Global Information Assurance Certification Paper

Era of Spybots - A Secure Design Solution Using Intrusion Prevention Systems

GCIH Gold Certification

Author: Siva Kumar

Adviser: Richard Wanner

Accepted: September 2007

© SANS Institute 2008, Author retains full rights.

Introduction

This paper is presented in the form of a case study. It utilizes a fictitious company, GIAC Enterprises, a growing small retail company whose clients span the nation. In early spring GIACE was compromised with the Spybot worm which caused a business outage.

To assist with the remediation GIACE contracted a security consulting firm to investigate and propose a robust, secure solution to mitigate these worms as well as protect the business from similar future attacks.

The security consulting team conducted a detailed incident handling process. The following sections flows through all the phases indicated in the PICERL methodology. The goal of the security consulting team is to provide a secure design solution for GIACE current and future needs meeting the corporate requirements.

Environment

The GIACE network infrastucture shown in figure-1 consists of dual-homed data centers. Each data center has distribution layer routers facing the Internet traffic, trading partners via a DMZ environment, core layer switches protecting sensitive business applications and a WAN layer to support all point to point connections and retail connectivity. GIACE uses a combination of Checkpoint firewalls at the DMZ and the Cisco 6509 chassis at the core layer. Most of the machines are workstations segmented based on their geographic location.

A full mesh topology was implemented to provide “High Availability” functionality. The current infrastructure is also a scalable architecture for future growth.

All workstation traffic is unrestricted between their retail connections and the Internet. The GIACE workstations are Windows based systems running Symantec AV security client. GIACE uses Radia to push updates to the workstation since the system owners do not have administrative rights. Radia is a centralized software downloader that installs workstations with new software applications, operating systems installations (service packs), patches etc. This also helps to standardize workstations across diverse user community. GIACE had a Symantec AV client user license agreement as part of their maintenance contract on all workstations. This gives GIACE some form of security assurance.

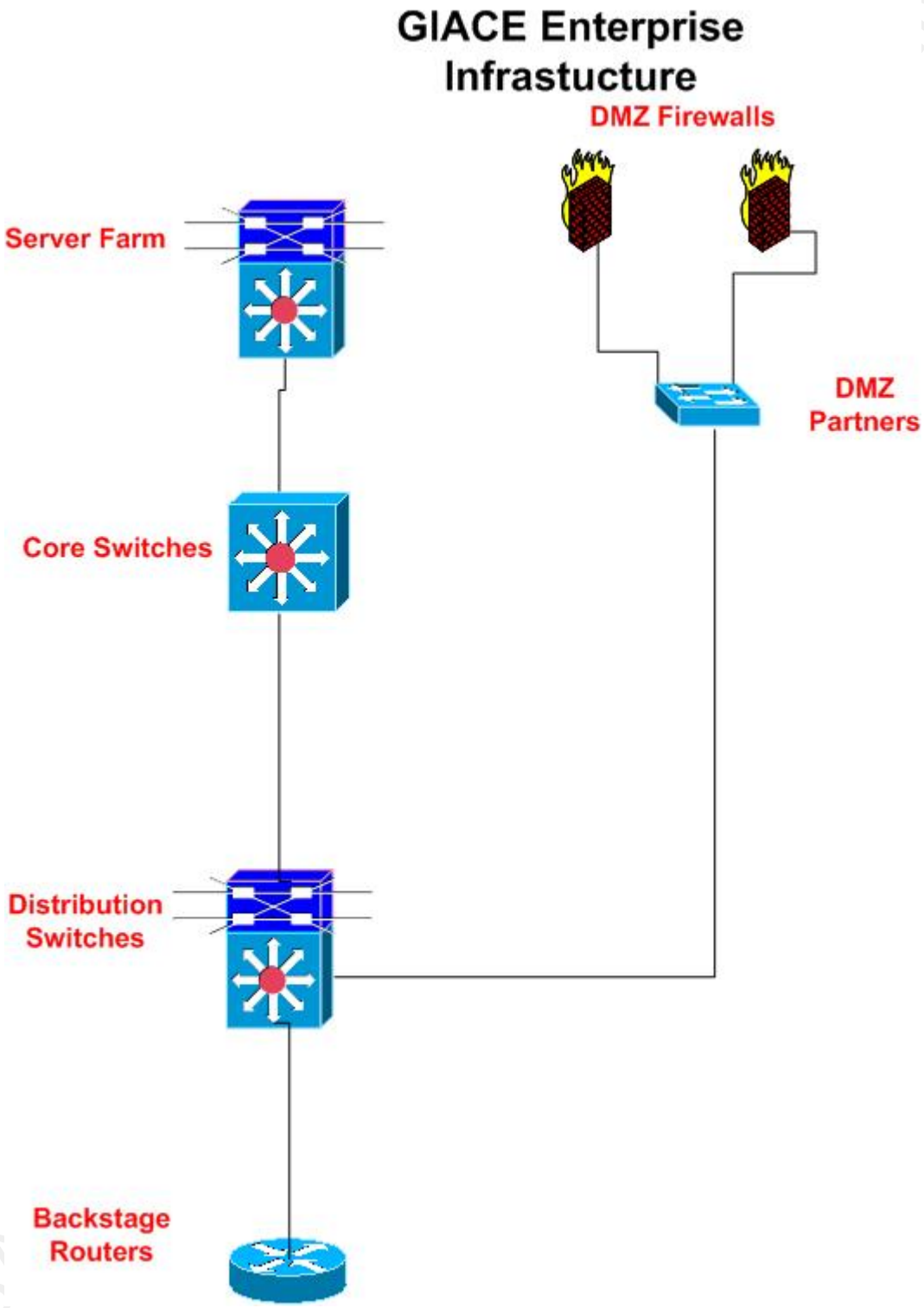


Figure 1: GIACE Infrastructure

Attack Process

In early spring the GIACE Help Desk Service Management application tracked a stream of workstation performance issues. The IT operations team discovered that it was not an isolated system since new tickets with same issues were reported in other geographic locations.

The operations team also noted steady outbound traffic originating from the problem workstations on their DMZ firewalls on TCP ports 8555 and 2967 to specific destinations 204.138.154.20 and 54.163.146.74 at the network boundary. Backup firewall logs from previous months didn’t show any normal activity on these ports or destinations. It was ascertained that these workstations were in fact the point of focus. They noticed other new systems reporting the same behavior. It was quite evident that there was a worm attack in progress and it was unknown about the spread across other systems.

Incident Handling Process

GIACE contracted an outside security consulting firm to investigate the current attacks and counter measures for future attacks including their security infrastructure assessment. The security consulting firm consisted of forensic experts, architects and incident handlers. They followed the SANS - PICERL methodology in their incident handling process.

Preparation Phase:

The consulting security firm formulated the team based on the six basic communication interrogatives (Zachman, 2007).

What (Data) – administrative privileges
How (Function) - GIACE process flow – on call rotation
Where (Network) – list of devices (firewalls, workstations)
Who (People) – GIACE organization structure
When (Time) – time events
Why (Motivation) – GIACE business Goals/Strategy

The security team found several key issues. GIACE does not have a formal incident handling team. They do have a problem escalation process via their NOC (network operations center) – Operations – Engineering. The security team activated the required team from the list of on-call rotation people. GIACE also provided the necessary access to the critical peripheral devices and access to the logs. The goal of the preparation phase is to get the team ready to handle incidents.

Identification Phase:

The goal of the identification phase is to gather events, analyze them and determine whether there is an incident. The security team analyzed the firewall logs provided by GIACE, setup sniffer traces between the affected hosts. They deployed snort sensors to capture additional data. Their analytical process is again based on the following six criteria: (Zachman, 2007)

What (Data) – tcp dumps, snort deployment
How (Function) - snort filter tools
Where (Network) – perimeter firewalls, workstations
Who (People) – on call person reports
When (Time) – attack in progress
Why (Motivation) – GIACE infrastructure analysis

The coorelation yielded on the firewalls/workstation:

1. Defined range of ip-address on tcp port 2967 on DMZ firewall logs.
2. A new NL.exe file creation on affected workstations
3. Unknown domain connection to ftpd.3322.org
4. Unusual higher bandwidth utilization causing network performance issues.
5. Lowered security level on the Symantec Antivirus tool.

The above events, in particular the lowered security level on the offended workstation when compared to a normal

functioning workstation, suggested the possibility of a vulnerability related to the Symantec Antivirus tool.

The Security team further consulted the Symantec "Security Response System" and identified that this port (tcp 2967) is being employed by a variant of Spybot (Detected by Symantec AV as W32.Sagevo.Worm) (Doherty, 2007).

Identification occurred at all three levels namely DMZ firewalls (network perimeter detection), IP address source range on work stations (host perimeter detection) and antivirus tools, shared access services (system level detection).

The security team declared that an incident has been identified.

Containment Phase:

The goal of the containment phase is to stop the bleeding, prevent the attacker from getting any deeper into the impacted systems, or spreading to other systems. The security team consulted with the GIACE legal team regarding the forensic analysis needed for the compromised workstations.

As a short term containment strategy it is decided to quarantine the affected workstations by moving them offline from network. The users were notified via e-mail that the affected systems will undergo routine maintenance. The workstations were disconnected from their network connection activity. System hard drives were duplicated for evidence. They acquired review logs

of other periphery firewall devices to access the extent of the risk.

As a long term containment strategy the security consulting team proposed the following actions:

1. Patch the systems. At the time of this incident a patch was available to the public at the Symantec. Since GIACE does not have a formal incident response process a process break down and an oversight caused the spread of the worm.

2. Filter TCP port 2967 inbound/outbound at the network perimeter firewalls to ensure no unauthorized access.

Example:

```
deny tcp any any eq 2967 log
```

The logging provides additional details when the ACL is processed

3. Filter outgoing connections to 204.138.154.20 and 54.163.146.74 at the network devices.

Example:

```
deny ip any host 204.138.154.20
deny ip any host 54.163.146.74
```

The purpose of long term containment is to keep the production up while building a clean system during eradication.

Eradication Phase:

The eradication phase is to get rid of the infected worm, perform a vulnerability analysis and improve defense (protection techniques, hardening systems etc).

The security team consulted with Symantec's "Deep Site" Threat management System to perform a malware analysis and shared their findings with GIACE. A detailed malware analysis is beyond the scope of this paper.

Spybot Vulnerability Analysis

The W32.Sagevo worm spreads by exploiting the Symantec Antivirus Remote Stack Buffer Overflow Vulnerability (BID 18107) over TCP port 2967. (Security Focus, 2007)

In the paper titled "Symantec Client Security Exploitation and Activity Alert", Aaron I. Adams et al wrote:

"The symantec client security stack-based overflow vulnerability associated with Spybot worm identified earlier occurs when handling data transmitted over TCP port 2967. The precise issue occurs because of the erroneous use of the strncat() function. Specifically, the length of data copied during the strncat() is dictated by the result of a subtraction operation involving a static value minus the length of a user-supplied string. If the length of the string is greater than the static value, the integer will wrap, causing an unbounded

strncat() to occur and memory to become corrupted as a result. The destination buffer is 0x180 bytes in size.

The vulnerability is triggered using what is known as Type 10 messages, specifically when issuing the COM_FORWARD_LOG (0x24) command. By supplying a backslash character within the exploit packet, an attacker can trigger the aforementioned strncat() code to be invoked.

Upon triggering the bug, the attacker would be able to trivially exploit the issue by either overwriting the command handler's return address or a Structured Exception Handler Record, which would facilitate arbitrary code execution.

It appears that the exploit that is being used to leverage this issue by Spybot variants and Sagevo is derived from the same exploit base. The only differences are the exploit's payload, a bindshell for spybot and connect-back for Sagevo." (Adams, 2006)

Symantec's website provides the following technical details regarding this spybot:

" W32.Sagevo, when executed performs the following actions:

1. Copies itself as the following file:

%System%\wins\svchost.exe

2. Attempts to spread using the symantec client security and symantec antivirus elevation of privilege (as described in symantec advisory SYM06-010).

3. Creates 512 threads and then attempts to connect to a range of IP addresses on TCP port 2967.

4. Obtains the IP address of the compromised computer, generates an IP address, and attempts to infect the computer that has that address. The IP address is generated according to the following algorithms:

a. If the IP address is 192.168.C.D, it starts with 192.168.0.1.

b. If the IP address is 10.B.C.D, it starts with 10.0.0.1.

c. If the IP address is not one of the above and the third digit is greater than 11, it must be A.B.C.0. If the third digit is less than 11, the address must be A.B.0.0.

Example:

GIACE Infected workstation IP: 13.10.50.40

Scan pattern: 13.10.40.40, 13.10.40.41, 13.10.40.42, ..., 13.10.41.1

5. Increment the 0 part of the IP address by 1, attempting to find and exploit other computers based on the new IP address, until it reaches 254. If the IP reaches 240.254.254.254, the worm restarts the infection sequence with 10.0.0.0 again.

6. Drops the following .bat file and deletes itself:

%Temp%\NL[RANDOM].bat

7. Downloads a .bat file from the server and executes it.

Eradication process recommended by Symantec:

1. Disable System Restore (Windows Me/XP).
2. Update the virus definitions.
3. Run a full system scan.
4. Delete any values added to the registry.” (Doherty 2007)

The security team applied the appropriate patches on infected workstations. The patches were downloaded from the Symantec website: (proper license required)(Symantec support site, 2007)

Recovery Phase:

The goal of the recovery phase is to put back the impacted systems back into production in a safe manner and validate the host systems that the worm has been eradicated.

The security consultants deployed the quarantined workstations that has been patched back into the production network and ran test suites for an overall validation. The test suite consisted of:

1. Business unit tests
2. Functional test plans
3. Network traffic stress tests
4. OS and application logs validation

The security team also demonstrated that the patched workstation may not be re-infected again by this worm. They created a custom signature to trigger on the original attack vector utilizing the snort tool and proved that the system was indeed hardened. The GIACE e-mail system announced the system availability to the user community.

As part of the lessons learned phase GIACE security consulting evaluated the current network infrastructure and proposed/demonstrated an IPS based solution.

Lessons Learned Phase:

The goal of the lessons learned phase is to document what happened and improve the infrastructure capabilities for GIACE. This phase will also focus on the GIACE processes, technology road map and improved incident handling capabilities.

The security consulting team prepared a formal Incident Response Report to the Senior Management after proper consensus.

The Report focused on

1. Brief summary of the w32.sagevo virus exploitation.
2. Activities of the security consulting team.

3. Executive summary and recommendations.

As an extension to their executive summary and recommendations the security consulting team proposed:

1. An IPS based secure solution for GIACE.
2. Infrastructure security for GIACE.
3. A formal incident handling team/process.

An IPS solution was proposed for the following reasons:

GIACE checkpoint DMZ firewalls were not capable of inspecting traffic beyond layer 3. There is always a possibility of worm attack using well known ports for backdoor entry. The stateful inspection firewall does not have the intelligence to look into the data payload.

GIACE workstation installed Symantec anti-virus software is isolated only to the workstations. They are signature driven and cannot protect from zero-day attacks or other denial of service type attacks. GIACE is reliant on the RADIA application push for new patches for individual workstations. An easy oversight may cause a delay in updating the patch and can cause a virus outbreak which was the case with GIACE in this incident. There is also a separate administrative component involved.

An IDS may not be a viable solution. GIACE must spend the time and resource to examine the reports generated, and remediate virus/worm as necessary. There is also a time lag to

re-deploy the system and may include a network downtime for sensitive financial applications.

A high-performance Intrusion Prevention System can function as a virtual software patch, where host patches are not feasible or not applied. It protects vulnerable computers from a compromise. An IPS proactively inspects all traffic through Layer 7 and blocks malicious traffic. An IPS is complimentary to the existing network security systems. (Telechoice, 2006)

Tipping Point IPS Secure Design

Figure-2 depicts the new infrastructure design proposed for GIACE. The placement of the IPS design is a 2 tiered approach. The tier-1 device placed outside the firewall is mainly focused on the Internet traffic inbound and outbound.

The tier-2 IPS devices are deployed at the datacenter focused on both inbound and outbound traffic and for quarantine purposes. They are also setup in (HA) high availability mode to decrease the likelihood of interrupted GIACE traffic. With this design the IPS devices are centrally located to encompass all the geographic sites of GIACE. It also cuts the operating costs in deploying at all divisions within GIACE individually.

The reasoning for a tier-1 IPS device outside the firewall is to monitor the traffic which is dropped by the firewalls provided they are tuned. This will assist in monitoring the Internet traffic that targets GIACE proactively.

Tier-2 IPS devices assist in coorelating the tier-1 IPS as well as monitoring worm traffic that passed through the firewall using known ports.

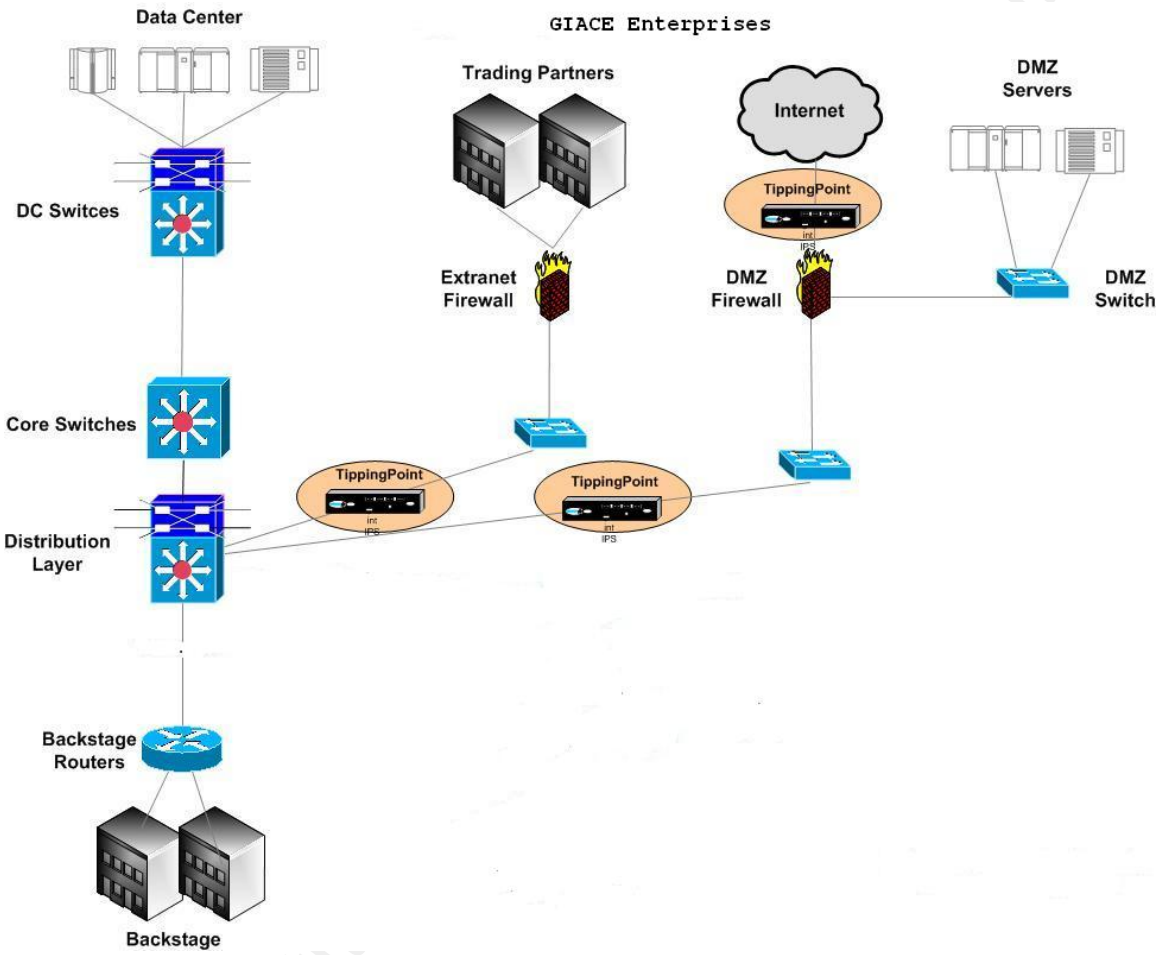
The inline design blends easily with the existing infrastucture. Being a layer-2 (bump in the wire) device the IPS devices are easier to manage and there are no routing protocols (MPLS, OSPF) configuration changes to the existing architecture are needed.

A single vendor for all IPS devices is recommended because of centralized management, reduced interoperability issues and lower maintenance/support costs.

Figure-3 depicts a single IPS device which is cross connected with the WAN layer routers via HSRP (Hot Standby Routing Protocol). The fall back mode assures un-interrupted production traffic and also uses the ZPHA (Zero Power High Availability). The architecture also allows for traffic classification based on DSCP (Differentiated Services Code Point) and complex rate shaping QOS (Quality of Service) policies. The IPS devices operate at wire speed (gigabit) blocking malicious attacks with low latency.

The proposed network infrastructure protects GIACE from Spybot style worm attacks. A quarantine action is also put in place in case of a similar incident in the future (Appendix).

Figure 2: GIACE Network Design



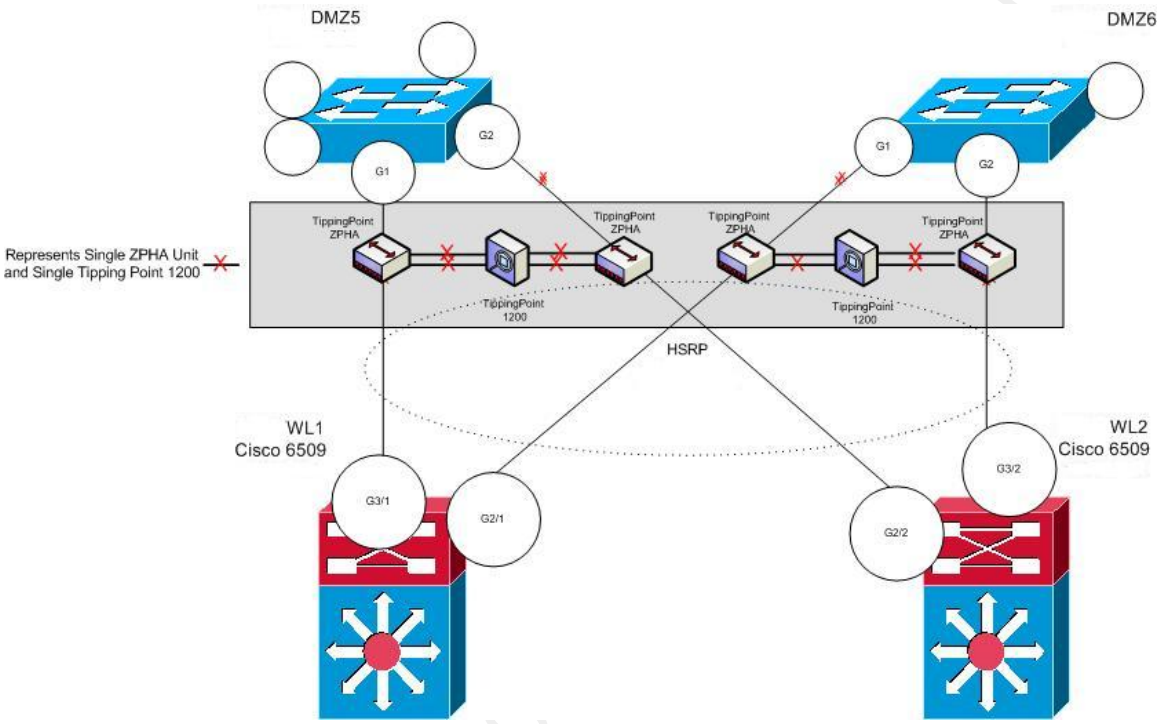


Figure 3: GIACE Network Design - Detailed

GIACE Infrastructure Secure Design

The security team evaluated the existing infrastructure, identified areas of network security vulnerabilites and recommended some best security practices for GIACE network in addition to the IPS solution.

Physical layer:

GIACE workstations were not following any security policies. Workstations were accessible by bystanders. The patch panel/switch ports where the network connections are attached were also accessible in open.

The security team recommended using workstation locks for individual owners as well as separate secure room/enclosure to access the patch panel.

Datalink layer:

GIACE workstation network connections were not properly hardcoded to switch ports. Workstation owners were allowed to plug in to any open ports on the switch. This provided wider security vulnerability for GIACE. GIACE often have third party vendors at their premise using their own laptops. Any compromised laptop would easily infiltrate GIACE network if they are connected to the available live switch ports.

The security team recommended MAC based security on the switch ports. 802.1x is an IEEE standard for media access at

layer 2. GIACE current technology vendor supports 802.1x port based security and should be leveraged for layer 2 network control. A NAC (Network Access Control) based solution further quarantines workstations that are not patched and lowers the risk of network threats like worms and viruses.

Network Layer:

GIACE has vlan segmentation at the corporate level. Workstations in zone 1 also share the same vlan as zone 2 workstations. This causes any virus outbreak to propagate within the vlan. There was also no emergency acl to protect in case of an outbreak. There was no authentication for control routing protocols.

The security team recommended segmenting further the GIACE internal network by creating layer 2 segments in layer 3 switches. Micro segmentation is a cost effective method to harden the network against worms. Preparing emergency and roll back acl policies assist in containing worm outbreaks. Cisco IOS ACLs and VLAN ACLs provide additional traffic filtering. For routing between the aggregation switches and routers MD5 authentication is recommended.

Example:

```
router ospf 5
 router-id 172.25.0.24
 log-adjacency-changes
 area 140 authentication message-digest
 passive-interface default
```

```
 no passive-interface Vlan81
 no passive-interface Vlan94
 no passive-interface GigabitEthernet7/16
 network 172.25.0.24 0.0.0.0 area 150

interface Vlan75
 description ****GIACE financial****
 ip address 172.25.95.1 255.255.255.0
 ip helper-address 172.25.148.18
 no ip redirects
 ip ospf message-digest-key 1 md5 7 04521901583B54
```

GIACE infrastucture routers should utilize Loopback interfaces for purpose of routing and security. The Loopback should be sourced for NTP, AAA, logging etc.

```
Example:
interface Loopback0
ip address 172.25.0.24 255.255.255.255
no ip redirects
no ip unreachables
no ip proxy-arp
```

Transport Layer:

GIACE utilized firewalls only at the DMZ layer. Any syn flood attacks originating from inside can easily compromise the network. GIACE also were using the NTP (Network Time Protocol) for logging but in-band.

The security team recommends a server layer firewall approach utilizing the Cisco FWSM inline modules which can easily integrate into existing 6500 chassis. The firewall service modules provide enhanced reliability and integrates firewall security inside the GIACE network infrastucture. Network Time Protocol is essential for time-stamp accuracy for logging, because logs are polled under different devices geographically. It is recommended that NTP traffic is carried out of band management.

Session Layer:

GIACE client-server connectivity still utilizes telnet method of access. The security team recommends migrating from telnet to SSH2 protocol for all admin access to GIACE servers.

Presentation Layer:

GIACE uses custom applications and most of them were outsourced. There is no data encryption for the internal traffic. The security team recommends data encryption as well data compression if feasible. This enhances in prevention of data snooping or masquerading.

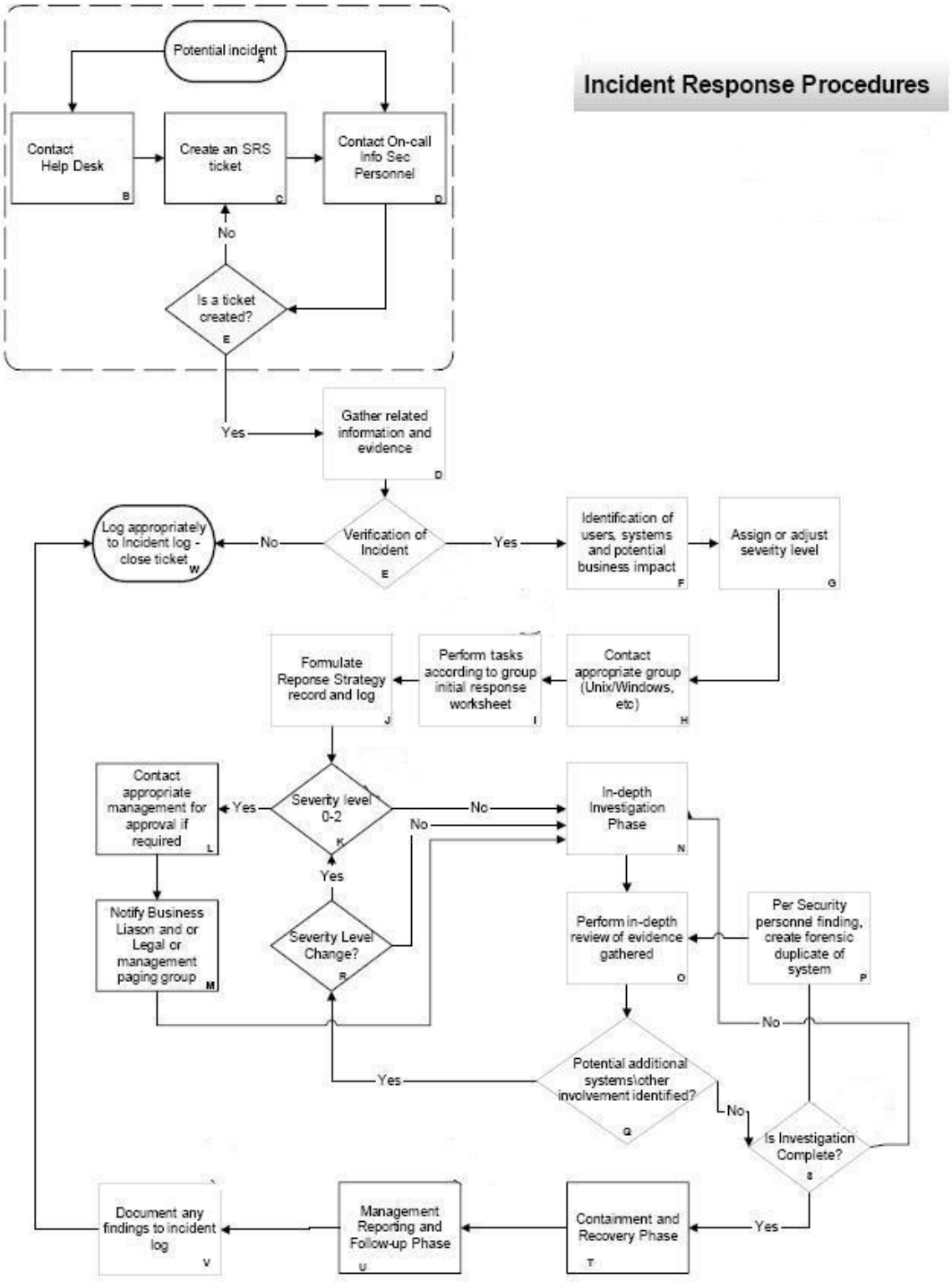
Application Layer:

GIACE did not have a dedicated appliance like IPS to mitigate worms/viruses. The current SNMP polling is in-band using known community strings. The security team recommended an

in-line IPS solution with low latency. The SNMP traffic should be out-of band or on a dedicated vlan with private community strings.

GIACE incident handling process

GIACE is inadequately prepared for incidents of this type. As preparation for future incidents, establishing a dedicated computer security incident response team (CSIRT) is recommended. This team will provide rapid response and reduce future events and also establish performance standards. The suggested members could be the on-call person from a multi-disciplinary team including operations, network management, legal counsel, human resources, disaster recovery / business continuity planning. The security team proposed the following flow chart template for incident response process.



Conclusion

This document has attempted to show how any organization can be vulnerable to a worm attack when there is a break in the process flow. It also demonstrates the SANS-PICERL methodology as the Incident Handling Process.

The next section focuses on the Infrastucture secure design using an Intrusion Prevention System. GIACE infrastructure is re-designed to deploy an IPS integrated secure solution. A series of screen shots (Appendix) shows a TippingPoint configuration template for spybot style virus that can block and quarantine in the future.

The next section focuses on general infrastructure design focusing on the network security. The solution proposed overlays using the existing vendor technology.

An IPS is recommended for a long term strategic solution for GIACE. The blended threat suppression approach provides a proactive solution for future needs.

This sort of architecture using in-line IPS can be used to reduce the complexity, deployment costs, and maintenance costs of deploying individual network elements.

References

The SANS Institute. *Security Policy Project*. Retrieved August 15, 2007, from sans.org. Web Site: http://www.sans.org/resources/policies

Northcutt, Stephen (2002). *Network Intrusion Detection.* SAMS

Skoudis, Ed (2006). *SANS Security 504: Hacker Techniques, Exploits and Incident Handling*. SANS course

Adams, Aaron et al(2006). Symantec Client Security Exploitation and Activity Alert. Retrieved August 15, 2007, from symantec.com. Web site: https://tms.symantec.com/

Doherty, Stephen (2007). W32.Sagevo – Symantec. Retrieved August 15, 2007, from symantec.com. Web site: http://www.symantec.com/security_response/writeup.jsp?docid=2006-121309-3331-99&tabid=1

Cisco connection Online Retrieved August 15, 2007, from cisco.com. Web site: http://www.cisco.com/en/US/netsol/ns731/networking_solutions_solution.html

Case for an IPS (2006). Retrieved August 15, 2007, from telechoice.com. Web site: http://www.telechoice.com/presentations/caseforips.pdf

Symantec support site (2007). The SYM06-010 patch for Symantec Client Security and Symantec AntiVirus. Retrieved August 15, 2007, from symantec.com. Web site: http://entsupport.symantec.com/docs/n2006052609181248

Denial of Service and Distributed Denial of Service Protection. Retrieved August 15, 2007, from tippingpoint.com. Web Site: http://www.tippingpoint.com/resources_whitepapers.html

Zachman Architecture (2007), Retrieved August 15, 2007, from wikipedia.org. Web site: http://en.wikipedia.org/wiki/Zachman_framework

Security Focus, Symantec antivirus Remote stack buffer overflow vulnerability. Retrieved August 15, 2007, from securityfocus.com. Web site: http://www.securityfocus.com/bid/18107

Irwin, Victoria (2004) RSA Conference paper, Retrieved August 15, 2007, from rsaconference.com. Web site: http://www.rsaconference.com/uploadedFiles/VirtualSoftwarePatch.pdf

Bejtlich, Richard (2005). *Extrusion Detection: Security Monitoring for Internal Intrusions.* Addison-Wesley Professional.

Appendix

This section includes TippingPoint device configuration pertaining to the prevention of spybot style worm attacks. It includes setting up profiles/filters, host level, SMS IPS level and monitoring functionalities. The configuration can be applied either directly on the device or pushed via SMS (Security Management System). This SMS system consists of a Java based SMS client and SMS Server.

The ease of use with configuration assists the administrators a free choice of defining interfaces as trusted or untrusted. Also they have an option to scale their filter settings across segments or traffic patterns. (Irwin, 2004)

TippingPoint IPS is focused on blocking exploitation of the threats underlying these bots rather than the individual bots themselves. The TippingPoint approach provides a much higher level of protection. The first one, w32.sagevo, exploits the SYM06-010 vulnerability, which the IPS can detect and block with custom filter 4463: SYMANTEC: AntiVirus Client Buffer Overflow.

The simple approach would be to enable this filter in Block and Notify, or configure a quarantine action to notify users that they are infected. The second approach is a blended threat, and can exploit a number of vulnerabilities.

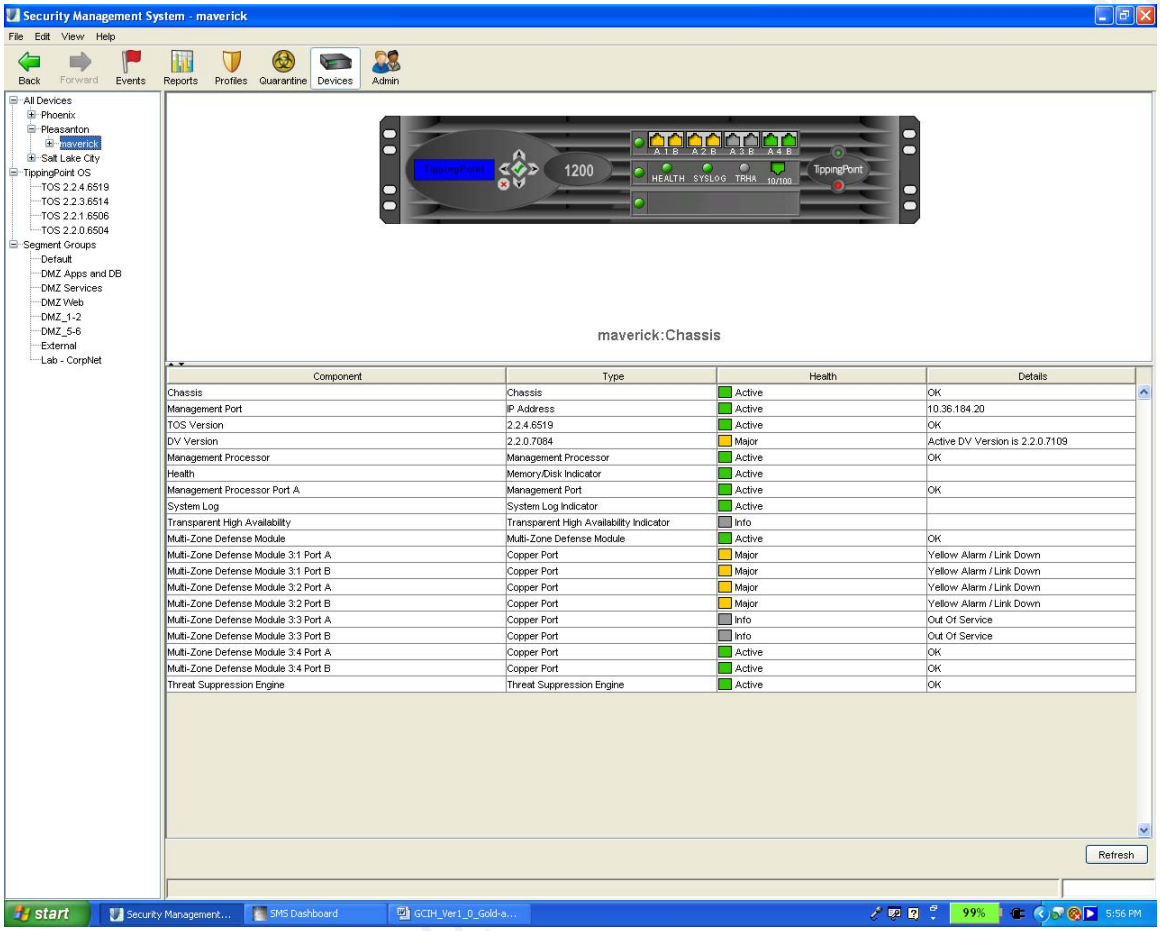


Figure 4: IPS – Device Details

Using the SMS client the user can select the IPS device that needs to be configured. The above screen shows the details of the IPS device – includes the digital vaccine release, TOS version and an overall health check.

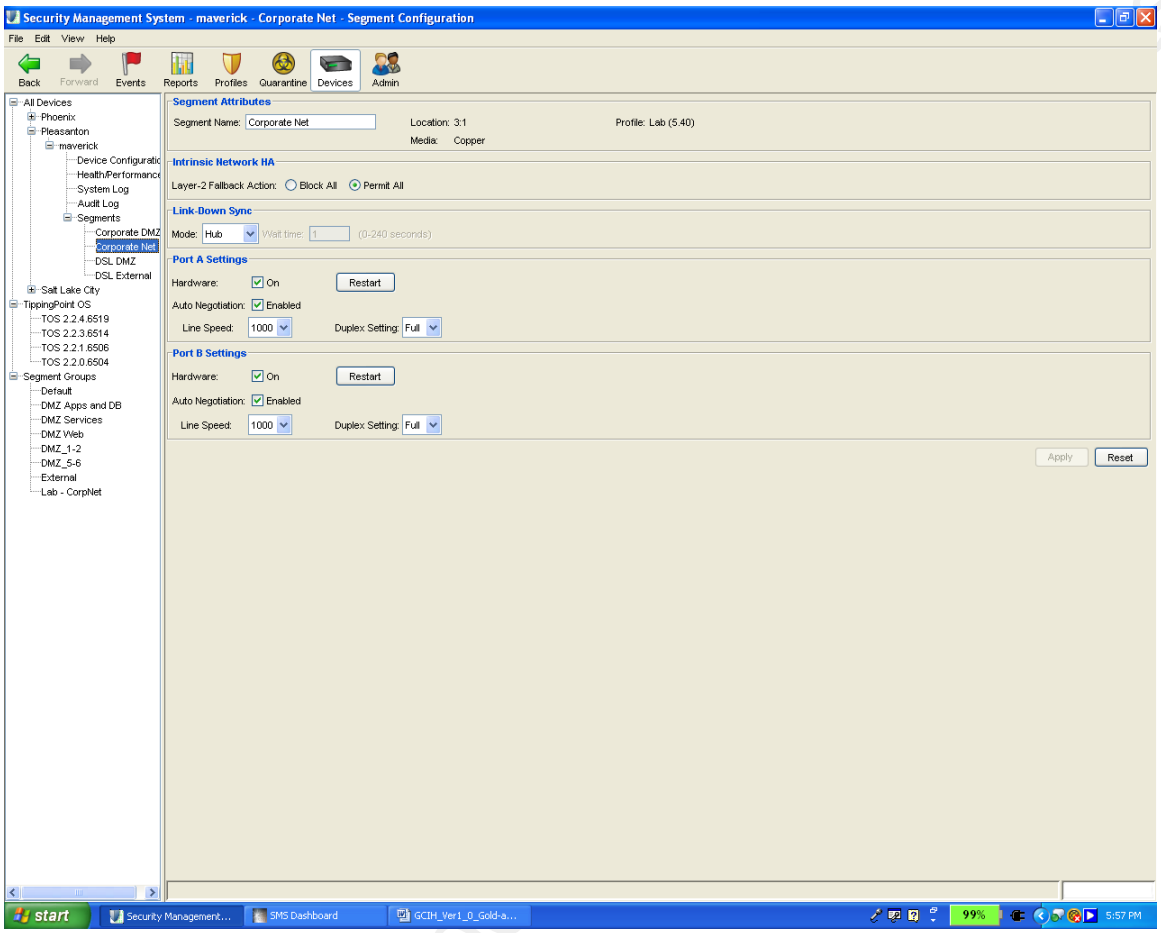


Figure 5: IPS – Device configuration

This screen shows how the network traffic can be segmented for GIACE. It shows all interfaces can be logically selected as internal or external.

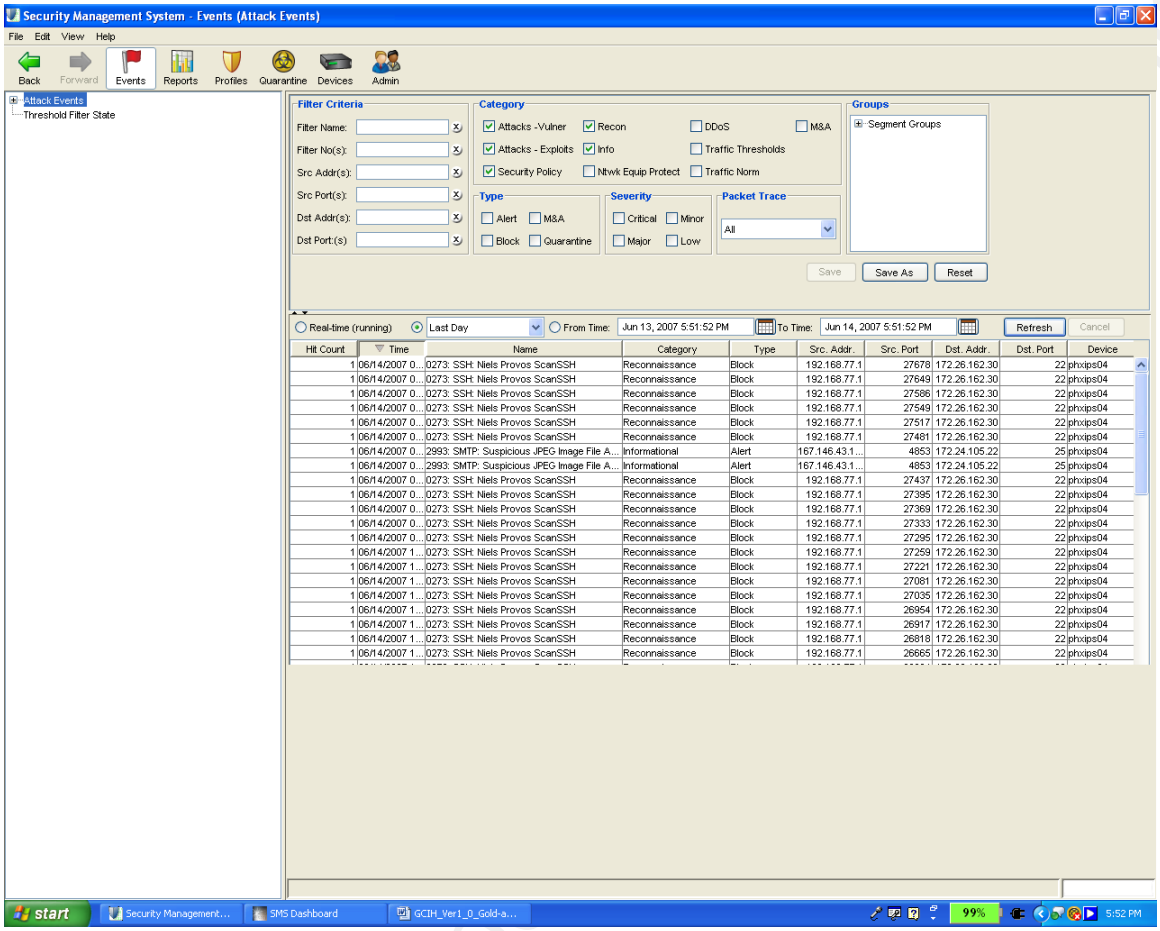


Figure 6: SMS – Attack Events

The main interface window is shown above. By selecting the events tab, a current snap shot of all activities for the pre-defined time period is displayed. The events screen provides number of options for monitoring attack detection and response. Also categorizes attack levels. The name category shows the predefined filter and shows the current types (eg block, enable mode). It also provides the source/destination ports as attack vector.

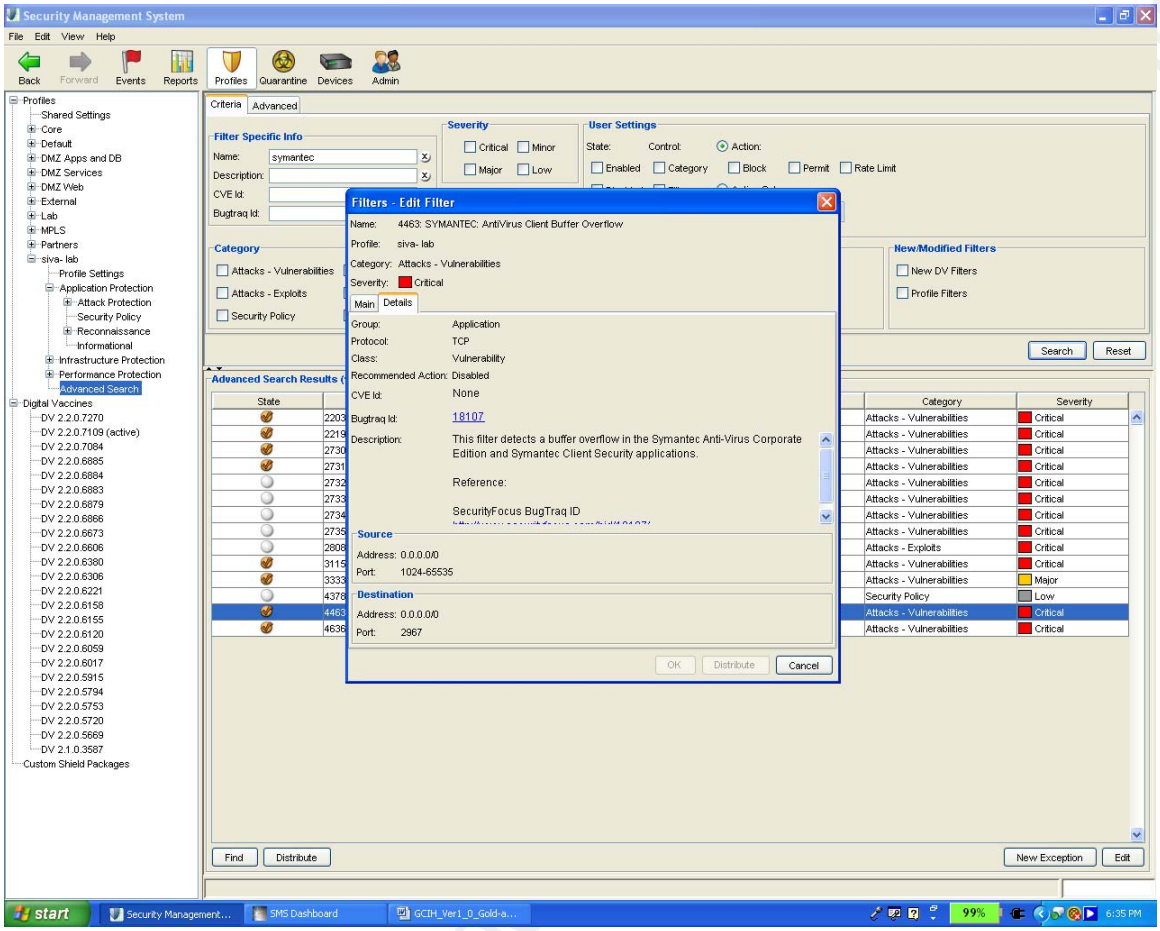


Figure 7: Application Filter Search

In the profiles tab an advanced search is performed. “Symantec” is used as the filter specific info. This yields a set of predefined available filters. By double clicking the “4463 – antivirus client buffer flow” filter more details are available regarding the vulnerability.

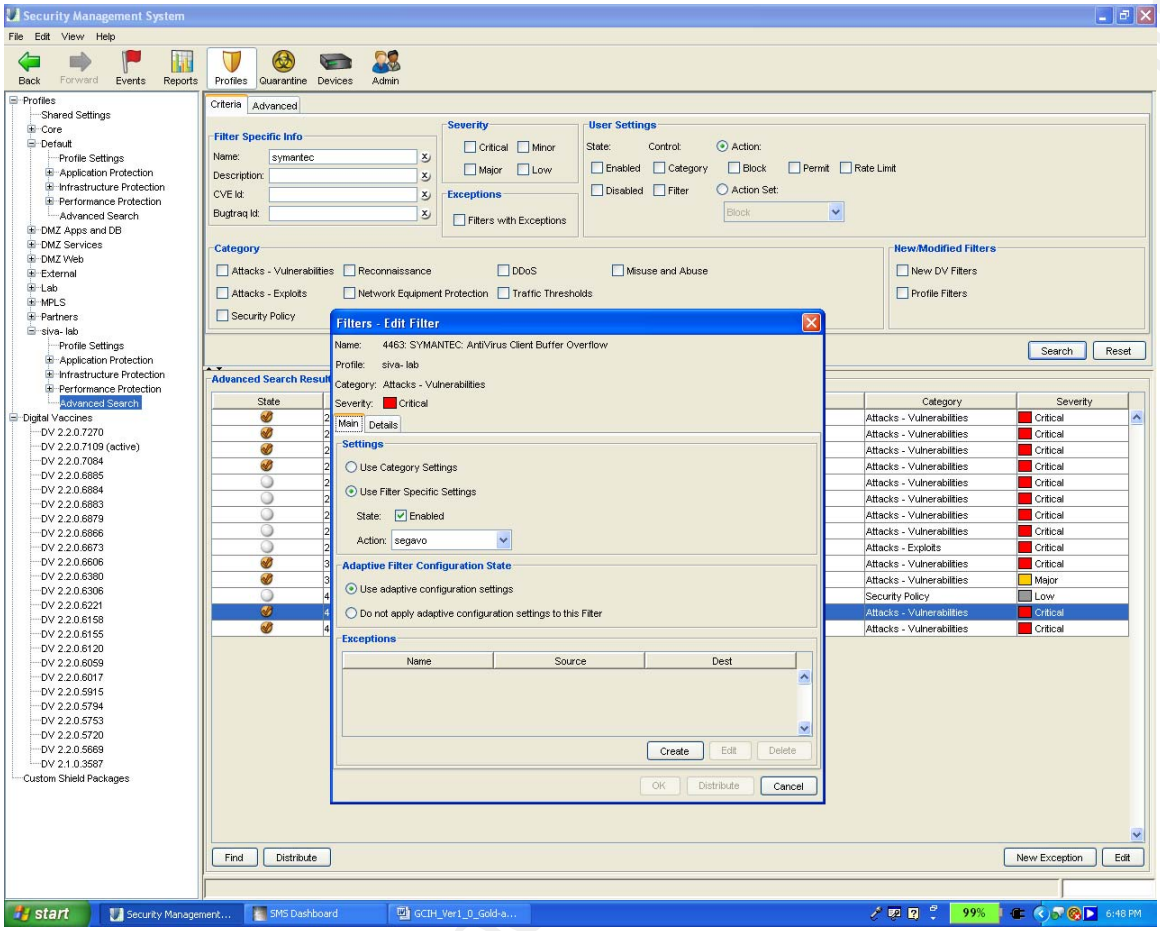


Figure 8: Sagevo - Apply Filter Settings

In the above screen shot shows a new filter named “sagevo” being edited. This is the first step in the process of creating a filter.

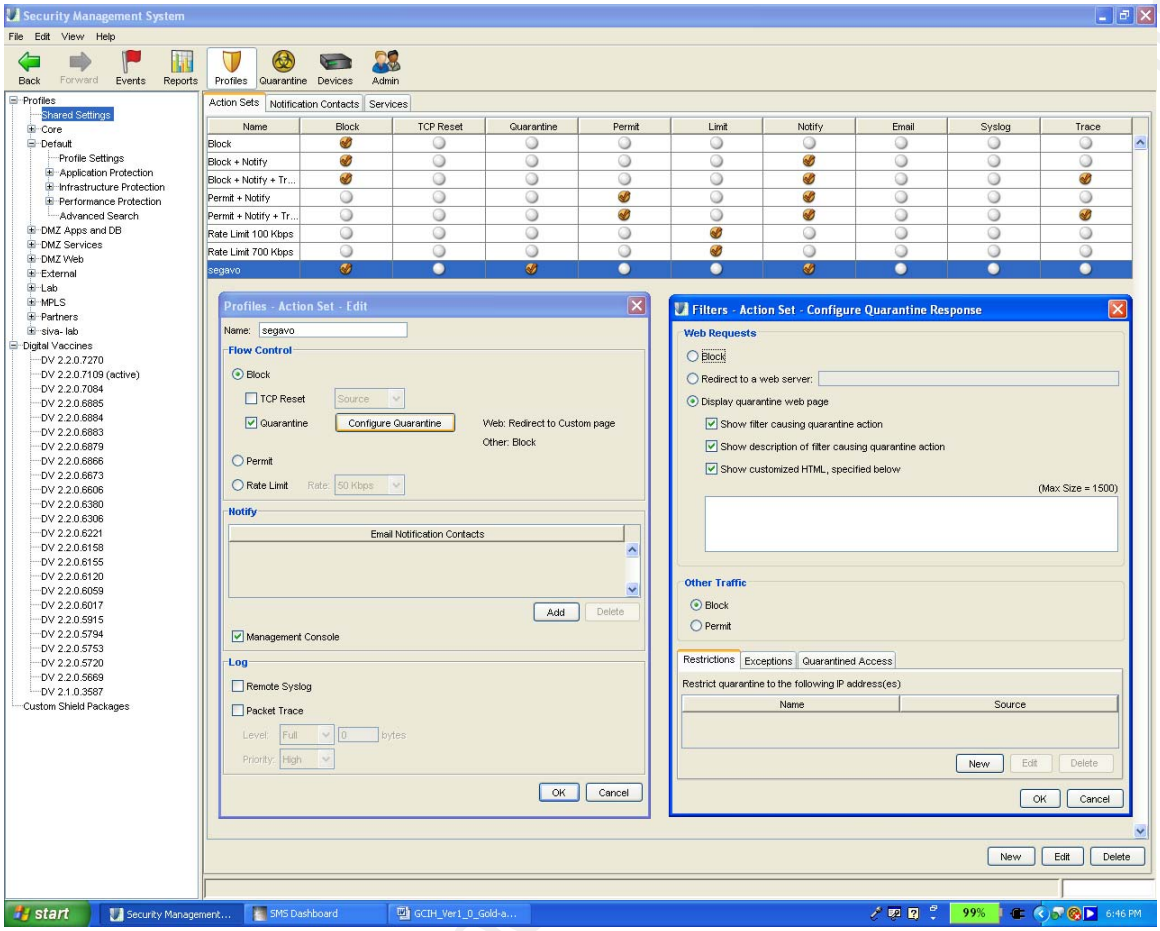


Figure 9: Sagevo Filter – Action Set

A new filter profile “sagevo” is configured in the previous action set. Block and Quarantine action is selected. It also provides options to quarantine –eg a web page or a simple block options.

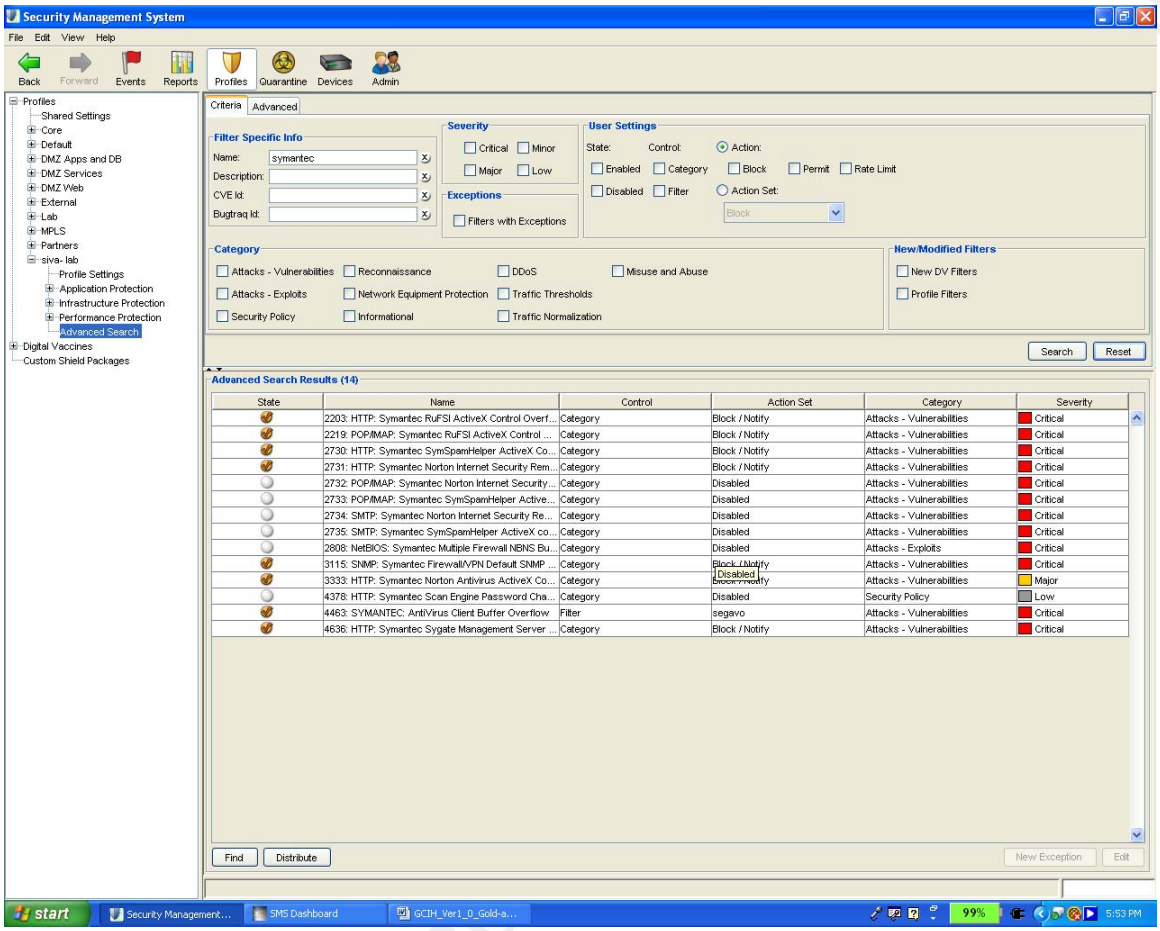


Figure 10: Filter Search for malicious virus

The profiles tab (advanced search window pane) shows the list of active predefined profiles and their state (Action set). The filter specific criteria for “symantec” show a list of defined filters, and current control measures taken. The user defined ruleset “Segavo” is listed and applied as enabled state.

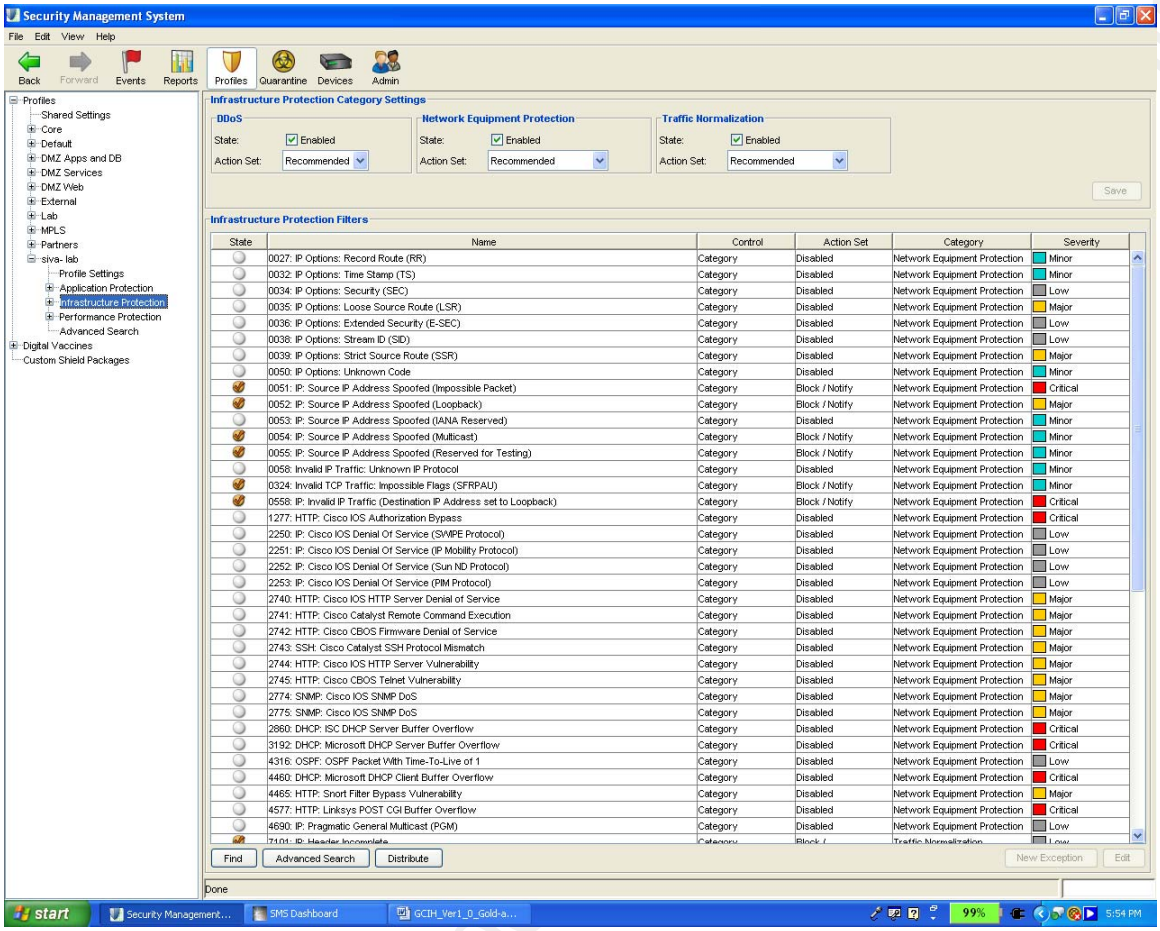


Figure 11: Infrastructure protection settings

The Profiles tab and the infrastructure window pane shows all the recommended filters with their corresponding severity level. Users have the option to activate or deactivate the filters by checking the radio button. The security team enabled most common filter settings.

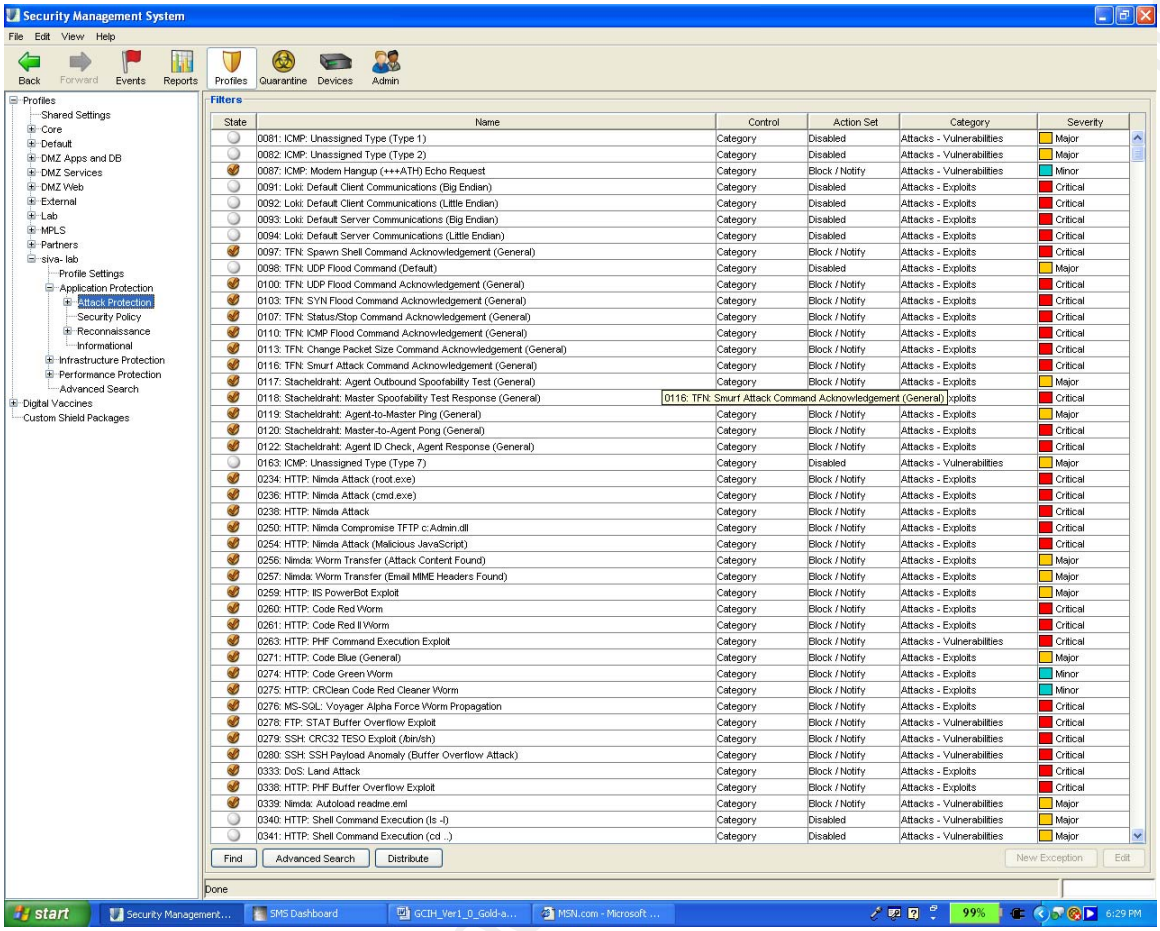


Figure 12: Application Profile

The application filter profile shows a set of pre-defined filter categories that defend against known and unknown exploits. It shows a list of recommended filters for GIACE that are currently in enabled state.

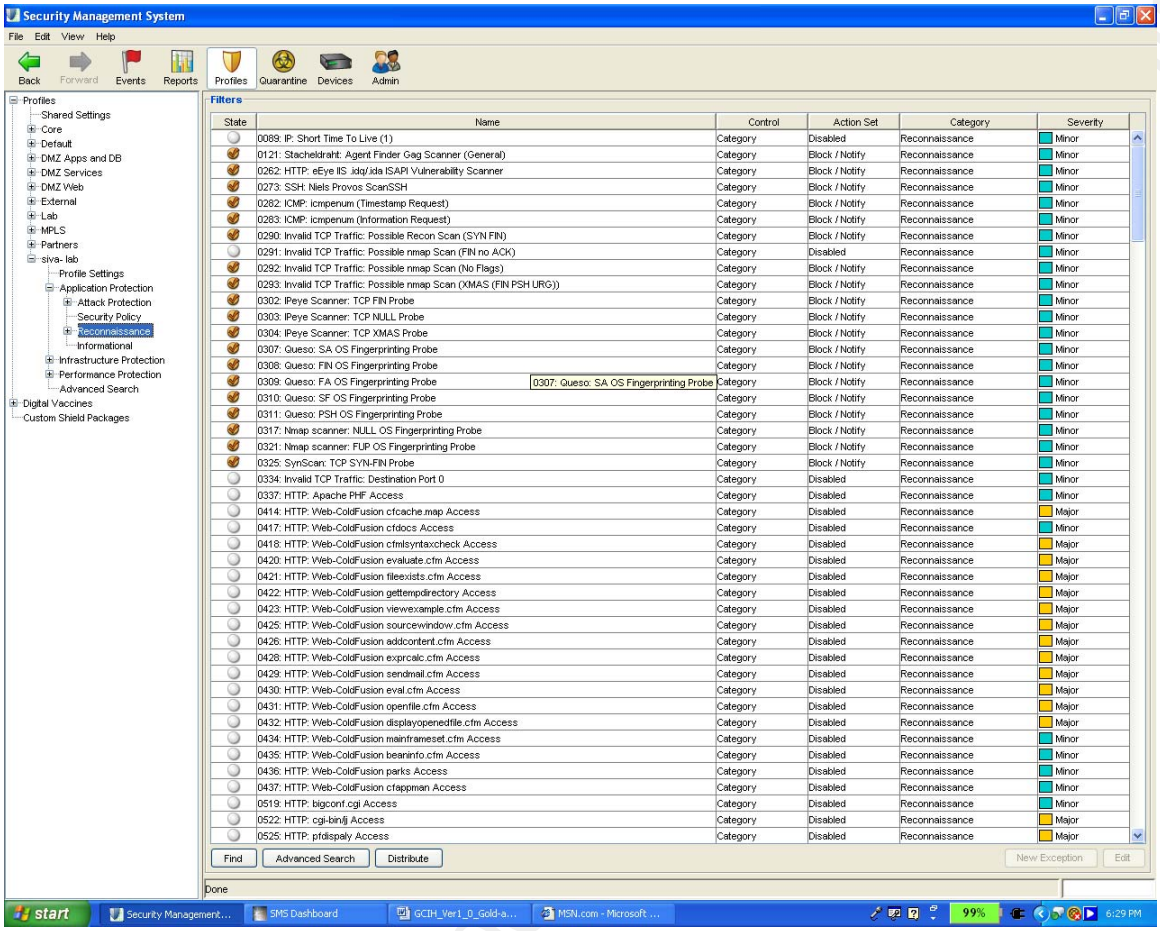


Figure 13: Reconnaissance Profile

The reconnaissance filters include probes and scan sweeps. The above screen shot shows the recommended reconnaissance filter settings for GIACE.