**Computer Science 530 - Assignment #2 -- Fall 2013**

In the desktop security mechanism, each host has its own firewall. This means, that there is an essential crunchy layer outside each of the hosts on the network. Whenever there is a compromise (meaning a software application that has malicious code and intends to harm the system) - it can also mess up the inbuilt firewall on the host that it is currently infecting, and also it can interfere with the other software processes that are running on that host. The embedded firewall on a NIC card can prevent this from infecting the entire system. Usually, the host based firewall systems are implemented on systems that are closer to the cluster of data which it is protecting and hence is given more protection.

Signature-based detection works by scanning the contents of computer files and cross-referencing their contents with the “code signatures” belonging to known viruses. A library of known code signatures is updated and refreshed constantly by the anti-virus software vendor.

If a viral signature is detected, the software acts to protect the user’s system from damage. Suspected files are typically quarantined and/or encrypted in order to render them inoperable and useless.

Clearly there will always be new and emerging viruses with their own unique code signatures. So once again, the anti-virus software vendor works constantly to assess and assimilate new signature-based detection data as it becomes available, often in real time so that updates can be pushed out to users immediately and zero-day vulnerabilities can be avoided.

Viruses are generally not brought into the host from the network, but pulled from the outside (when we download any software). A virus is essentially lethal against a firewall, because a firewall is used to protecting from worms, from the network. Virus checking is done when there are known patterns that the firewall recognizes. The desktop security suite shows that the server and client are protected against known patterns against viruses. Only the worms which are on the network which enter the host system are kept from coming in by the firewall. An Intrusion Detection system evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators.

A File Viewer with regex matching called Swatch is used in most signature based detection mechanisms. It provides for pattern matching against known attack patterns. This is used with Snort.

Network-based ID involves looking at the packets on the network as they pass by some sensor. The sensor can only see the packets that happen to be carried on the network segment it’s attached to. Packets are considered to be of interest if they match a signature. Three primary types of signatures are string signatures, port signatures, and header condition signatures.  Based on the components of an IDS, the Network based IDS most commonly uses the notifier and the director whenever there are suspicious packets that flow into the system. The notifier is central to the system.

For an anomaly based component, for the desktop security suite, we can consider the anti-virus software itself (like Avast/ McAfee) to collect all the data. If there are any signs that some software running on the host desktop, the anti-virus software makes a note of it, and places it in Quarantine and tells the user that a virus has been placed there. This is the typical response towards any attack. The user then has an option either to check the contents and say that it isn’t malicious, or can permanently stop files like that from entering the system by changing the firewall policy. Desktop security suites also provide for backup, anti-phishing and anti-spyware, and continuous signature spam updates, to reduce the number of false positives. Signature based detection also allows for

* **Identifies** spyware and adware before they can run on your PC
* **Blocks** unwanted inbound and outbound Internet traffic
* **Filters** unwanted and malicious e-mails and "phishing" web sites.
* **Prevents** most offensive online content, including pop-ups and ads
* **Enhances** privacy with a digital document shredder
* **Updates** automatically to protect against new threats

These are all forms of attacks, wireless malware can transmit through these techniques to enter into the system or Insider attacks.

For a Network based Intrusion detection system, there are quite an alarming number of false negatives, with a signature based detection mechanism. For example, if we take the Snort mechanism, it is a lightweight and simple, easily configurable system. The components are unlike the ones in any desktop suite, it consists of a packet decoder, detection engine and a logging/alerting system. The detection engine uses a set of predetermined rules to see if a packet should be flagged or not. It has a 2 D linked list of chain headers and options.

The anomaly based detection works in sync with the signature based detection, in the way that once a threat or a behavior of a packet is recognized, it becomes a signature. This form of detection has a lot of overhead on the network, because every packet is checked and filtered, and doing exhaustive monitoring uses a lot of resources.

Most NIDS do not have any application/usage when an application in the host itself goes rogue. Since it has already bypassed the firewall and into the host, there is no control from the NIDS over it.

Desktop security protection is better against viruses that the host downloads accidentally, because the NIDS can’t do anything since it is already on the system. If an attack is disguised as several messages, and not just one packet, then the desktop security won’t be able to do much about it, because it mostly relies on signature based detection, and these attacks don’t necessarily cause harm by themselves. An anomaly based detection mechanism in the network, coupled with a signature detection system should be able to stop these kinds of attacks. (called fragmentation attacks)

Examples : (Time based Fragmentation NIDS attacks)

Suppose the IDS fragmentation reassembly timeout is 15 seconds and the system is monitoring some Linux hosts which have a default fragmentation reassembly timeout of 30 seconds. After sending the first fragment the attacker can send the second fragment with a delay of 15 seconds but still within 30 seconds.

Now, the victim reassembles the fragments whereas at the IDS the fragmentation reassembly timeout parameter kicks in and a timeout occurs. Remember, here the second fragment received by the IDS will be dropped as the IDS has already lost the first fragment, due to time out. Thus the victim will reassemble the fragments and will receive the attack whereas the IDS will not make any noise or generate alerts.

Another case of this kind of attack would be:

By default, Snort has a fragment reassembly timeout of 60 seconds. Compare that to Linux/FreeBSD where it is 30 seconds. This can be evaded as well. Consider that the attacker has fragmented the attack packet into four segments: 1,2,3,4.

The attacker sends frag2 and frag4 with a false payload (referred as 2', 4'), which are received by both the victim and the IDS. She waits until the fragments' reassembly timeout occurs at the victim's end and it drops the initial fragments (30 seconds in this case).

The beauty of the attack is that the victim still has not received fragment 1 so it will quietly drop the fragments and no ICMP error message will be thrown by the victim. The attacker then sends packet (1, 3) with a legitimate payload. At this stage, the victim has only fragments (1, 3) whereas the IDS has fragments (1,2',3,4'). Remember that the 2,4 fragments sent by attacker have a false payload.

Since the IDS has all the 4 fragments it will do a TCP reassembly. Also, since fragments 2 and 4 have false payloads the net checksum computed will be invalid. So, the IDS will drop the packet. However, now the victim has only fragments 1,3. If the attacker now sends fragments 2, 4 again with valid payload, the IDS will have only these two fragments (2,4 with a valid payload as the previous fragments have been reassembled and dropped) whereas the victim will have all (1,3,2,4) fragments all with a valid payload, and it will do a reassembly and read the packet as an attack. (Source: Symantec)

A kind of attack that is particularly handled by the NIDS is:

* DDoS- Denial of Service (attempt to make a machine or network resource unavailable to its intended users- the machine could be a server)
* ARP Spoofing
* Zero Day Attacks

A smart configurable Snort with timely responses and previous signature based detection mechanisms would be perfect in stopping these attacks whereas a desktop security IDS wouldn’t be as helpful.

A general overview about the kinds of attacks that a Desktop security IDS could prevent would include attacks against: (on a particular host)

* Trojan Horse - Comes with other software.(similar to working of the battle of Troy – Trojans )
* Virus - Reproduces itself by attaching to other executable files.
* Worm - Self-reproducing program. Creates copies of itself. Worms that spread using e-mail address books are often called viruses.
* Logic Bomb - Dormant until an event triggers it (Date, user action, random trigger, etc.)

In terms of any Microsoft Windows attack by a virus, consider the following situation:

Some viruses disable System Restore and other important Windows tools such as Task Manager and Command Prompt. Many such viruses can be removed by rebooting the computer, entering Windows safe mode with networking, and then using system tools or Microsoft Safety Scanner. System Restore on Windows Me, Windows XP, Windows Vista and Windows 7 can restore the registry and critical system files to a previous checkpoint. Often a virus will cause a system to hang, and a subsequent hard reboot will render a system restore point from the same day corrupt. Restore points from previous days should work provided the virus is not designed to corrupt the restore files and does not exist in previous restore points. (Source :Wikipedia)

Most commonly used process for Responses

– Notify administrator

– System or network lockdown

– Place attacker in controlled environment

– Slow the system for offending processes

– Kill the process