Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Host Intrusion Prevention Systems and Beyond

Copyright SANS Institute
Author Retains Full Rights

AD

Host Intrusion Prevention Systems and Beyond

GSEC Gold Certification

Author: Jonathan Chee, jchee@uhfcu.com

Adviser: Dominicus Adriyanto

Accepted: June 2, 2008

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

1. Introduction.....3

2. What is a Host Intrusion Prevention System and how it works.....4

3. Benefits of implementing an HIPS.....6

4. Implementing, configuring, and tuning an enterprise HIPS

4.1 Implementing a HIPS.....7

4.2 Configuring a HIPS.....9

4.3 Tuning HIPS Alerts.....12

5. HIPS protection compared to IDSs, NIPSs, and anti-virus/anti-spyware.....20

6. New features of HIPS.....21

7. HIPS Challenges.....22

8. Conclusion.....23

9. References.....24

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

1. Introduction

Host Intrusion Prevention Systems (HIPS) are becoming more of a necessity in any environment, home or enterprise. Host Intrusion Prevention Systems protect hosts from the network layer all the way up to the application layer, against known and unknown malicious attacks. Even with today's firewalls, Intrusion Detection Systems (IDS), and other network protection we implement, "hosts are still vulnerable to the myriad of attacks through all the different vectors". (Corman, 2005)

Although anti-virus, anti-spyware, and firewall vendors are changing the way they scan, both are far too often reactive (i.e. Creating signatures and blocking ports and/or IP addresses). We need to start being proactive and start using preemptive measures to stop unknown vulnerabilities. Computers and end users need to start using a combination of preventive measures to protect ourselves and stop designing our defenses with single points of failure. Firewalls, Network Intrusion Prevention Systems (NIPS), and Intrusion Detection Systems (IDS), do not protect hosts from layer 7 attacks. When attacks or probes are fragmented and sent to a host using evasion techniques, firewalls, NIPSs, and IDSs may not be able to block the attack or alert you because they may not interpret what the host may see. In addition, if the attack is trying to exploit an unknown vulnerability the anti-virus or anti-spyware probably will not stop it if it doesn't have the signature for it. This is just one example of why Security Administrators and home users need to use a HIPS.

Here, I will try to provide some insight into implementing, configuring, and tuning an enterprise HIPS. In addition, I'll

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

compare HIPS protection against traditional protection, review new features of HIPS, and lastly, the challenges it still faces. I will be using the IBM ISS Proventia Desktop/Blackice (Home IPS version) HIPS as my example.

2. What is Host Based Intrusion Prevention Systems and how it works?

Host Intrusion Prevention Systems or HIPS is a combination of a personal firewall, IDS, and anti-virus plus something. (Cole, Fossen, Northcutt, Pomeranz, Wright, 2006) IBM Internet Security System's plus something is their virus prevention system (VPS), buffer overflow exploit prevention, IPS (replacing IDS), and application control. The VPS is a proprietary technology that uses behavioral analysis instead of signatures to prevent worms, viruses, Trojans, and spyware.

By combining several preventive measures, users now have multiple layers of protection against various types of attacks. Personal firewall, buffer overflow exploit prevention, and IPS protect against local and network based attacks. Anti-virus, VPS, and application control defend against application based attacks. "A HIPS is like an airport security checkpoint. A variety of technologies look for multiple types of threats, including checking bags and people for weapons and chemical residues, and utilizing facial recognition software to identify wanted individuals. Still to prevent attacks you need some idea of what to look for."(Corman, 2005)

How host Intrusion Prevention Systems work is the "HIPS software uses the shim functionality inserting itself into the operating system to intercept the receipt and delivery of packets on the network." (Cole, Fossen, Northcutt, Pomeranz, Wright, 2006) (See figure 2.1) (Booth, 2007)

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

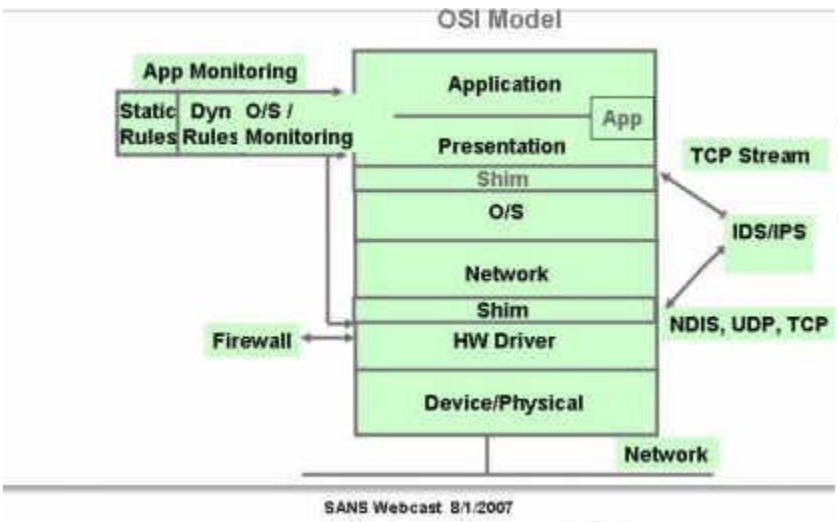


Figure 2.1

Proventia Desktop/Blackice executes files virtually before it reaches the operating system. Once Proventia Desktop has determined that all packets and files are not malicious, it will execute the commands in the live environment. If anything is suspicious or out of the ordinary, Blackice will stop it or flag it, quarantine it, and alert you to examine it further. If the packet or file is an executable, Blackice will ask whether or not to allow it through or to terminate the program. (See Figure 2.2)

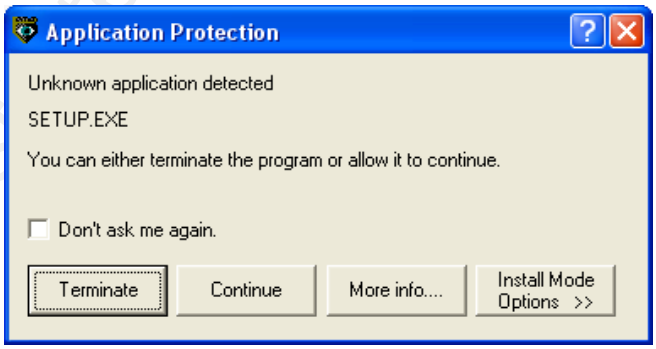


Figure 2.2

This shows exactly what files are attempting to execute.

For unknown/zero-day vulnerabilities, Host Intrusion Prevention Systems separates itself from the firewalls, IDSs, NIPSs, and anti-viruses. By baselining the host and executing

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

the files virtually first, Proventia Desktop learns how the OS and applications should operate. Whether it is installing a new program or simply executing an application, the HIPS should flag out of the ordinary behavior or system calls. In addition, because HIPS systems are anomaly based and not signature based, it has the ability to stop unknown and zero-day exploits by monitoring all traffic on the host and analyzing system calls. Not to say that the HIPS will stop all unknown and zero-day attacks, but depending on how the attack is carried out, HIPS is more likely to stop it than most other protective measures.

Therefore, it does not matter whether or not it is a network or application attack, Host Intrusion Prevention Systems cover most of the attack vectors. Even though a HIPS is protecting a workstation, we still need to remember that there is no one silver bullet that stops everything. Host Intrusion Prevention Systems do have their weaknesses and vulnerabilities such as if the HIPS service is stopped. If the service is stopped then the HIPS is not running.

3. Benefits of implementing a Host Intrusion Prevention System

First and foremost, enterprise and home users now have increased protection from unknown zero-day attacks. Because HIPSs use anomaly detection, there is a better chance that it will stop an attack trying to exploit an unknown vulnerability as opposed to traditional protective measures.

A second benefit of using a HIPS is that the need to be running and managing multiple security applications such as anti-virus, anti-spyware, and software firewalls to protect your PC may be combined into one. Depending on the environment, you may only need to implement a HIPS on the workstation, like Proventia Desktop. Users now have a firewall, anti-virus, anti-

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

spyware protection, and application control in one application. The best part is not having to worry about making sure that multiple security applications work together correctly.

Another benefit is Total Cost of Ownership (TCO). In implementing a HIPS only one security application may need to be purchased instead of three *(again depending on your environment).* Therefore, instead of paying three license and support maintenance costs every year there is only one that will need to be paid. On the other hand, there are additional costs that follow with implementing and maintaining a HIPS, which will be discussed later.

In addition, "HIPS systems provide an advantage for organizations who struggle with patch management challenges and the short window of time between when a vulnerability is announced and when it is actively being exploited."(Cole, Fossen, Northcutt, Pomeranz, Wright, 2006) It provides organizations time to test the patches before installing them on production workstations.

Lastly, because many users are now mobile, there is a pressing need to protect the internal network from the vulnerabilities introduced from mobile users. "Distributing HIPS throughout the organization provides a better method of defending and extending our network perimeter."(Cole, Fossen, Northcutt, Pomeranz, Wright, 2006)

4. Implementing, configuring, and tuning an enterprise HIPS

4.1 Implementing a HIPS

Implementing an enterprise HIPS takes a lot of time and preparation. Whoever will be implementing and configuring the HIPS should have a thorough understanding of how the network is designed, know what applications are being used and how they

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

function. Some applications may need to write to the root of the primary drive, others may need to communicate over specific ports. Whatever the case may be, a thorough understanding of the network is needed or serious problems could arise while implementing the HIPS.

Most HIPS systems are managed by a centralized management console. Proventia Desktop is managed by Site Protector. Within Site Protector there is an Agent Manager which enables the Security Administrator to control what the agents will deny and permit on each workstation. Some specific things that are essential to know before configuring the agent's rules and policies are:

- What ports do the applications communicate over?
- Is the communication between the clients and servers only inbound, only outbound, or both? In other words who initiates the communication, only the servers, only the clients, or both?
- What protocols do the applications use - UDP, TCP, ICMP, etc?
- Are there branches or remote sites that need to communicate with workstations at the main branch? If so, what IP addresses will need to be permitted?

It is also a good idea to check if the HIPS that will be used comes with its own anti-virus. If it does, determine if the HIPS is able to run concurrently with the anti-virus/anti-spyware already being used. Most HIPS systems integrate their own anti-virus/anti-spyware and most likely will not be able to run concurrently with another vendor's anti-virus/anti-spyware software.

A great feature of Proventia Desktop is that it has the flexibility to set different filtering rules. It can filter by

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

IP type, IP address, UDP, TCP, ICMP, or create a custom filter. (See Figure 4.1 Below)

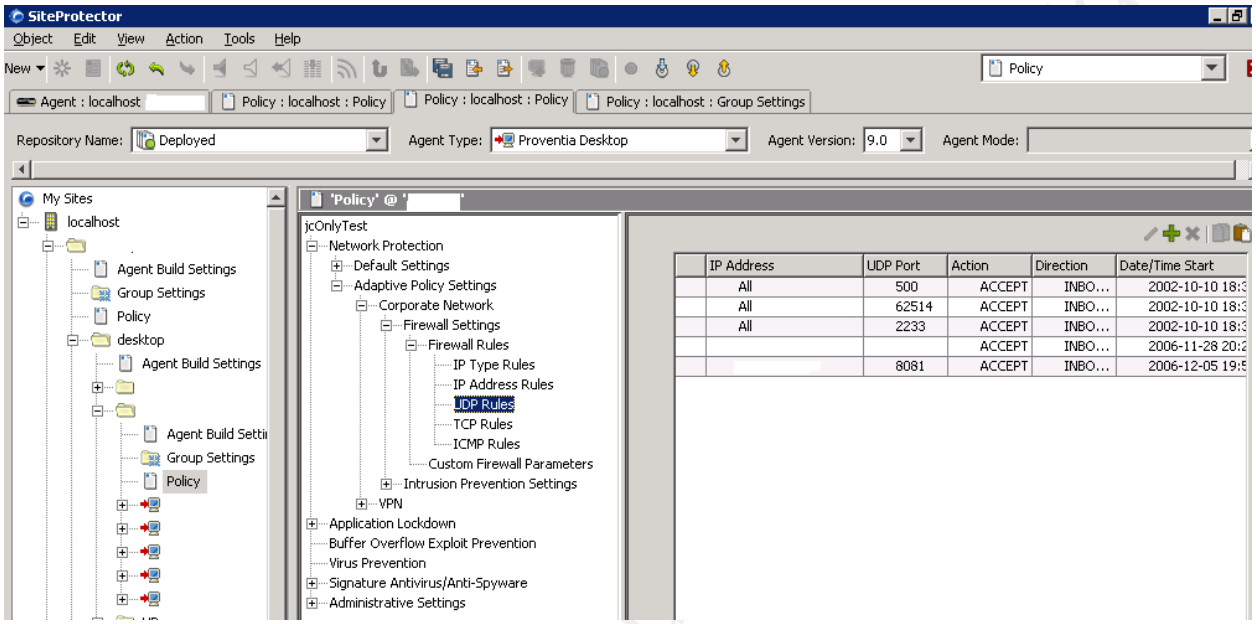


Fig 4.1

For example, lets assume Trend Micro virus scan agents communicate over port 3035. In order for the virus scan agents to communicate with the server, the IP address of the server and port 3035 would need to be permitted under the UDP and TCP Rules in every group.

Therefore, depending on which HIPS is chosen, make sure that it is flexible enough to have the ability to filter by different rules, and control the agents granularly.

4.2 Configuring a HIPS

Once there is a thorough understanding of the applications and their communications, begin creating the groups. If everybody will have the same rules and policies then only one group is needed. For companies that have mobile or remote workers, HIPS systems are very useful. HIPSs are able to provide relatively the same level of protection as internal workstations. Also, a VPN policy for your mobile laptops can be created to make sure they are updated and running. For

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

instance, if the Marketing department uses a mobile laptop with an application that communicates on port 20 TCP, the Security Administrator can create a specific policy that permits only port 20 over VPN. In addition, the policy can be set so that if the agent cannot "phone home" or cannot communicate with the Agent Manager, to not allow the laptop to connect to anything else. "Phoning home" is when Proventia Desktop checks in with the Agent Manager making sure that it has the latest policies and updates. This is one way to ensure that all your agents are up to date and running.

One precaution to make sure that the agent service never stops is to set the agent protection to prevent unauthorized shutdown of the agent services (See figure 4.2).

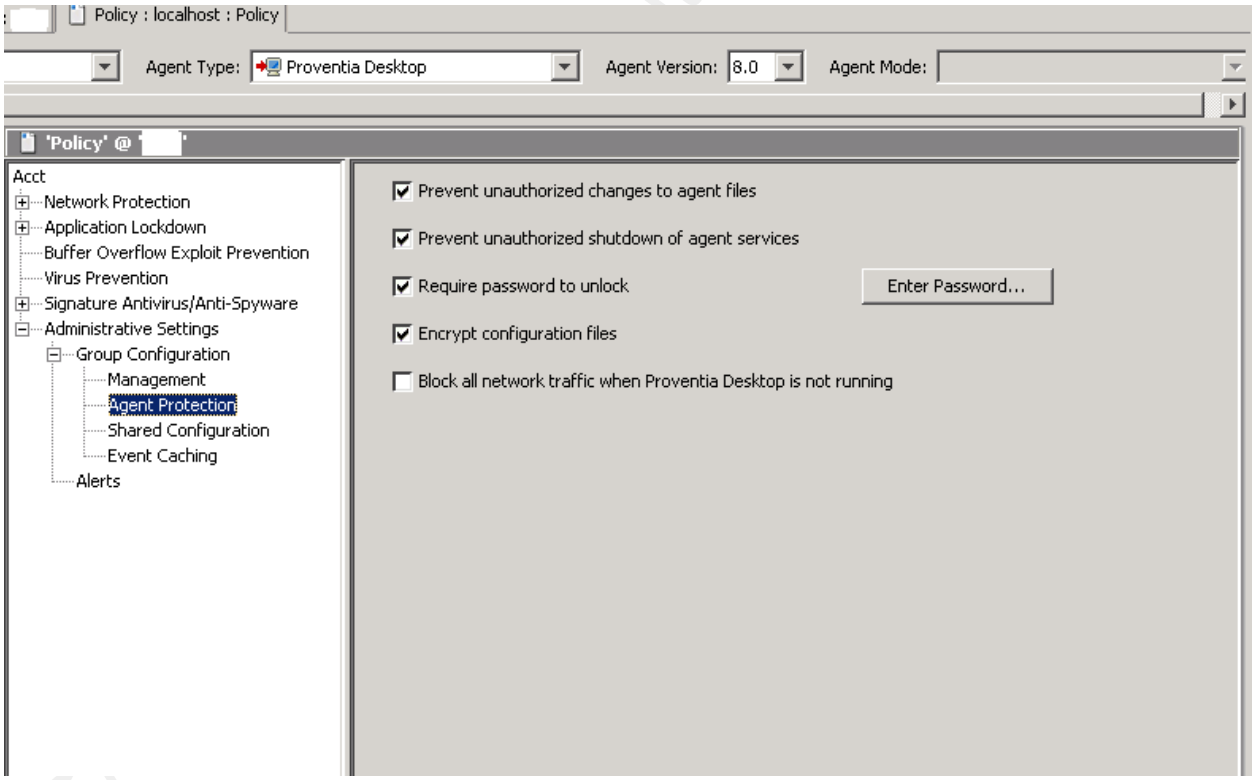


Figure 4.2

This ensures that only administrators can shut down the agent service with a password, if the password option is set. If the password option is not set, anybody with administrative

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

privileges will be able to shut down the service. Additionally, there are options to encrypt the configuration files and prevent unauthorized changes to the agent files. If the password option is set, the agent password must be entered every time a change needs to be made. These options need to be set for each group and each group's password can be different. This works out well for those that would like to delegate control. If only one person will be managing the agents, it is probably not a good idea to set different passwords for each group.

An important thing to remember when configuring the HIPS agents is to implement the most restrictive policy allowed and then permit only what is needed. Never permit everything and then scale back. There is always a chance of missing something leaving the workstations vulnerable to attack.

The next step is to create and assign each group's rules and policies based on the applications that they use. If all the workstations use the same applications or are somewhat similar with just a few additional applications on some of them, copy the policies and modify them so that it will fit specific groups. After the groups have been created with their respective rules and policies start setting up the test environment. Having multiple workstations will be very useful.

During testing, be sure to test all communication that occurs on the workstation within the test environment to avoid any interruptions. For those that have remote sites, it may be necessary to have someone setup duplicated workstations at each site to test the applications and/or communications to and from the remote site. The workstations being used for testing should replicate production workstations. Large enterprises most likely will not be able to replicate all the different workstations, but still need to be sure not to miss any applications being used. If something is missed the HIPS will

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

stop any application not permitted and may cause some disruptions or down time.

Once all applications have been tested thoroughly and made sure that everything will run correctly, start to deploy the agents to your production workstations. While deploying the agents do not deploy them to all the workstations at once. Deploy the agents to workstations that will be least affected if something goes wrong. Also, only deploy the agents to one or two workstations in each department at each site (if there are remote sites). Let them run for a few days or however long is needed to verify that all communication and applications have been permitted. After everything is running smoothly, deploy the agents to the rest of the workstations.

4.3 Tuning HIPS Alerts

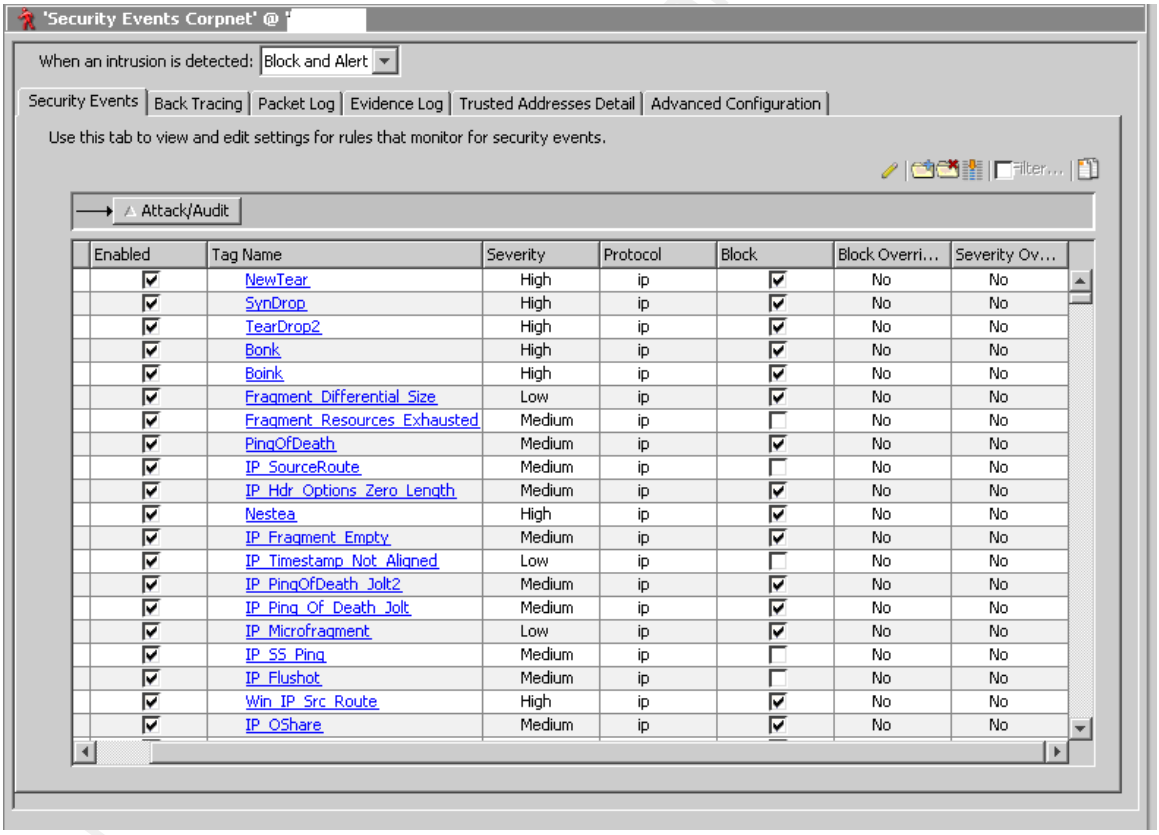
Tuning HIPS alerts will take some time as false-positives have always been a problem with IDS and IPS sensors. When tuning any IPS or IDS alerts, the first thing to do is baseline the alerts. Investigate the alerts and find out which alerts are relevant and those that are not. Begin with the high severity alerts first and then work your way down to the medium and low severity alerts. There may be some alerts that will be triggered and will not apply to the environment which can be excluded quickly.

For example, if there are a lot of Windows attacks being triggered and there are only Linux or Unix operating systems being used, obviously these are false-positives that do not need to be investigated and the signatures could be turned off. Another example is if SNMP or DHCP is being used in the network. DHCP and SNMP traffic will be traversing the network all the time triggering a lot of alerts. It might be better to turn off SNMP and DHCP alerts so that it doesn’t get too annoying. If

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

the alerts need to stay on, think about changing the severity to a medium or low.

Using Proventia Desktop as an example, Figure 4.3 shows a few default signatures that IBM Internet Security Systems provides. They give the ability to enable, disable, block, or override the block for each signature they have. So if an application continuously sets off an alert, but you know it is a false positive, use the option to turn that particular signature off or change the severity on the signature. The general goal of tuning alerts is to not waste time investigating false-positives that are triggered repeatedly.



Enabled	Tag Name	Severity	Protocol	Block	Block Overri...	Severity Ov...
☑	NewTear	High	ip	☑	No	No
☑	SynDrop	High	ip	☑	No	No
☑	TearDrop2	High	ip	☑	No	No
☑	Bonk	High	ip	☑	No	No
☑	Boink	High	ip	☑	No	No
☑	Fragment_Differential_Size	Low	ip	☑	No	No
☑	Fragment_Resources_Exhausted	Medium	ip	☐	No	No
☑	PingOfDeath	Medium	ip	☑	No	No
☑	IP_SourceRoute	Medium	ip	☐	No	No
☑	IP_Hdr_Options_Zero_Length	Medium	ip	☑	No	No
☑	Nestea	High	ip	☑	No	No
☑	IP_Fragment_Empty	Medium	ip	☑	No	No
☑	IP_Timestamp_Not_Aligned	Low	ip	☐	No	No
☑	IP_PingOfDeath_Jolt2	Medium	ip	☑	No	No
☑	IP_Ping_Of_Death_Jolt	Medium	ip	☑	No	No
☑	IP_Microfragment	Low	ip	☑	No	No
☑	IP_SS_Ping	Medium	ip	☐	No	No
☑	IP_Flushot	Medium	ip	☐	No	No
☑	Win_IP_Src_Route	High	ip	☑	No	No
☑	IP_OShare	Medium	ip	☑	No	No

Figure 4.3

Depending on the environment certain alerts may be of importance. Going back to the previous example and assuming that the opposite is true, DHCP is *not* being used in the network and DHCP alerts are being triggered, it might be a good idea to

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

find out where the DHCP request is coming from and why. It may be one of the employees trying to use their home laptop in the network or it could be a malicious person trying to release a worm or Trojan in the network.

In either case, knowing about high severity alerts as soon as possible and finding the cause behind the alerts helps in preventing any malicious attacks from happening or avoiding any possible outbreaks from personal computers ridden with malware.

If static IP addresses are being used, change the alerts to be notified every time a DHCP request is broadcast. To change this in Site Protector go to Proventia Desktop "Security events Corpnet", which is when the agents have "phoned home" to the server, and go to the security events tab (See Figure 4.4).

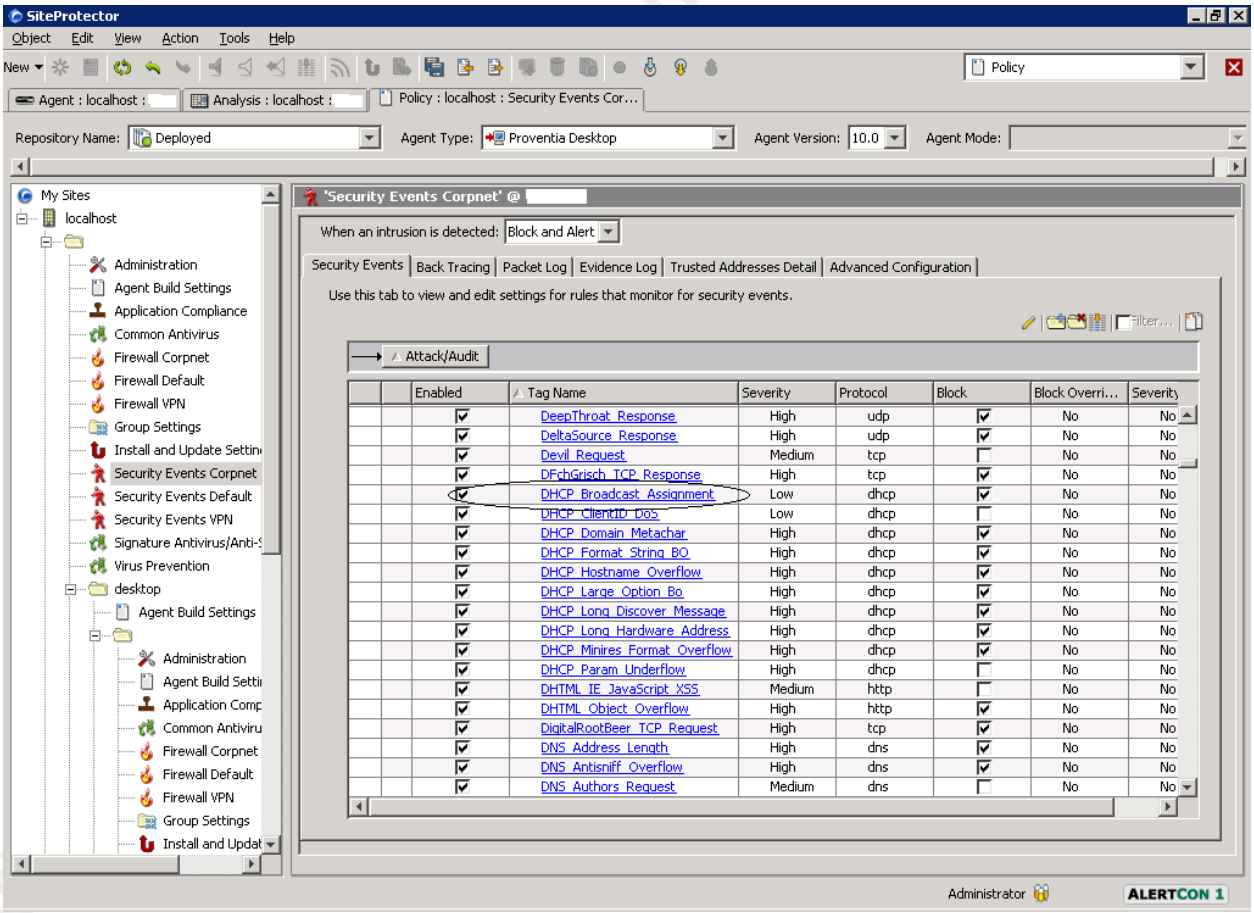


Figure 4.4

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

On the security events tab find the DHCP Broadcast Assignment signature and edit the severity (See figure 4.5).

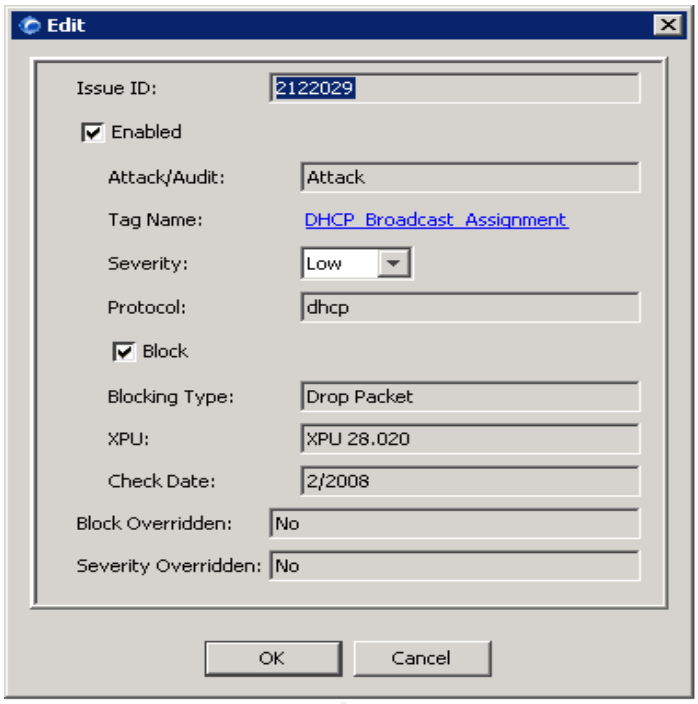


Figure 4.5

Change the severity to high, to be notified about any DHCP requests. This will trigger the alert as a high severity. Why should it be set as a high severity? Two reasons: one, the system should be configured to email the Security Administrator when any high severity alert is triggered. Two, if static IP addresses are being used why is there a DHCP request being broadcasted. After the signatures have been edited, test the alerts by connecting a workstation configured for DHCP and see if it triggers a high alert.

If DHCP *is* being used in the network, think about changing the alert so that it does not trigger at all. Unchecking the signature will turn off the alert. (See figure 4.6)

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

		☑	DCOM_SystemActivation_DoS	Low	dcom	☐	No	No
		☑	DeepThroat_Response	High	udp	☑	No	No
		☑	DeltaSource_Response	High	udp	☑	No	No
		☑	Devil_Request	Medium	tcp	☐	No	No
		☑	~~DFchGrisch_TCP_Response~~	High	tcp	☑	No	No
		☐	DHCP_Broadcast_Assignment	Low	dhcp	☑	No	No
		☑	~~DHCP_ClientID_DoS~~	Low	dhcp	☐	No	No
		☑	DHCP_Domain_Metachar	High	dhcp	☑	No	No
		☑	DHCP_Format_String_BO	High	dhcp	☑	No	No
		☑	DHCP_Hostname_Overflow	High	dhcp	☑	No	No
		☑	DHCP_Large_Option_Bo	High	dhcp	☑	No	No
		☑	DHCP_Long_Discover_Message	High	dhcp	☑	No	No
		☑	DHCP_Long_Hardware_Address	High	dhcp	☑	No	No

Figure 4.6

To change any other default signature to reduce false-positives or false negatives "Security Events Corpnet" would be where to change it. (See figure 4.4)

Another feature to help with tuning alerts is viewing events by groups, if groups have been created. Being able to view alerts and events by groups helps give an idea of what really may be happening with a certain agent or group. Figure 4.7 shows what the general event view may look like. Figure 4.8 shows the events and alerts for a particular group.

Tag Name	Status	Severity	Event Count	Source Count	Target C
HTTP_IIS_Unicode_Wide_Encoding	Detected attack (vuln not scanned recently)	High	12	1	5
Content_Incorrect_Extension	Simulated block (blocking not enabled)	High	7	2	5
Content_Incorrect_Extension	Detected event	High	6	3	1
EventCollector_Error	Detected event	High	5	1	1
MSRPC_Svcctl_Remote_Control	Detected event	High	3	1	1
Brute_force_login_attack	Detected event	High	3	3	3
HTML_Hostname_Overflow	Detected attack (vuln not scanned recently)	High	2	1	1
MSRPC_SuspiciousEncryption	Detected event	High	1	1	1
Content_Compound_File_Bad_Extension	Detected event	High	1	1	1
Brute_force_login_likely_successful	Detected event	High	1	1	1
RPC_CallIt_Unknown	Attack failure (blocked at host)	Medium	2646	1	1
RPC_CallIt_Unknown	Detected event	Medium	589	1	1
TCP_Port_Scan	Simulated block (blocking not enabled)	Medium	408	46	8
TCP_Port_Scan	Detected event	Medium	361	78	22
MSRPC_Pipe_SAMR_Failed	Detected event	Medium	256	1	1
SMB_Winreg_File	Detected attack (vuln not scanned recently)	Medium	101	49	3
All Proventia protection stopped	Detected event	Medium	98	56	56
Rendezvous_Detected	Detected attack (vuln not scanned recently)	Medium	67	1	2
XML_EntityRef_DoS	Detected event	Medium	33	2	2
HTML_NullChar_Evasion	Simulated block (blocking not enabled)	Medium	30	1	4
Logon_process_registered	Detected event	Medium	17	3	3
HTML_NullChar_Evasion	Detected event	Medium	15	1	4
Failed_login-unknown_error	Detected event	Medium	11	2	2
Email_Executable_Extension	Detected event	Medium	10	2	2
Startup_of_important_programs	Detected event	Medium	7	2	2
Computer_account_changed	Detected event	Medium	6	1	1

Figure 4.7

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

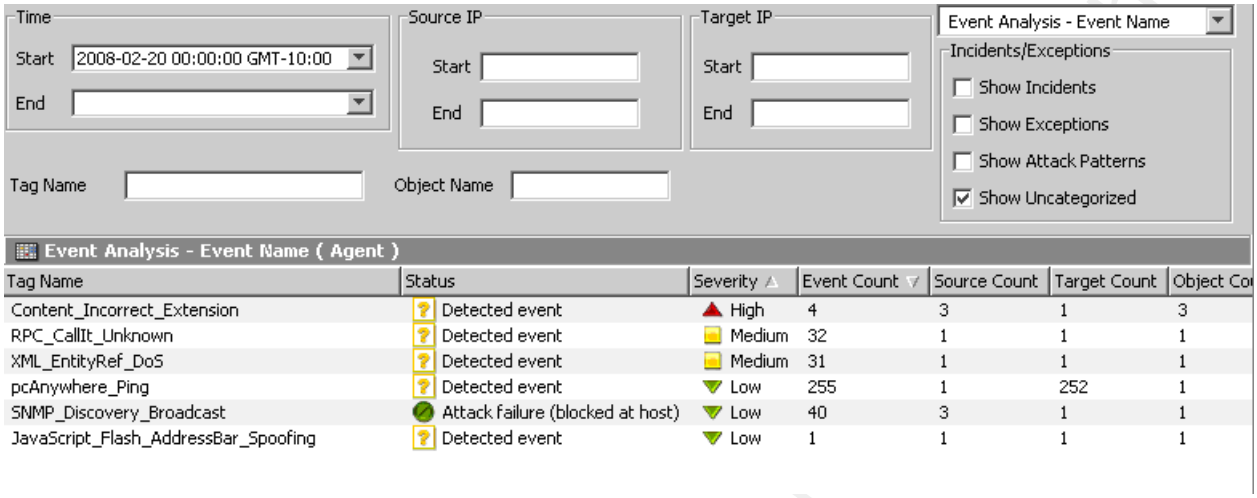


Figure 4.8

In the event that suspicious events or specific alerts are being triggered, there is the option to break it down to a specific group or agent. This may provide insight as to whether or not a particular application on a specific workstation is triggering false-positives or triggered by all workstations.

The next step after configuring the alerts is to configure the notifications. It is critical to know when high severity alerts are being triggered. If somebody is attempting a DoS attack on a workstation and high severity alerts are being triggered, it is imperative to know immediately in order to ascertain the situation and respond appropriately. Therefore, Site Protector needs to be configured to email a notification when high severity events are triggered. To configure notifications in Site Protector go to Central Responses and select Response Objects (See figure 4.9).

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

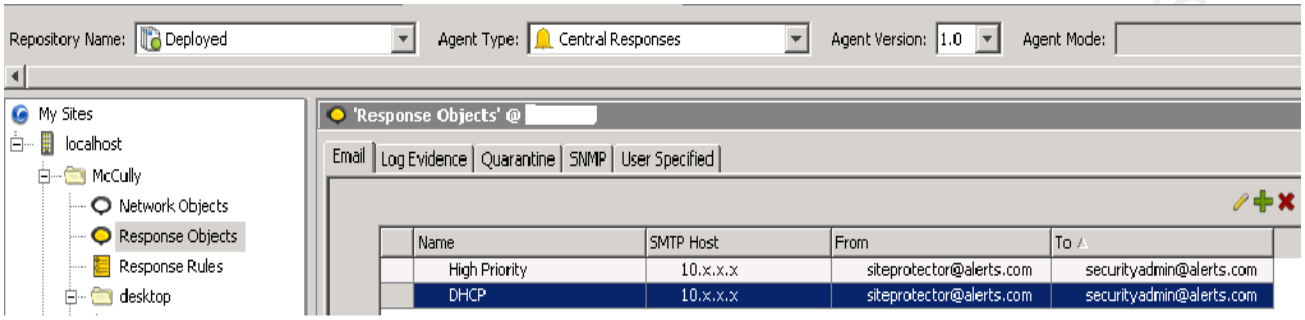


Figure 4.9

Here, add specific alerts such as DHCP alerts, to be emailed when they are triggered.

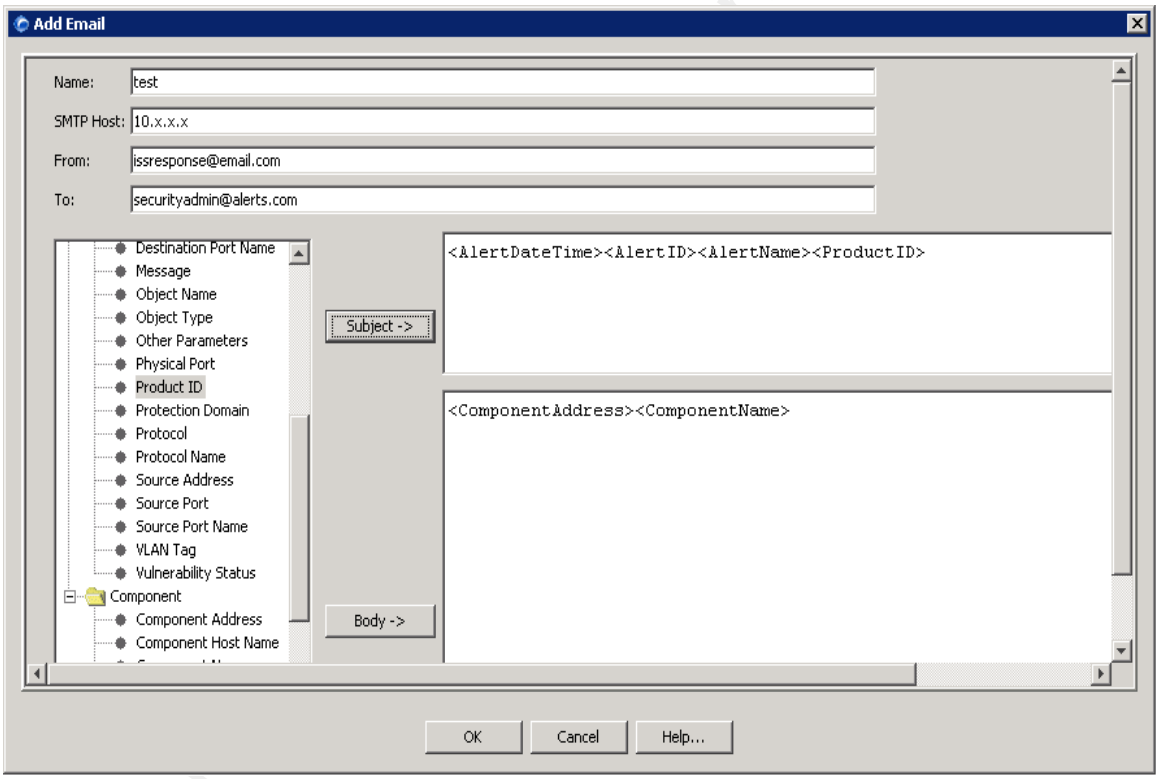


Figure 4.10

Figure 4.10 shows how to customize the email to include specific information about the alert, for example the source address, destination address, the name of the alert (AlertID), Agent Address, etc. This feature can be very useful for those that have handheld devices with access to their email. If a high severity alert gets triggered and Site Protector is configured

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

to email a notification whenever those alerts are triggered, the Security Administrator will know immediately. On the other hand, notifications can be very annoying if the alerts are configured incorrectly. Therefore, Administrators need to be careful when configuring the alerts.

Once all of the agents have been deployed and the alerts are tuned, there is the never ending task of monitoring all the alerts, agents, and event logs. Alerts will also have to be continuously tuned as well as the agents to work with new vulnerability patches and new programs. Each time a new program is added or a new vulnerability patch is released, test it in a non-production environment and determine what needs to be permitted, just as with any other program or patch being added. Make sure that any alerts or signatures that have been turned off do not create any vulnerabilities in the network.

Understanding the applications and knowing what is traversing the network is an essential part in tuning alerts. The more that is known about the network, the faster the alerts can be tuned.

Also, depending on how many and what kind of applications are running will determine how long it will take to tune. The more applications being run, the more false-positives may be triggered. As new vulnerabilities arise, new signatures will follow with the probability that those new signatures will trigger false-positives from your applications. Be sure to check that the new signatures do not overwrite the settings on any current signatures.

To solve the false-positive problem, continue doing what is already being done. Test any new applications or patches in a test environment and see what alerts they trigger. Then make the necessary changes to reduce the false-positives.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

To help understand the overall process of implementing, configuring, and tuning a HIPS, Figure 4.11 shows the steps from beginning to end.

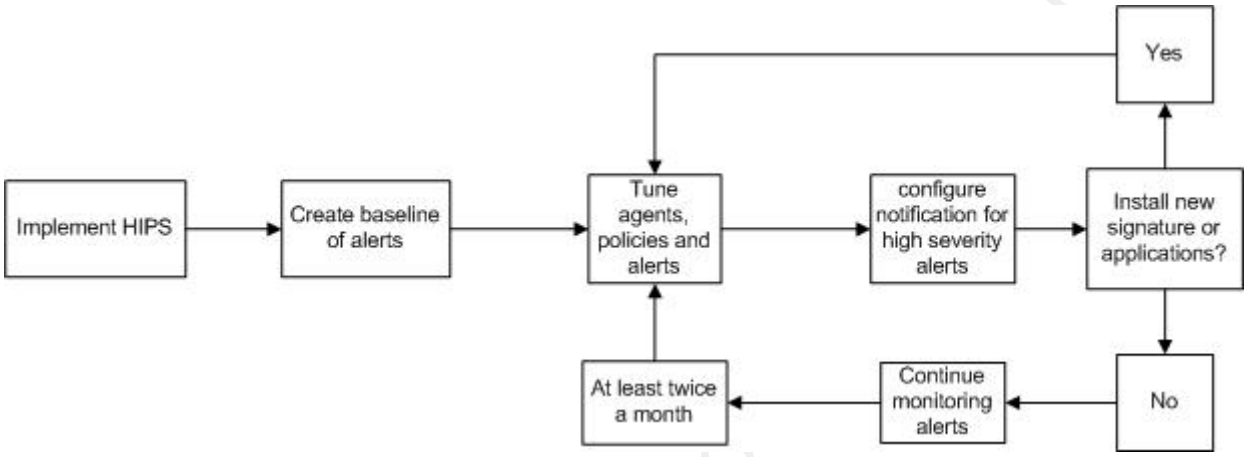


Figure 4.11

5. HIPS protection compared to IDSs, NIPSs, and anti-virus/anti-spyware

So how does HIPS compare to IDSs, NIPSs, and anti-virus/anti-spyware? We will compare IDSs first. IDS is a very good tool to have in your network. An IDS has the capability to tell you exactly what has happened on the network. Where it falls short is that it cannot stop an attack from happening. An event must occur before it will send an alert that there has been an intrusion. Also, if the attack is being carried out on the workstation, the file is fragmented, and it is using evasion techniques, an IDS may not be able to alert on it because the packets are being assembled and interpreted differently than the end host. An IDS is good for alerting and recovery purposes, but unfortunately cannot prevent an attack from happening. Some products such as Tripwire are similar in that it will send an alert and tell you that an attack has happened and what file(s) were changed, but again it is after the fact.

Next we compare NIPSs. NIPSs are a little better than IDSs in the sense that it has the ability to stop malicious attacks,

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

but unfortunately cannot stop or alert on as many things as a HIPS. The reason being, NIPSs cannot afford to have false-positives. Depending on where the NIPS is located within the network, the rules and policies cannot be as restrictive as a HIPS. If the NIPS is triggering false-positives, it could create a DoS on the network. Legitimate traffic may be trying to get through, but the NIPS may be denying that traffic thinking it is malicious.

In addition, both IDSs and NIPSs are unable to see inside encrypted traffic. Because both are unable to see inside encrypted files, neither can stop or alert on any encrypted files. All they can do is pass the files on to its destination.

Lastly, there are anti-virus and anti-spyware protection. Anti-virus and anti-spyware vendors have made great strides in how they scan for viruses, trojans, worms, and spyware, but still rely heavily on signatures. This is where the protection is weak. If somebody does not send in logs for an attack or the vendor does not discover the new virus or spyware, a signature cannot be created for it. Yes, they do scan and stop known viruses, trojans, and spyware, but they lack the ability to stop the unknown which is where everybody is the most vulnerable. What you don't see can hurt you.

Thus, HIPS protects hosts in ways that other types of protection cannot. This is not to say that IDSs, NIPSs, anti-virus, and anti-spyware are not needed. All should definitely be used, but if it is not feasible to have all of them or if you are deciding what to spend the budget on first, this should give an idea of where to start.

6. New Features of HIPS

New features HIPS vendors are releasing target new vulnerabilities that are being exploited in today's

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

environments. Take for example Computer Associates (CA) HIPS. Their HIPS features such things as restricting USB devices, alerting and denying any confidential information being copied off to USB/CD/DVD, or when infrared devices are being used. Another feature being used is "Dynamic rule creation for custom applications where applications that have not been thoroughly analyzed by vendors for analysis, detection techniques are put into a learning mode. In learning mode the HIPS learns how the workstation operates, what files are allowed to be altered, what system calls are being made, keys accessed, etc."(Cole, Fossen, Northcutt, Pomeranz, Wright, 2006)

7. HIPS Challenges

Like any other protective measure, HIPS has its fair share of challenges. "Plaguing HIPS deployments are implementation and maintenance challenges – testing updates, deploying updates, troubleshooting updates etc." (Cole, Fossen, Northcutt, Pomeranz, Wright, 2006) Yes those are quite concerning, but none are more important than false-positives. Like NIPSs and IDSs, HIPSs have problems keeping false-positives to a minimum. In some cases, false-positives may become so annoying that the alerts are ignored because it is triggered too often. Security administrators should never let it get to this point because once alerts are ignored there is no point in having alerts. It defeats the purpose of having alerts.

To prevent this from occurring a constant tuning of the alerts is needed, at least twice a month if not more. Depending on how often applications are added or workstations are updated with vulnerability patches.

Additionally, the cost of actually implementing an enterprise HIPS could be cost prohibitive. Not only is there the cost of the product itself, there is also the amount of

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

hours it will take to implement, whether it be internal staff or a consultant. Also add in the cost of managing the system. Is there adequate staff as well as the training to be able to manage the system once it is implemented? Will the Security Analyst understand what the alerts mean when it is triggered? These are just some of the challenges HIPS still face.

8. Conclusion

With a plethora of vulnerabilities out there, security administrators need to constantly mitigate the risks associated with the ever changing environments and applications being introduced. As you can see, Host Intrusion Prevention Systems are an invaluable tool, but we need to remember that it is not the "silver bullet" for workstation security. “They can be a great addition to a solid, layered defense including firewalls, NIPSs, IDSs, and anti-virus applications among other things, but should not replace them.” (Bradley, 2005)

“As each host protection technology possesses strengths and weaknesses, selecting just one technology for comprehensive host protection results in too much risk to the host environment. Any single technology represents a singular point of failure. Employing the different technologies in concert brings risk exposure to threats down to acceptable levels. In addition, combining multiple host protection technologies into a single host protection solution significantly reduces management costs. When developing a host protection strategy, only a comprehensive solution can keep you ahead of the next threat.” (Corman, 2005) Are your hosts protected from the unknown?

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

9. References

Corman, December 29, 2007 (2005). Defining the Rules for Preemptive Host Protection:. from iss.net Web site: http://www.iss.net/documents/whitepapers/ISS_Preemptive_Host_Protection_Whitepaper.pdf

Cole, E, Fossen, J, Northcutt, S, Pomeranz, H, Wright, J (2006). *SANS Security Essentials*.SANS Institute.

Booth, Patricia (2007, August 1). Tool Talk Webcast: Host Based Intrusion Prevention (HIPS), what does it do for me?. Retrieved February 17, 2008, from www.sans.org Web site: https://www.sans.org/webcasts/access.php?id=91296&pid=21e2dc296e4f5df5edfec8744017f63f2109b9a038e488aaf775ae7c339b79ba#

Bradley, T (08/04/2005). Things To Look For In This Last Line of Defense. *Host-Based Intrusion Prevention*, Retrieved 2/27/08, from http://netsecurity.about.com/cs/firewallbooks/a/aa050804.htm

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced