Active Security Or: How I learned to stop worrying and use IPS with Incident handling

Doug Brown

ACTIVE SECURITY OR: HOW I LEARNED TO STOP WORRYING AND USE IPS WITH INCIDENT HANDLING

GIAC (GCIH) Gold Certification

Author: Doug Brown, dougb@hp.com
Advisor: Rob VandenBrink

Accepted: December 30, 2013

Abstract

A highly customized use of Intrusion Prevention Systems (IPS) will benefit organizations throughout the incident handling process. Considerations for incident preparation, identification, containment, eradication, recovery, and lessons learned are provided. This paper focuses on the HP TippingPoint IPS technology in the incident handling framework. Intrusion prevention has a critical role feeding information into the narrative any security incident, and improving the overall security posture of the protected organization.

1. Active Security through Prevention

Beyond the obvious nomenclature for viruses and worms, several lessons can also be gleaned from the world of epidemiology and applied to information security. Although most parents agree that rigorous vaccinations will not stop every illness, an old aphorism still illustrates one of these lessons: “An ounce of prevention is worth a pound of cure.”

Although no practical prevention will completely eliminate security incidents, the considered use of the right prevention technologies will provide benefits throughout the incident handling process. Security incidents are complex narratives told from different perspectives throughout an organization. Each involved desktop, server, router, switch, and firewall may reveal some portion of the story for each incident. Achieving a more nuanced narrative for an incident involves the inclusion of different story tellers, the possible addition of different device types, and well-researched decision making about filter usage and detection priorities.

Whereas many different tools would be worthy of inclusion, this paper will focus on fully integrating the Intrusion Prevention System (IPS) within each phase of the organization’s incident handling framework. Specifically, this paper focuses on the HP TippingPoint IPS, a leader in the Gartner Magic Quadrant for IPS (“HP TippingPoint positioned,” 2012). Some of this functionality may also exist on other IPS solutions not covered herein.

The HP TippingPoint IPS solution functions differently from traditional Intrusion Detection Systems (IDS). Whereas an IDS may serve an important role in revealing portions of the security narrative, as a passive device an IDS generally only detects events and records them for later review. This passive detection lends itself to a different level of rigor in filter writing: principally, a higher tolerance for false positives. Contrast this with the HP TippingPoint IPS, which functions best as an in-line device that makes active decisions about packet disposition based upon the configured filter policy. This in-line usage of the IPS necessitates different types of filters from IDS-based solutions and a dedication from HP TippingPoint to providing accurate filter results with almost no false positives ("HP TippingPoint DVLabs," 2013). These fundamental differences between the IDS and IPS type filters allow for a fuller security narrative but also necessitate that the IDS and IPS solutions be considered independently and not confused with each other. This IPS solution is not simply active IDS.

2. Incident Response

2.1. Preparation

During the Preparation phase of Incident Handling, defining what is normal for an environment at the outset allows for later recognition of the abnormal. The process of establishing the baselines, policies, and procedures for information security and incident handling at the outset yields great benefit later. This advance work will likely also reveal some supplementary changes that can further support complete prevention of many incidents and faster recognition of the incidents that do occur. During the preparation phase, a review of exposures is appropriate. One method for an exposure review is the Know-Limit-Protect (KLP) methodology, which includes the steps detailed below.

2.1.1. Know the Exposures

Baseline audits, inventories, and vulnerability assessments of systems may reveal opportunities for improvement. Configuring an appropriately sized IPS with a majority of the filters enabled using detection protocol only, or "Permit + Notify" action, allows for the deeper discovery of the types of network transactions being performed and the systems involved. This process can also identify surprise applications that may be present in the environment, such as user-installed downloads that are outside of organizational norms or unpatched applications installed on servers for some long-forgotten test.

2.1.2. Limit the Exposures

By turning off or removing all unnecessary services from systems, fully patching any remaining services, and configuring the firewall to deny everything that is not explicitly allowed, external exposures can be significantly limited. Utilizing an inline IPS, "Traffic Management"-type filters can also be configured to provide packet filtering: allowing, denying, or trusting transactions based upon the protocol, source, or destination information specified.

2.1.3. Protect Any Remaining Exposures

Inline IPS is particularly well suited for defending any necessary exposures that may remain, such as ports 80/TCP and 443/TCP to webservers. Research and review of the available IPS filters will provide additional filters specific to the protection of the exposed applications or operating systems. Once identified, activated, and tested, these IPS filters employing a "Block + Notify"-type action add another layer of defense for the exposed assets, such as providing deep packet inspection and protection for the Apache vulnerabilities related to a hypothetical web farm.

The HP TippingPoint IPS solution ships with a default profile that enables approximately 2300 filters for items that should never legitimately exist on a network, including certain attacks such as buffer overflows as well as malicious downloads. In addition to these default filters, more than 5400 additional filters, broadly considered policy choices, are available for use based on the requirements of the protected environment.

Reviewing this additional body of non-default filters allows a significant level of customization to the IPS implementation. OS- and application-specific filters are just one example of this further customization. For the Apache example, this IPS solution includes 35 default-enabled filters with 74 additional non-default filters of varying criticality for events such as information disclosure from misconfigured servers and cookie handling denials of service.

2.2. Identification

Omnipresent attacks against the protected environment provide a steady stream of event data that has traditionally been sourced from external hosts to the destination of the protected network. Like background noise on the Internet, these non-specific external attacks will always occur. When hosts internal to the protected network begin triggering events for similarly undesirable activities, a successful attack or other harmful incident may be the genesis. For this reason, leveraging the concept of "directionality" within the protected environment allows rapid separation of events between "inbound" (events triggered by external hosts) and "outbound" (events triggered by internal hosts) and permits the use of different filter policies based upon traffic origin. IPS filter policies can be further customized using the HP TippingPoint features of "Policy by CIDR" and "Policy by VLAN." As an example, these could be used to apply specific policy filters to server systems that may not be desirable for user systems, as explained below.

The HP TippingPoint default filters trigger for events such as buffer overflows or command injections. Detecting these events originating from the internal systems, or outbound from the network, provides an immediate indication that an incident has occurred and further containment may be necessary. Beyond those default filters, the addition of various policy-type filters allows identification of other behaviors that may indicate either an incident or a deviation from best practices. Some examples of additional filters to consider are the following:

3972: HTTP: Windows Executable Download
4653: HTTP: Executable Attachment Download via Webmail
5437: HTTP: Windows Executable Download Spoofing
6109: HTTP: Malformed Windows Executable Download

Specifically, the filter 3972 can either alert on, or completely prevent, the download of any Windows executable files (applications) over HTTP. Some organizations block executable downloads for their entire environment; however, this may create an additional support load to field user requests. A more measured approach of generally allowing such downloads for most user systems could be differentiated from any web browsing or downloading directly from a server console, which would certainly fall outside of best practices. Following this more measured approach, an option might be to enable these filters and others like them only for the server systems using a CIDR- or VLAN-based policy. Defining the allowed behavior for the protected servers and enabling these additional filters allows for the rapid identification of any compromised system that is attempting to download additional malicious items such as any key loggers, Trojans, remote shells, or command and control software.

These types of download filters are not limited to HTTP or Windows Executables. Many downloads can be recognized over several other protocols, such as the following:

3078: SMB: Suspicious JPEG Image File Download

5944: FTP: FTP GET/MGET Commands

6945: TCP: Microsoft Windows Executable Transfer Over High Ports

6946: TCP: Suspicious File Transfer

9146: FTP: Malicious File Transfer

10473: SMB: Malicious .scr File Download

11287: SMB: Malicious Windows Metafile Download

11793: TFTP: File Download Attempt

Beyond attempted downloads, at this stage of incident identification, several additional filters can also indicate any attempts to exfiltrate data from the compromised system or the organization. Some of these include the following:

1565: Tunneling: Data Transfer Using socks2http

1569: Tunneling: httptunnel Data Transfer

1570: Tunneling: Fire Extinguisher Data Transfer

1591: Tunneling: HTTPort Data transfer

2232: FTP: anonymous User Login

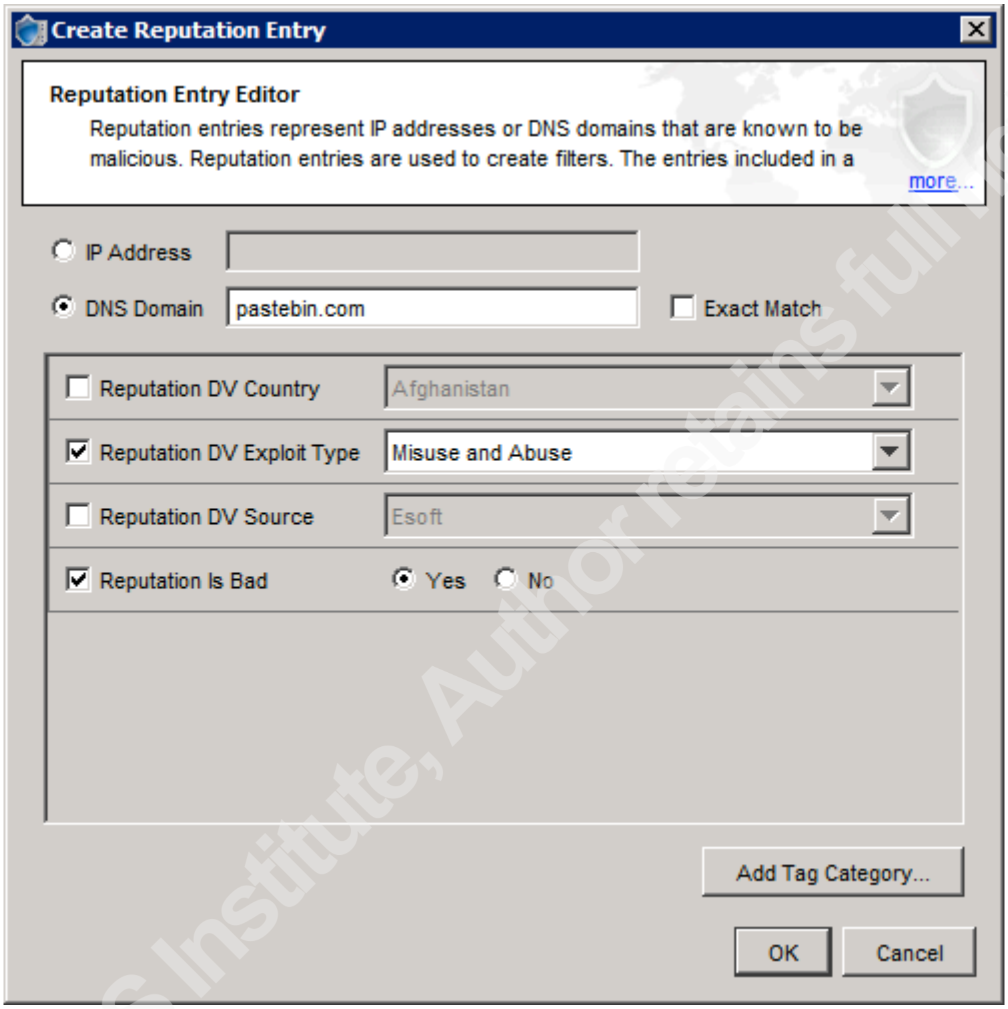
2233: FTP: ftp User Login

4904: TFTP: PUT Command

5943: FTP: FTP PUT/MPUT Commands

11731: HTTP: Megaupload File Upload

Other potentially suspicious events, such as access to "Pastebin," can also be recognized and prevented using other IPS tools such as the "IP/DNS Reputation" functionality to alert on, or completely block, access to those specific sites. This TippingPoint IP/DNS Reputation service is a blacklist of more than one million hosts known as botnets, spam hosts, phishing sites, or sources for other malicious activities ("Reputation"). Updated several times each day from multiple sources, this service also provides another advantage: the ability to add additional entries for any points of concern, such as the example below for Pastebin.



Reputation Entry Editor

Reputation entries represent IP addresses or DNS domains that are known to be malicious. Reputation entries are used to create filters. The entries included in a

○ IP Address

● DNS Domain: pastebin.com   □ Exact Match

□ Reputation DV Country: Afghanistan

☑ Reputation DV Exploit Type: Misuse and Abuse

□ Reputation DV Source: Esoft

☑ Reputation Is Bad: ● Yes ○ No

2.3. Containment

The throughput capacities of HP TippingPoint IPS units generally allow for multiple segments of a protected network to be inspected. Beyond the inspection of traffic inbound and outbound on the network perimeter, the inspection of traffic between the network core and the server VLAN or within user network segments allows the use of IPS to subdivide internal networks into “Attack Domains” (i.e., smaller areas within the network in which problems can spread before being stopped by IPS inspection). A problem with a user’s system can be isolated to a small portion of the user network, thereby preventing it from impacting any of the organization’s servers. Although this subdivision into Attack Domains is effective in limiting the size of many multiple-casualty incidents, this type of containment becomes a fixed fortification of sorts. As American General George Patton famously quipped, those become “a monument to the stupidity of man” (Weir, 2007).

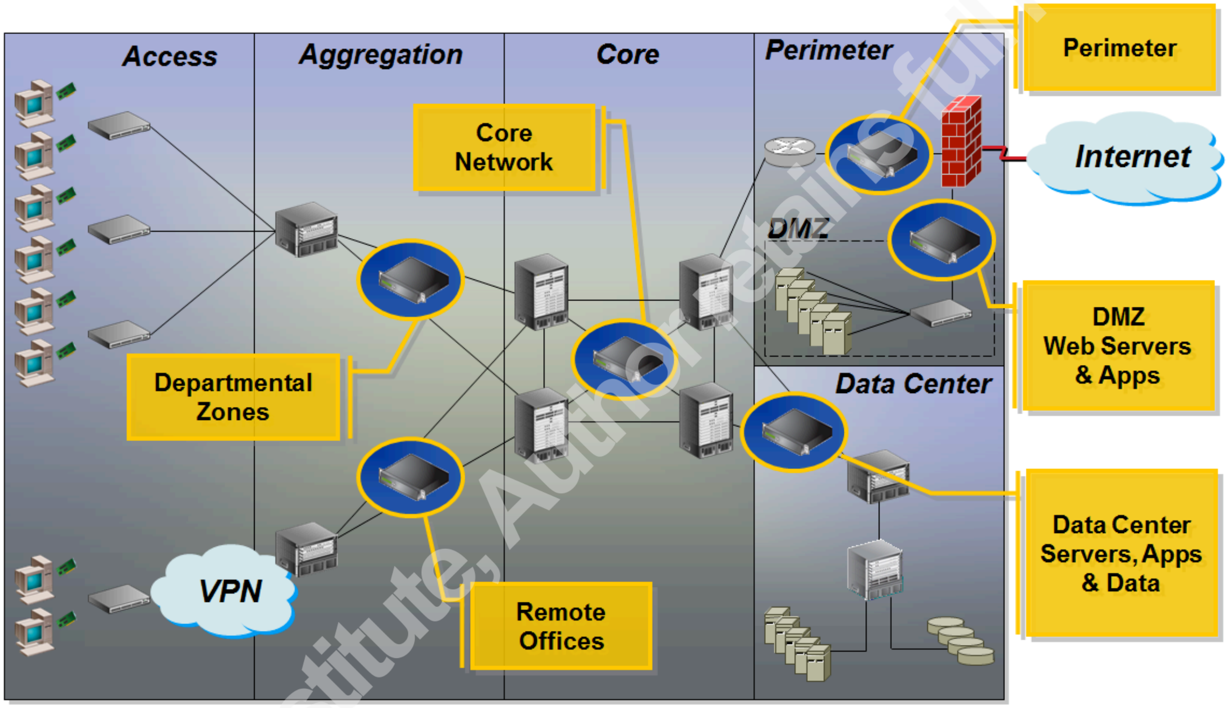


Figure 1 - Attack Domains

The goal of containment should always be to limit an incident’s size to a single system. With the HP TippingPoint solution, this singular containment can be accomplished through the use of the “Responder” functionality. Responder was built to provide a vendor-agnostic way for the IPS environment to integrate with the rest of an organization’s infrastructure, such as the network switches. Responder is configured to recognize IPS events, such as matches to particular filters of special interest or concern, as inputs. Then, based on those inputs, Responder executes customized actions, or outputs. These actions may include isolating affected systems in a different VLAN or executing a "switch disconnect" (interface shutdown) to remove a system completely from the network.

Incidents happen quickly. Using Responder to accomplish incident containment provides the added advantage of significantly decreasing reaction time over anything recognized and manually executed by a person. Responder never sleeps. In the scenario described above, Responder could trigger on those download or upload attempts from the most sensitive systems and isolate the system causing the match, likely stopping the theft of the organization's most sensitive information.

Another benefit of using Responder is in correlating a series of events potentially originating in different parts of the organization or even detected on different IPS units. The HP TippingPoint IPS solution offers several non-default filters in which detection of a single event may be insignificant, but a repeated series of events clearly indicates a problem. Some of these filters are as follows:

1401: MS-SQL: Login Failure
1660: SMB: Windows Logon Failure
2796: SMB: Windows Repeated Logon Failure
12850: SSH: SSH Login Attempt Server Response

Recognizing that actual users are highly unlikely to type their password incorrectly more than five times within a two minute window allows for the configuration of Responder to distinguish and isolate brute force attempts by correlating specific events and reacting only when a threshold of too many events is crossed. The penetration technique of running the list of most common passwords against known accounts would be identified and stopped quickly using this method, whereas normal user activity of occasionally failing to type a password correctly would not trigger isolation.

2.4. Eradication

After a security incident has occurred and been contained, the process of further unraveling the complex narrative begins. Answering "The Five Ws" (i.e., who, what, when, where, and why) may be employed as a common starting point to unravel the full narrative through investigation. Another approach may be to simply follow the mantra of French essayist Michel de Montaigne and ask “Que sais-je?” roughly translated as “What do I know?”), and from the basis of known facts, one can investigate and scrutinize what transpired with each incident (“Michel Eyquem de Montaigne”).

Ideally, an accurate baseline of the compromised system(s) exists. Host-based IPS tools like Tripwire excel at creating these baselines and allowing the rapid identification of any changes to the system, such as answering fundamental questions like what has been added and what has been changed? In the absence of a Tripwire-like tool, the best alternative to ensure a clean host may be either a backup restore or fresh install; however, these would only be an option if other tools reveal the exact “when” of the original compromise, and a safe method exists for bringing any missing data current. With their increasing complexity, all of the layers and hidden elements of the full compromise will likely not be apparent. The network tools also play a role in this eradication process. Identifying unauthorized inbound communication to the compromised host reveals ports and protocols (e.g., “what service was responsible for this host answering SSH on port 7000?”) and allows the process of fully identifying and removing that backdoor to begin. Pinpointing unauthorized outbound communication from the compromised host can reveal which particular piece of malware was involved.

Using the SSH example from above, a few examples of IPS filters that can help to identify these transactions are as provided below. Filters for inbound communications include the following:

5601: SSH: SSH Login Attempt Client Request
5706: SSH: SSH Login Attempt On Non Standard Ports
9944: SSH: SSH Login Attempt On FTP Port
9945: SSH: SSH Login Attempt On SMTP Port
9946: SSH: SSH Login Attempt On DNS Port
9947: SSH: SSH Login Attempt On POP/IMAP Ports
9948: SSH: SSH Login Attempt On HTTP Ports
9949: SSH: SSH Login Attempt On RDP Port

9950: SSH: SSH Login Attempt On VNC Port
12850: SSH: SSH Login Attempt Server Response

The first and last filters in the above list, and other similar filters for different protocols, may possibly fire on legitimate traffic if the host legitimately runs that service. However, using such filters will help complete this security narrative. For those cases in which a host legitimately runs that service, each filter includes "Filter Exceptions" where expected transactions can be excluded from firing the filter. For example, SSH from administrative desktops may be normal and an appropriate exception, whereas SSH from hosts in Luxembourg may be worth blocking or at least investigating.

For outbound communications, some useful filters include the following examples:

9534: Backdoor: Spyeye Botnet Command and Control Phone Home Request
9536: Backdoor: Zeus Botnet Command and Control Phone Home Request
9731: Backdoor: Gumblar Botnet Command and Control Request
9879: HTTP: Sasfis Botnet Command and Control Request
10483: Backdoor: Zeus Botnet 2.0 Client Registration
10487: Backdoor: Zeus Botnet 2.0 Phone Home Request
12410: Backdoor: Zeus (Aeacus Variant) Botnet Command and Control Initial

If the filters listed above have fired, this can point to a particular piece of malware being used on the compromised host. Following up with knowledge about that piece of malware, its place in the narrative, and recommendations for the removal of that malware will aid the eradication process.

2.5. Recovery

Once the security narrative is complete, the investigation and cleaning of the compromised host is concluded, and eradication is deemed successful, then the process to return it to service may begin. Was the original vector of compromise fully identified and mitigated? The attacker may likely attempt to return. Additional monitoring and protection of the compromised host is advisable. That security narrative can bolster the process of identifying additional IPS filters to enable, fine-tuning the policy for other security mechanisms such as the firewall, and enabling additional logging at the host and network levels. Based upon any identifiable elements that point to the attack's signature, custom IPS filters may also be written to enhance the additional protection. Even an old passive IDS system may play a useful role with a simple filter to log all traffic from outside the network to the compromised host. Some key elements of the recovery should include full confidence in the eradication process, the expectation of further attacks, and additional measures to monitor and protect.

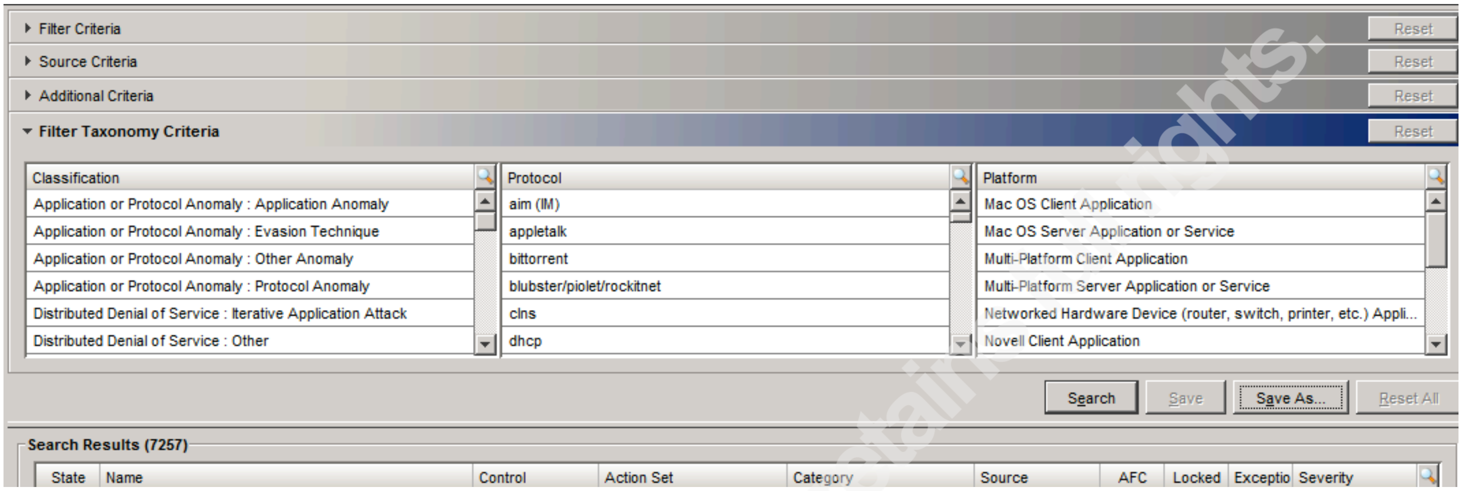
Another tool provided by the TippingPoint IPS, and possibly other devices in the environment, to assist this monitoring and recovery process is SFlow. The newest TippingPoint IPS devices include SFlow collector capabilities. Through the statistical sampling of network traffic, SFlow allows information such as "top talkers" or "top applications" to be tracked and provides the data sets necessary for deeper forensic analysis of the network traffic ("Inmon Technology"). Although the proactive use of SFlow may help during the Identification phase of the incident, the use of it here for enhanced monitoring during recovery drives to a desirable outcome.

2.6. Lessons Learned

By the post-mortem phase of incident handling, hopefully much more is known about the incident's origin, which exposures were vulnerable, and what the attacker hoped to accomplish through the attack. The broadest possible narrative of the security incident has been completed. This knowledge of the incident provides another feedback loop for further fine-tuning the IPS filter policy:

- Which tools or vulnerabilities were involved in the initial incident?
- What additional tools or protocols were installed or used by the attacker?
- What bonus filters could be enabled on the IPS to prevent this in the future?

With an additional pool of several thousand filters available for activation, the IPS policy should be further customized to the organization and likely threats. Referencing back to the known facts of the security narrative, the multi-faceted search capabilities of the solution allows for the further identification of beneficial filters and the capability to write new custom filters tailored to the attack. The image below shows a portion of these search capabilities with different levels of criteria:



Classification	Protocol	Platform
Application or Protocol Anomaly : Application Anomaly	aim (IM)	Mac OS Client Application
Application or Protocol Anomaly : Evasion Technique	appletalk	Mac OS Server Application or Service
Application or Protocol Anomaly : Other Anomaly	bittorrent	Multi-Platform Client Application
Application or Protocol Anomaly : Protocol Anomaly	blubster/piolet/rockitnet	Multi-Platform Server Application or Service
Distributed Denial of Service : Iterative Application Attack	clns	Networked Hardware Device (router, switch, printer, etc.) Appli...
Distributed Denial of Service : Other	dhcp	Novell Client Application

Search Results (7257)

State	Name	Control	Action Set	Category	Source	AFC	Locked	Exceptio	Severity

3. Conclusion

Beyond the evident role of preventing security incidents, Intrusion Prevention can play a larger role in incident handling. All of the available tools and sources of data should feed into the security narrative for each incident, and Intrusion Prevention is a very different tool from the more widely known Intrusion Detection technologies. In particular, the HP TippingPoint solution discussed herein provides an available set of filters complementary to other technologies, often minimizing the amount of overlap and differentiating in the nature of the detection.

Although preventing incidents remains the ultimate goal, the use of Intrusion Prevention technology also benefits all portions of the incident handling process. At the preparation phase, IPS helps to specify protection details. During the identification, containment, eradication, and recovery phases of the incident handling process, IPS will speed the response, limit the scope, feed the forensic process, and enhance the monitoring; these additions significantly improve the nature of the incident handling process. Finally, during the lessons learned phase, all of the facts of the incident, as revealed both by the IPS and possibly by other story-tellers in the environment, feed back into IPS tuning to further enhance the level of protection that this valuable tool contributes.

Doug Brown, dougb@hp.com

4. References

HP TippingPoint positioned as a leader in the 2012 Gartner magic quadrant for network intrusion prevention. (2012, July). Retrieved from http://www.hpenterprisesecurity.com/register/2012-gartner-magic-quadrant-nip

HP TippingPoint DVLabs Security Intelligence Offerings. (2013, December). Retrieved from http://h20195.www2.hp.com/V2/GetPDF.aspx%2F4AA4-4772ENW.pdf

Inmon Technology (n.d.). Retrieved from http://www.inmon.com/technology/index.php

Michel Eyquem de Montaigne - biography. (n.d.). Retrieved from http://www.egs.edu/library/michel-de-montaigne/biography/

Reputation digital vaccine® service. (n.d.). Retrieved from http://h17007.www1.hp.com/nl/en/solutions/security/reputation-digital-vaccine/

Weir, W. (2007). 50 military leaders who changed the world. (p. 173). Pompton Plains NJ: New Page Books.