Lab Report 20

1. Assessment Sheet
2. **What is the difference between an IDS and an IPS?**

An ID focuses much on the information collection while an IPS is focusing on block the suspicious connections or intrusions based the analysis report which derived from IDS.

1. **Why is it important to perform a network traffic baseline definition analysis?**

From making a network traffic baseline, we can know whether this traffic is normal or abnormal which helps us identify suspicious activities in time.

1. **Why is a port scan detected from the same IP on a subnet an alarming alert to receive from your IDS?**

The alerts that come from the same IP on a subnet show that the machine might be compromised. As an attacker, he/she might gain remote access to a workstation and a vulnerability scan might be ongoing.

1. **If the Snort IDS captures the IP packets off the LAN segment for examination, is this an example of promiscuous mode operation? Are these packets saved or logged?**

It’s definitely not promiscuous mode because promiscuous model allows us to sniff all packets over the network. All these captured packets are logged rather than saved.

1. **What is the difference between a host-based IDS and a network-based IDS?**

The host-based IDS is deployed in individual machines instead of install on a device which monitor the entire network. In network-based IDS, we cannot protect a particular host within this network.

1. **How can you block attackers, who are performing reconnaissance and probing, with Nmap and Open VAS port scanning and Vulnerability assessment scanning tools?**

As every common reconnaissance and probing tools has its own digital signature, so we can try to identify these signatures first. And, then we should configure our IDS and IPS to generate alerts and block any penetrating tools on our external IDS/IPS.

1. **Why is it a good idea to have host-based intrusion detection systems enabled on critical servers and workstations?**

The network-based intrusion detection system cannot granulate the protection rules into host. The only thing they can do is to filter unwanted packets for entire network system. So, some malware or malicious code might bypass the general settings and infect the individual computer. Another thing is that some virus transmitted from USB or other portable devices, which network-based detection doesn’t take effect. So, the best thing we need to do is install host-based IDS and IPS for each critical server.

1. **Where should you implement intrusion prevention systems in your IT infrastructure?**

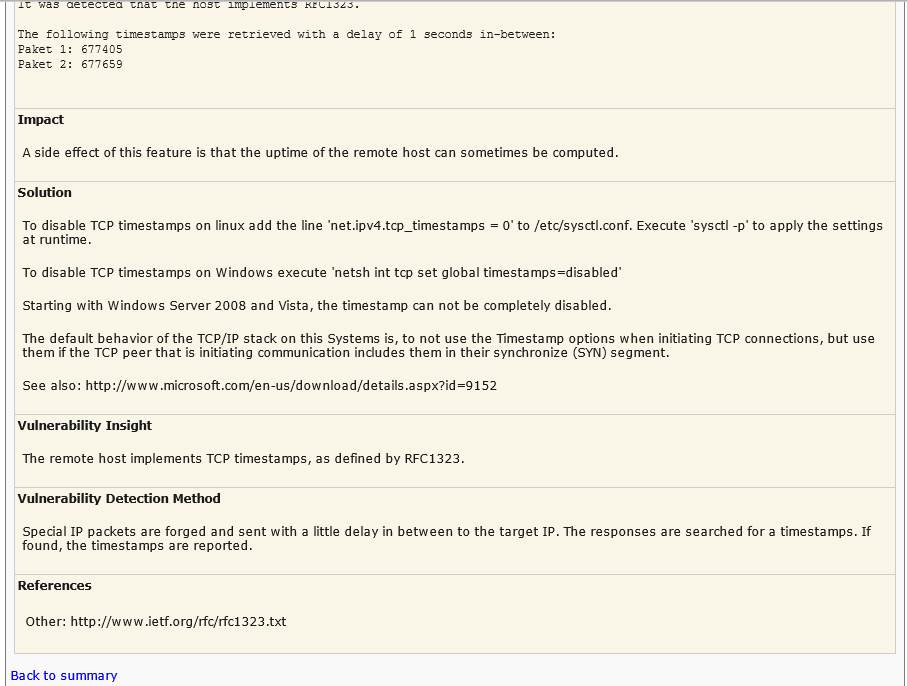
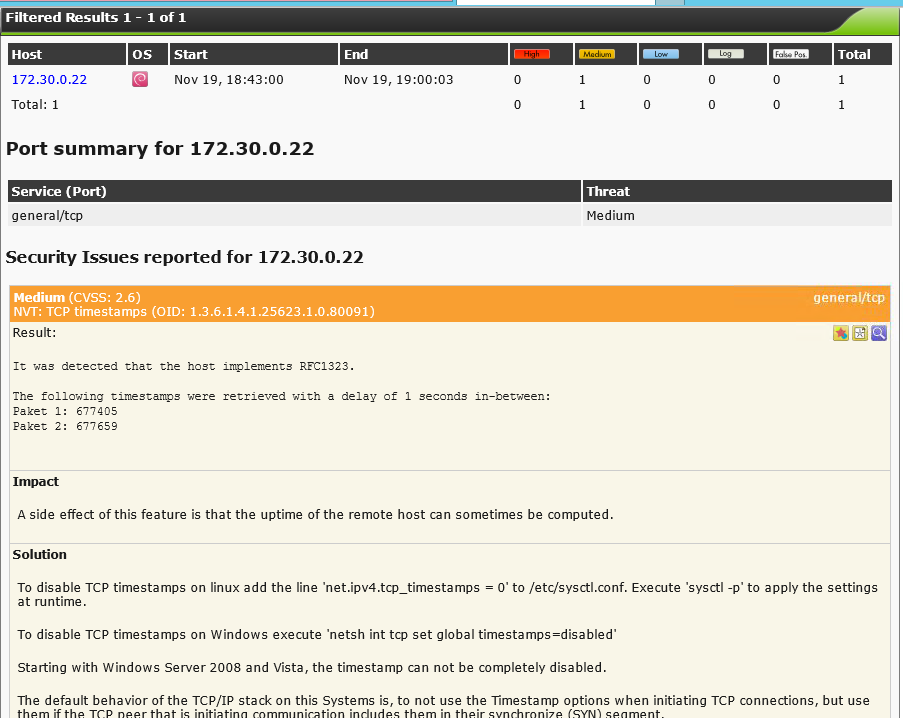
Usually, we will deploy IPS in the following places

* LAN to WAN domain
* The inbound and outbound point of Internet
* The critical devices which requires higher level of protection within our internal network environment.

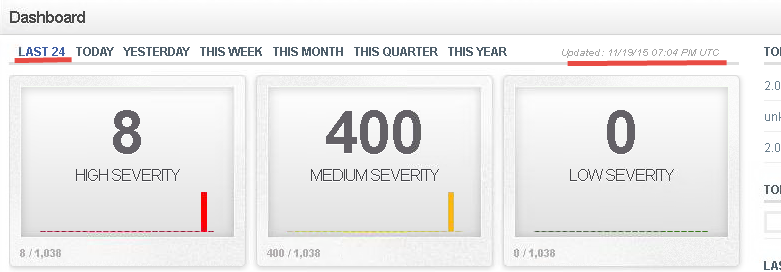
1. Challenge Questions

**Description:**

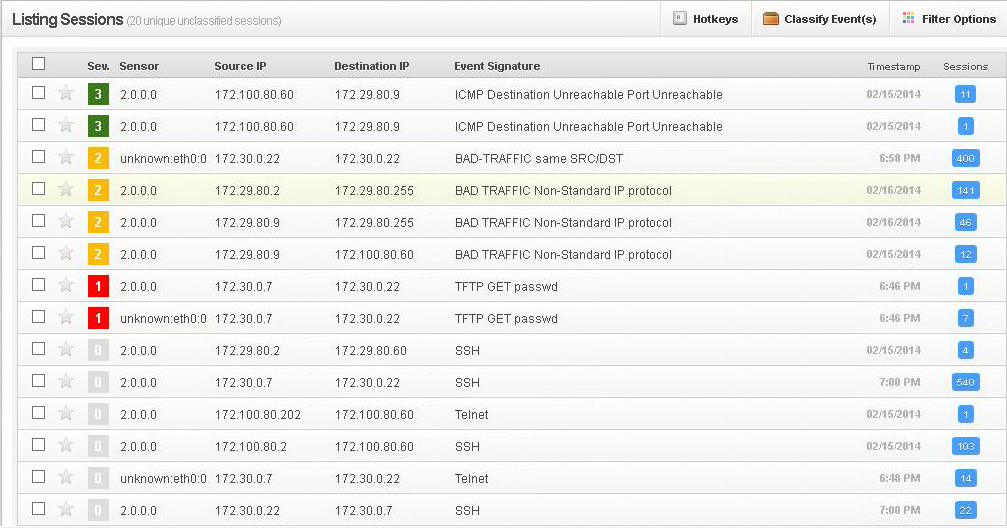
1. Report Screenshot
2. Filtered Results of OpenVAS

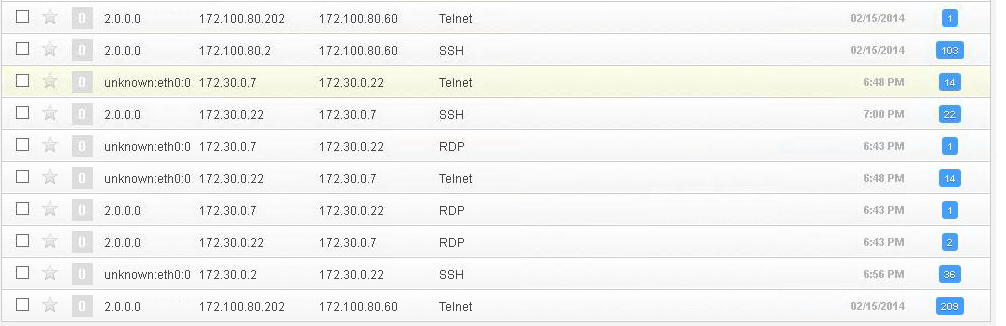


1. Alerts identified by Snort and the date that the report was run

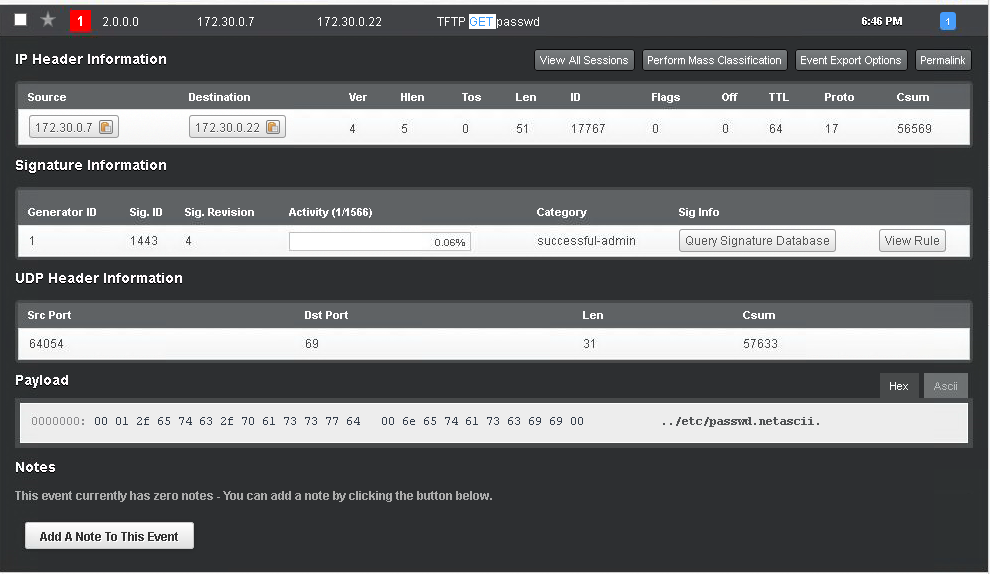


1. Abnormal sessions identified by Snort





1. TFTP GET passwd details



1. Other additional supporting text/image content