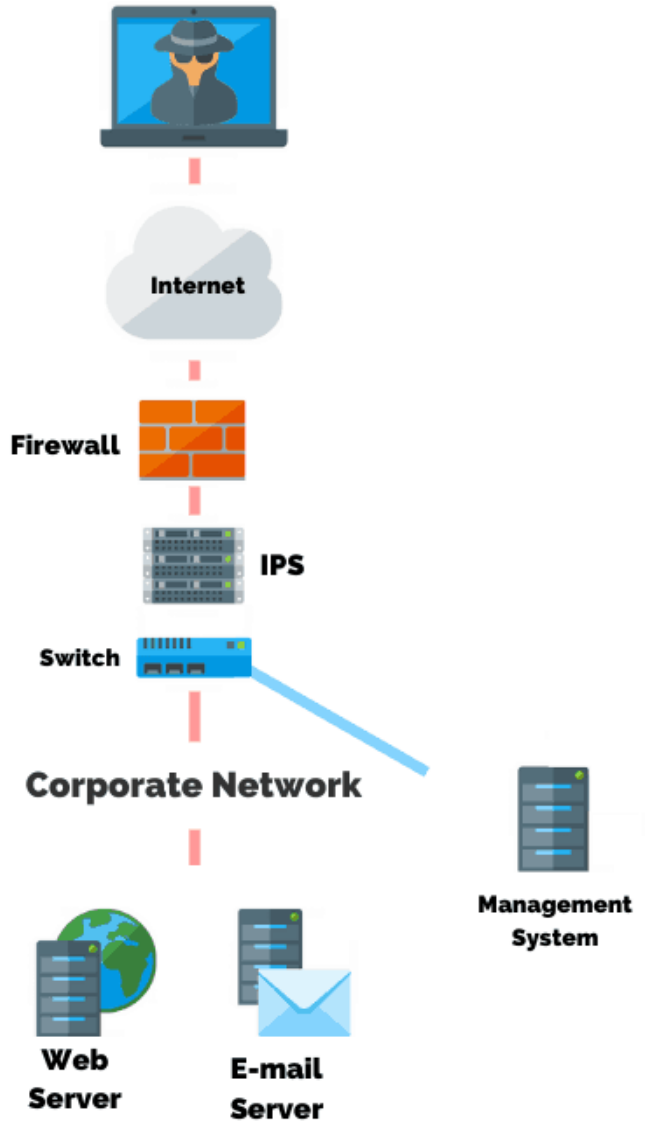


Figure: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/

IPS vs IDS vs Firewall

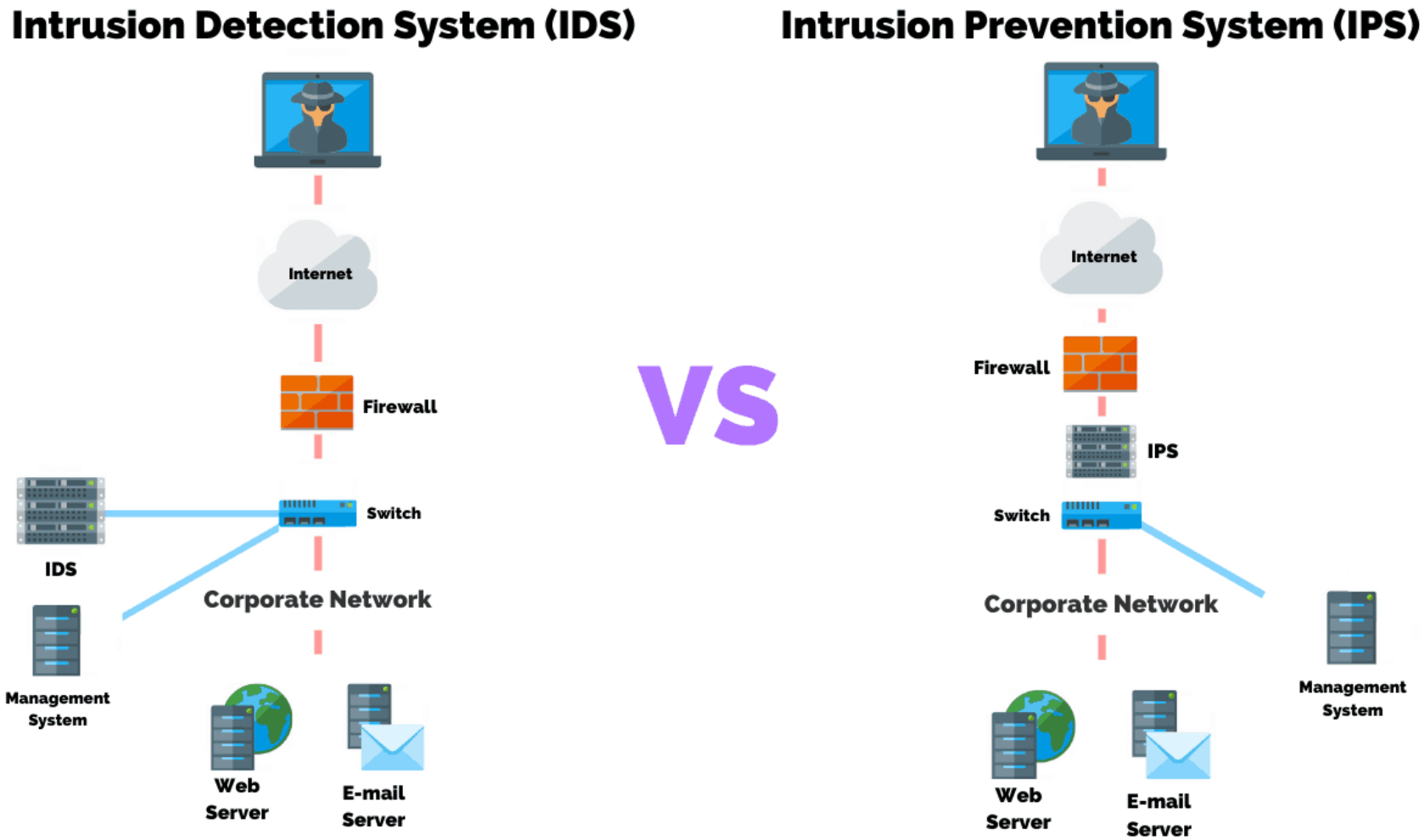


Figure: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/

SNORT

SNORT

- SNORT is the leading and most-known IPS in the entire networking world. SNORT's massive policy/rule –based database helps protects network traffic by deploying SNORT in an inline manner. As an IPS SNORT detects, alerts, and defends against network penetration attacks.

- **SNORT's three primary functions are:**
  - Packet sniffer
  - Packet logger
  - Full-blown network IPS

SNORT's Benefits

- **Additional Security:** As anomaly detection is one of SNORT's major advantages, it can work closely with other security functions within the network to provide a higher level of security at the application level. (SNORT has access to packet contents)

- **Increased efficiency:** SNORT is not the only security function present for protection. So, by detecting, and dropping malicious network traffic, SNORT reduces the load on other deeper security functions. This dramatically increases the efficiency of the network's defenses.
-
- **Time and cost efficiency:** SNORT is automated. This means reduced cost of management and operation. And a much more time efficient protection as minimal human input is required.

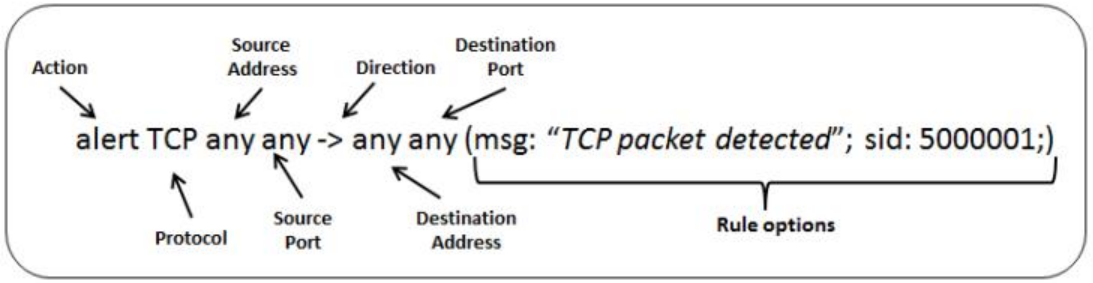


Figure: Trabelsi, Zouheir & Alketbi, Latifa. (2015). Using Network Packet Generators and Snort Rules for Teaching Denial of Service Attacks. 10.13140/RG.2.1.1196.4646.

How to install SNORT?

```
wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz

wget https://www.snort.org/downloads/snort/snort-2.9.19.tar.gz
```

```
tar xvzf daq-2.0.7.tar.gz

cd daq-2.0.7
./configure && make && sudo make install
```

```
tar xvzf snort-2.9.19.tar.gz

cd snort-2.9.19
./configure --enable-sourcefire && make && sudo make install
```

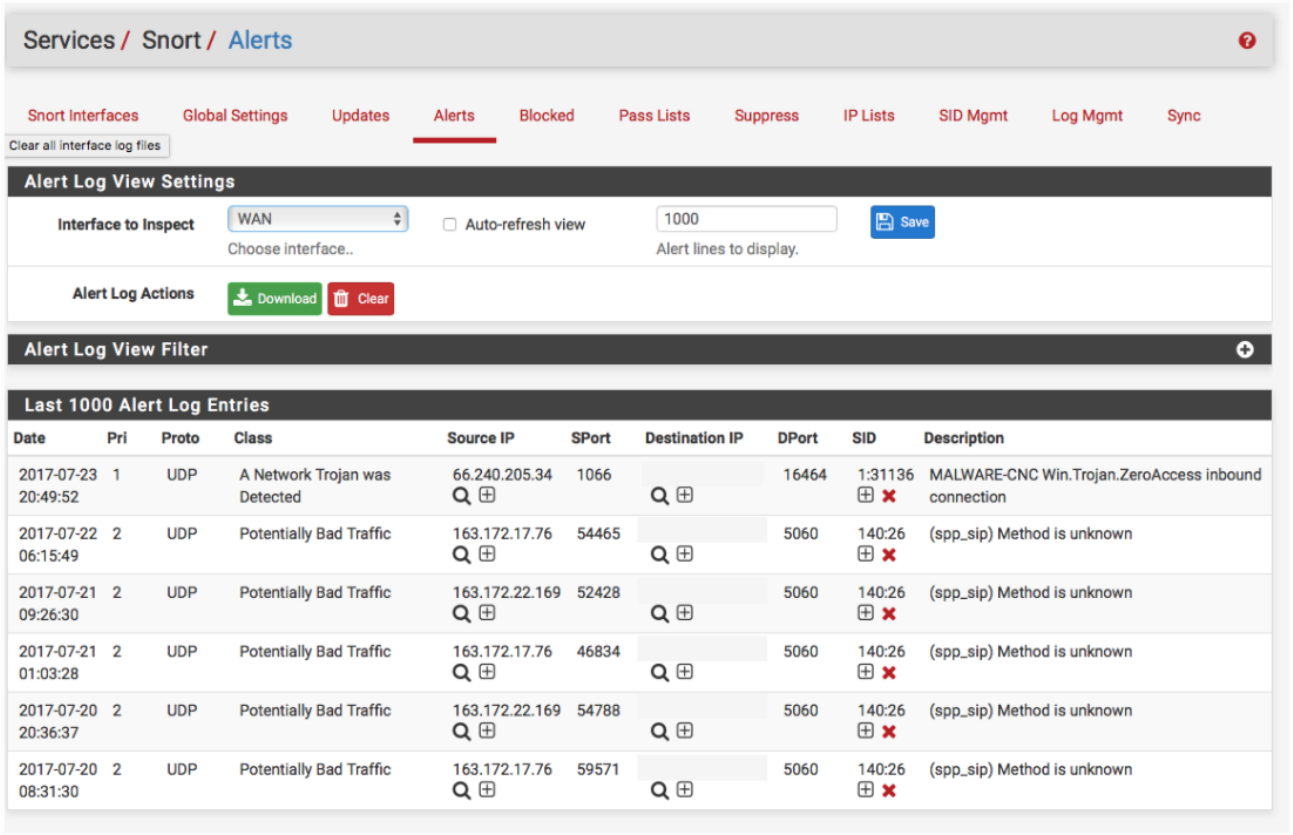
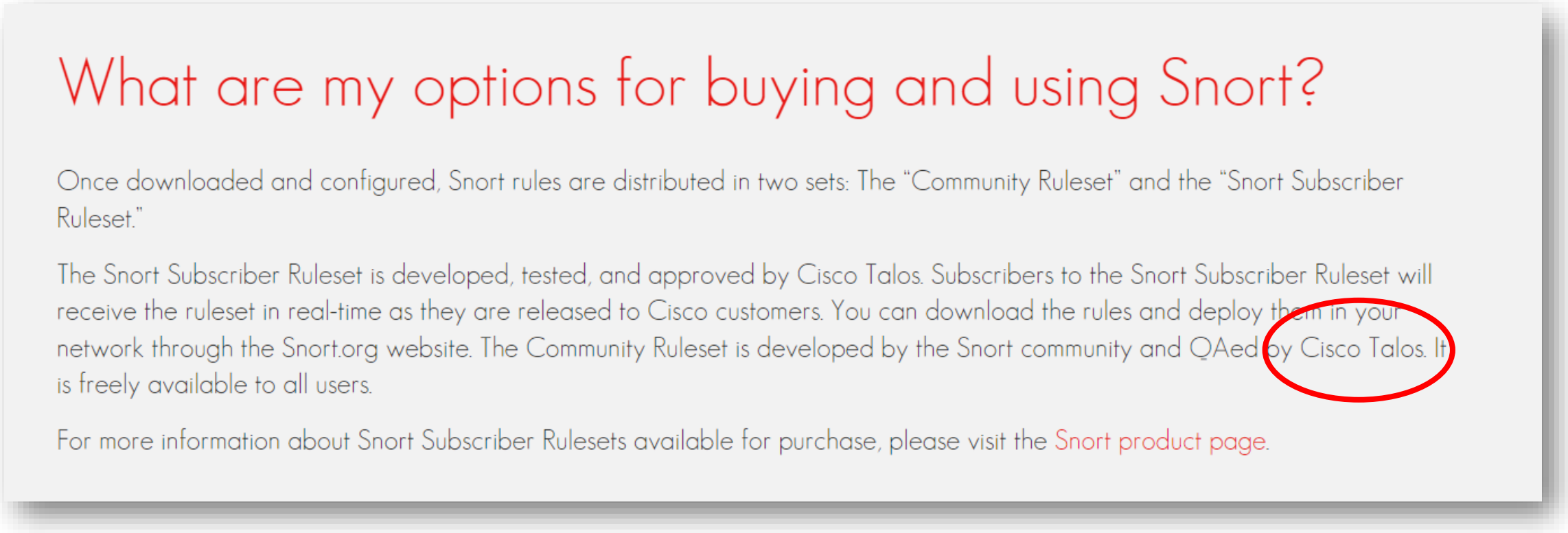


Image: https://www.snort.org/

Image: https://docs.netgate.com/pfsense/en/latest/packages/snort/alerts.html

SNORT and Cisco



What are my options for buying and using Snort?

Once downloaded and configured, Snort rules are distributed in two sets: The "Community Ruleset" and the "Snort Subscriber Ruleset."

The Snort Subscriber Ruleset is developed, tested, and approved by Cisco Talos. Subscribers to the Snort Subscriber Ruleset will receive the ruleset in real-time as they are released to Cisco customers. You can download the rules and deploy them in your network through the Snort.org website. The Community Ruleset is developed by the Snort community and QAed by Cisco Talos. It is freely available to all users.

For more information about Snort Subscriber Rulesets available for purchase, please visit the Snort product page.

Image: https://www.snort.org/

SNORT *VS* Network Attacks
A closer technical look

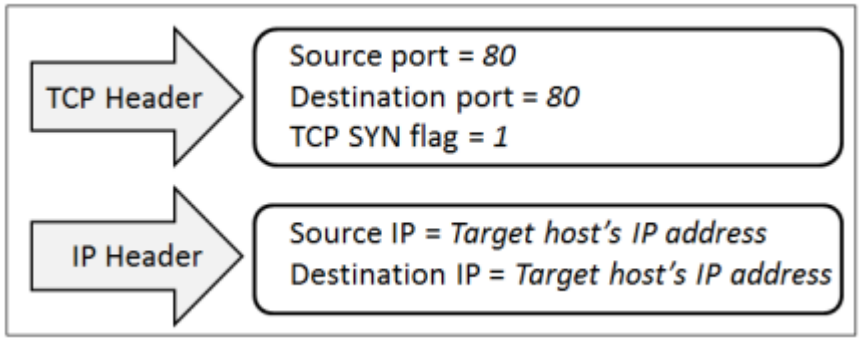
Attacks That SNORT Protects Against

Attack	Description
DDoS Attacks	An attempt to make a server, service, or network unavailable by overwhelming it with a flood of traffic from multiple, distributed computing systems.
Smurf Attack	A type of DoS attack in which a system is flooded by a large number of Internet Control Message Protocol (ICMP) packets, rendering the victim's network unresponsive.
Ping of Death	A DoS attack in which an attacker attempts to crash a system by sending malformed or oversized packets, using a ping command.
SYN Flood Attacks	A DoS attack in which large volumes of SYN (synchronize) packets (connection requests) are sent to a victim's server or firewall, rendering it unavailable.
SSL Evasion	Attackers exploit Secure Sockets Layer (SSL) / Transport Layer Security (TLS) encryption blind spots, using SSL/TLS to hide malicious content, evade detection, and bypass security controls.
IP Fragmentation Attack	Attackers overwhelm network resources by exploiting datagram fragmentation mechanisms, confusing the target system as to how TCP/UDP datagrams should be reassembled.
Port Scanning Attack	Attackers send requests to a range of server ports, with the goal of finding an active port and exploiting its vulnerability.
ARP Spoofing	Attackers send fake Address Resolution Protocol (ARP) messages, linking the attacker's MAC address with the IP address of a legitimate system and diverting traffic from that system to the attacker.
Buffer Overflow Attacks	Attackers exploit buffer overflow vulnerabilities, corrupting the execution path of an application by overwriting parts of its memory.
OS Fingerprinting Attacks	Attackers attempt to identify the operating system of a specific target and exploit its vulnerabilities.
SMB Probes	Attackers capture Server Message Block (SMB) protocol authentication requests, and relay them to another host.

Table: https://www.exabeam.com/ueba/ips-security-how-active-security-saves-time-and-stop-attacks-in-their-tracks/

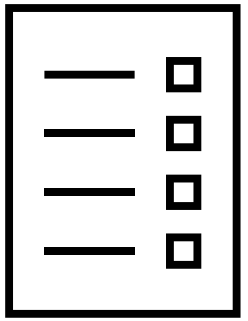
Land Attack Protection

- **What is the attack?** It's an attack that results in the subject machine requesting to connect to itself continuously. This is achieved when the attacker first spoofs then resends a TCP SYN packet to the machine with all sources and destinations set as those of the subject machine.



- **SNORT Rule for Land Attacks**

```
alert tcp any any -> any any (msg: "Land attack
detected"; flags:S; sameip; sid: 5000000; rev:1;)
```



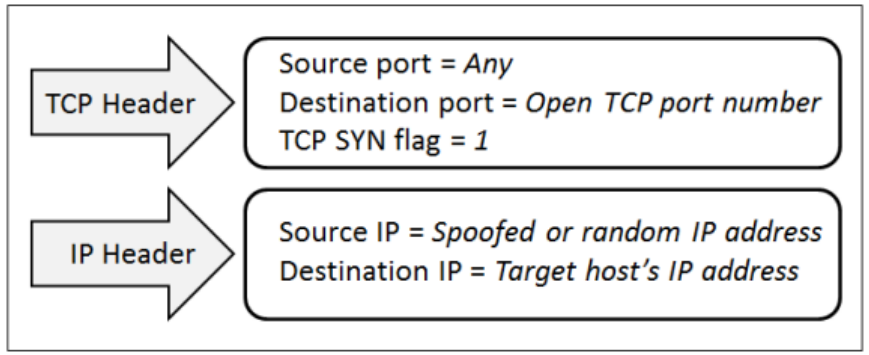
- **Screenshot of SNORT Detecting a Land Attack**

```
[**] [1:5000000:1] Land attack detected [**]
[Priority: 0]
01/02-10:32:32.993302 0:1E:B:2C:86:36 -> 0:24:E8:9D:86:36 type:0x800 len:0x3C
192.168.1.3:1 -> 192.168.1.3:2 TCP TTL:128 TOS:0x0 ID:4369 IpLen:20 DgmLen:40
******S* Seq: 0xCCCCCCCC  Ack: 0x0  Win: 0x4000  TcpLen: 20
```

Figures and SNORT request: Trabelsi, Zouheir & Alketbi, Latifa. (2015). Using Network Packet Generators and Snort Rules for Teaching Denial of Service Attacks. 10.13140/RG.2.1.1196.4646.

SYN Flood Attack Protection

- **What is the attack?** An attacker targets a host by flooding it with TCP SYN packets. However, these packet requests are sent from spoofed IP address. This means that the server will never be able to receive an ACK message back from these requests leading to a flood.



- **SNORT Rule for Land Attacks**

```
alert tcp any any -> 192.168.1.3 any (msg:"TCP SYN flood
attack detected"; flags:S; threshold: type threshold, track
by_dst, count 20 , seconds 60; sid: 5000001; rev:1;)
```

- **Screenshot of SNORT Detecting a Land Attack**

```
[**] [1:5000001:2] TCP SYN flood attack detected [**]
[Priority: 0]
01/02-10:50:53.152327 0:1E:B:2C:86:36 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x45
77.238.187.181:60783 -> 192.168.1.3:80 TCP TTL:128 TOS:0x0 ID:44551 IpLen:20 DgmLen:55
******S* Seq: 0x2CDCB70E  Ack: 0x0  Win: 0x0  TcpLen: 20
```

Figures and SNORT request: Trabelsi, Zouheir & Alketbi, Latifa. (2015). Using Network Packet Generators and Snort Rules for Teaching Denial of Service Attacks. 10.13140/RG.2.1.1196.4646.

A Quick Comparison

F. Leu and Z. Li, "***Detecting DoS and DDoS Attacks by Using an Intrusion Detection and Remote Prevention System***," 2009 Fifth International Conference on Information Assurance and Security, 2009, pp. 251-254, doi: 10.1109/IAS.2009.294.

Table 4. Detection accuracy of mixing resource and bandwidth consumption Attacks

Statistics / Secu.System	True Positive	True Negative	False Positive	False Negative	Detection Accuracy
McAfee	89.5%	100%	0%	10.5%	94.75%
Snort	89.5%	95.2%	4.8%	10.5%	92.35%
FG-100A	94.49%	100%	0%	5.51%	97.25%
CSIPS	100%	96.8%	3.2%	0%	98.4%

Table 2. Detection results of resource consumption attack on 15,645 pkts/sec

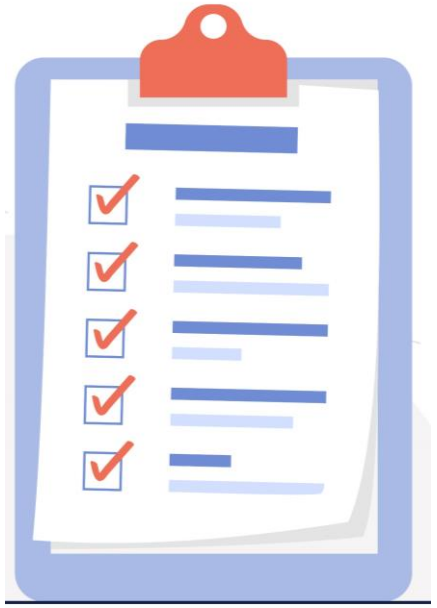
Statistics / Secu. Systems	ART/SD (sec.)	ATT/SD (sec.)	AWT/SD (sec.)	APL (%)	AML (%)
McAfee	2/0	10/0	--	77	49
Snort	8/0	15/0.02	--	41.5	15.9
FG-100A	1/0	10/0	--	92.2	40.9
CSIPS: in-bound	1.56/0.05	10/0	0/0	32.1	32.2
CSIPS: out-bound	1.48/0.019	10/0	0/0	33.5	34.6
CSIPS: forwarded	1.49/0.018	10/0	0/0	35.1	34.4

Table 3. Detection results of bandwidth consumption attack on 2,685 pkts/sec

Statistics / Secu.Systems	ART/SD (sec.)	ATT/SD (sec.)	AWT/SD (sec.)	APL (%)	AML (%)
McAfee	2/0	10/0	--	48	59.3
Snort	5/0	13/0.02	--	26.1	15.4
FG-100A	1/0	10/0	--	27.6	43
CSIPS: in-bound	1.32/0.1	10/0	0/0	38	27.2
CSIPS: out-bound	1.13/0.022	10/0	0/0	39.6	25.9
CSIPS: forwarded	1.18/0.015	10/0	0/0	38.7	26.8

Conclusion

- The Problem Overview
- Network Intrusions
- Network Intrusion Attack Examples
- How to Prevent a Network Intrusion?
- IPS vs IDS vs Firewall
- SNORT
- A Technical Look at SNORT
- SNORT VS Network Attacks
- Attacks That SNORT Protect Against



Additional Resources

- https://www.exabeam.com/ueba/ips-security-how-active-security-saves-time-and-stop-attacks-in-their-tracks/
- https://docs.netgate.com/pfsense/en/latest/packages/snort/alerts.html
- https://www.sciencedirect.com/topics/computer-science/network-intrusion
- A. H. Al-Hamami and G. M. W. Al-Saadoon, "*Development of a network-based: Intrusion Prevention System using a Data Mining approach*," 2013 Science and Information Conference, 2013, pp. 641-644.
- P. R. Chandre, P. N. Mahalle and G. R. Shinde, "*Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification*," 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2018, pp. 135-140, doi: 10.1109/GCWCN.2018.8668618.

Thank you!