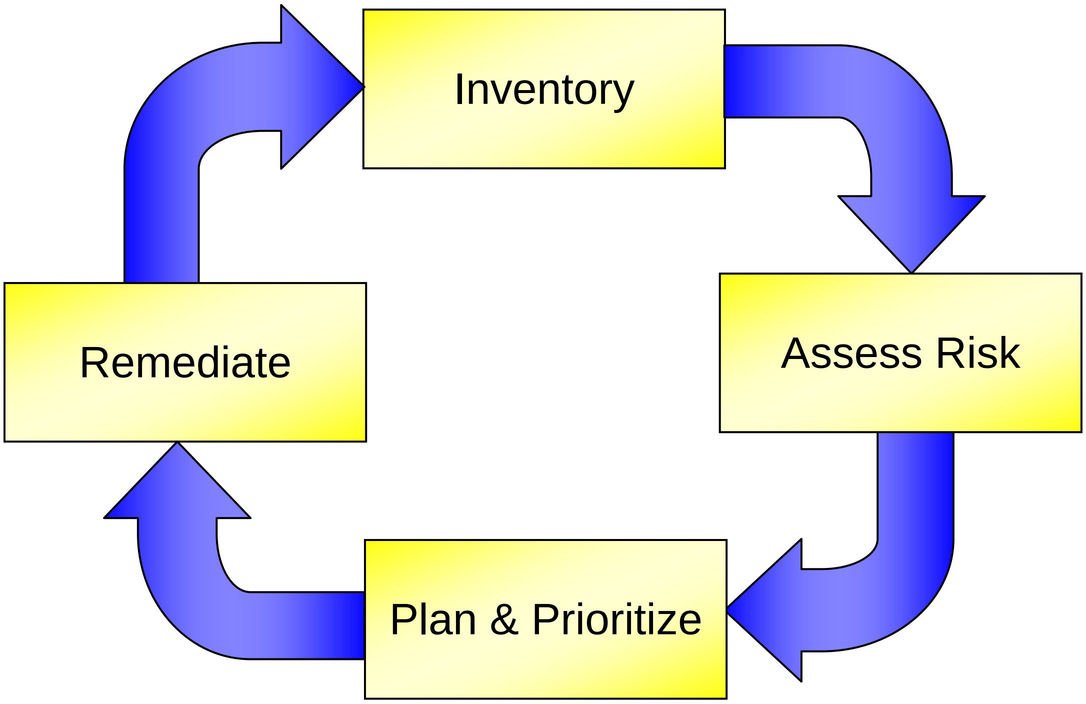
Toomey.org Consulting

White Paper

Advanced Uses of Symantec Enterprise Security Manager: Part 1



January 2006

Abstract:

Today's enterprises face unprecedented challenges in securing their servers, networks, gateways, data and infrastructure. Regulatory requirements such as the Sarbanes-Oxley Act and the Basel II New Capital Accord strain even the largest information security and IT departments. With tighter budgets and increased competition, the need for higher efficiency using fewer resources has never been greater.

This paper outlines several of the advanced features of Symantec Enterprise Security Manager™ (ESM). These capabilities can help security administrators "do more with less", getting additional benefit from the most mature policy compliance tool on the market today.

Advanced Uses of Symantec Enterprise Security Manager: Part 1

Table of Contents

Rev. 20060131

Introduction

Today's enterprises face unprecedented challenges in securing their servers, networks, gateways, infrastructure and data. Regulatory requirements such as the Sarbanes-Oxley Act of 2001 (USA) and the Basel Committee on Banking Supervision new accord (EMEA and Asia Pacific) strain even the largest information security and IT departments. With tighter budgets and increased competition, the need for higher efficiency using fewer resources has never been greater. This paper will describe the value proposition of Symantec Enterprise Security Manager (ESM) from an information security officer / user perspective as well as a more tactical perspective.

Symantec ESM contains many advanced features. These unique capabilities can help security administrators "do more with less", getting additional benefit from the most mature policy compliance tool on the market today.

The advanced uses of Symantec ESM described in Part 1 this white paper include:

1. Entitlements
2. Patch Templates
3. Remediation Capabilities
4. Command Line Interface (CLI)
5. ICE Module
6. Network Assessment Module

Many more advanced features could also be described, but are not included in this white paper. These include:

1. File Content Search (grep)
2. Remote Agent Re-registration
3. Random Audits
4. Baseline Snapshots
5. Using Cognos ReportStudio
6. Rich Content
7. VERITAS Backup Exec Checks
8. Password Cracking (dictionaries, Oracle, percentage)
9. Fully-Qualified Domain Names (FQN) of Modules
10. Policy Tool
11. Policy Research
12. Symantec Information Manager (SIM) Integration
13. Porting ESM Data to a new ESM Manager
14. Changing Message Severities
15. New CLI Commands

Symantec Enterprise Security Manager

Symantec ESM enables organizations to define, measure, and report on the compliance of information systems based on industry, regulatory and corporate security policies and standards to achieve governance, privacy and efficiency. By using Symantec ESM, companies can proactively avoid many costly security problems by ensuring systems are compliant. Symantec ESM provides preconfigured policies to speed up compliance with various regulations and standards. Symantec ESM helps answers the questions, "How secure is my enterprise?" and "Are we compliant with Sarbanes-Oxley and other regulations?"

Symantec ESM was first introduced in 1993 as the Raxco "Security Toolkit 3.0". Symantec ESM today contains over 120,000 security checks "out of the box", including password strength, patches, startup services, registry keys and file attribute settings. It is used by large enterprises and IT auditors to more easily measure compliance and show due diligence.

Entitlements

Overview

Entitlement checks were introduced in September 2005 with ESM SU24 and updated in ESM SU25 the following quarter. They were developed as a change management enhancement request by a large financial institution.

Entitlement is the guarantee for access to computer resources because of access rights.
Entitlements add change management to Symantec ESM:

- SU24 – Solaris Audit IDs / role based access
- SU25 – AIX & HP-UX audit detail enhancements

Practical Uses

Symantec ESM now does more than just policy and vulnerability checks. It ensures that only certain users, roles and profiles have access to certain files and directories. Entitlement checks are used heavily to ensure Sarbanes-Oxley Act (SOA) compliance to ensure that financial files can only be accessed by assigned individuals.

SOA concerns itself with the integrity of the financial reporting process for US publicly traded companies. One of the three operational guidelines established for financial data management is change management. Change Management is monitoring, detecting and reporting changes to the IT systems (i.e. registry), file, network and operations infrastructure that can impact the system of controls implemented to assure compliance with SOA mandates. Put simply, if the files and processes to generate quarterly financial statements are secure, then the CEO and CFO are more likely to sign, in good conscience, the documents before public disclosure.

Using Entitlements

The “role based access” checks for Solaris report when the users, roles, or profiles on the agent system do not match the ESM template definition. These role based access messages include:

- Mandatory attribute not found
- Forbidden attribute found
- Attribute not listed in template

Attributes may include read-only (Ro), read-write (Rw), execute (X), system (Sy), and hidden (H).

The new SU25 Windows check, “Max Administrator Accounts”, reports when the number of user accounts with administrative privileges, on the agent, exceeds the limit defined in the check. This ensures that the number of privileged accounts is limited per corporate policy. Too many admins makes for an insecure environment.

References

- Symantec ESM SU25 Release Notes, p. 26-27
  http://securityresponse.symantec.com/avcenter/security/Content/2005.12.22a.html

Patch Templates

Overview

Patch templates where introduced in 1998 before quarterly Security Updates (SUs). They are updated bi-weekly by the Symantec Security Response team. They are updated within 72 hours if a rapid response is needed, such as for Microsoft Tuesday Patch Day. Each bi-weekly update typically adds 170 - 680 new patch checks to the templates.

Patch templates contain a list of security patches for a given platform or application. They are used by the patch module to check for required and forbidden patches.

At the end of December 2005, Symantec ESM checked for 15,113 patches. ESM's patch templates are highly accurate. When new information is made available, patch entries are updated. 1,081 patch entries were updated in the November 21, 2005 patch update alone.

Practical Uses

Over 80% of all vulnerabilities are remediated with patches. For example, on the second Tuesday of each month, Microsoft releases new patches to address Windows vulnerabilities. If a critical patch was released to prevent "Code Purple", then an ESM audit can be created to check which systems have this new patch installed.

If a policy run is performed with only a single check for a specific patch, then the results can be easily viewed in the ESM console. If the patch template entry does not exist, then users can add their own patch entries rather than wait for Symantec to update them. Patch templates can be separated into more useful groups, such as separate templates for critical, non-critical, and operational patches.

If a certain Microsoft patch (Q317277) always hangs a particular system (Compaq Presario 711CL Laptop), then the patch check can check that that offending patch is <u>not</u> installed.

Using Patch Templates

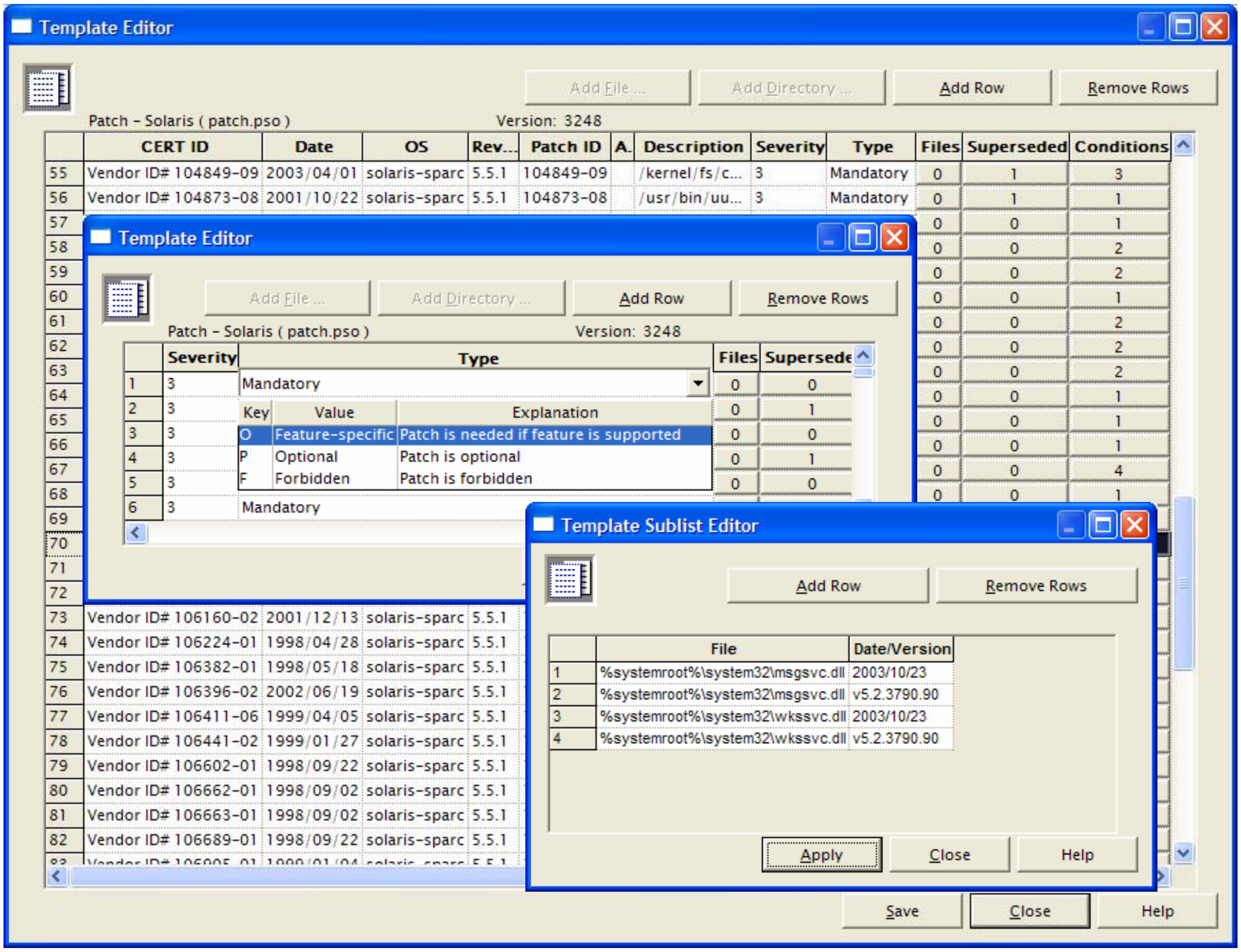
The ability to check for the presence of a component was added in 2003. Instead of reporting a missing patch for a service that was not installed or running, the patch templates now only report them as a policy violation if the services are actually installed and/or running. This makes the computer do the work.

Patch templates are user editable. Fields exist for the patch ID, description, effected files, severity and superseding patches. The format in the ESM console looks like a spreadsheet, but the template files can be edited with a simple text editor (see Figure 1). Since patch templates are updated frequently, some customers create scripts to make changes to different patch templates to match their particular preferences and security policy. These scripts are run after a LiveUpdate to retain their patch template changes.

The "Patch Percent (%) Compliance" enhancement was added in June 2005 in ESM SU23. The new "Patch results summary" option reports:

- Total number of available patches
- Checked patches
- Missing patches
- Forbidden patches

Since new vulnerabilities and patches are announced daily, systems are seldom 100% patched. This change now gives security managers credit for having 100 out of 101 patches installed.



Patch – Solaris (patch.pso) Version: 3248

	CERT ID	Date	OS	Rev...	Patch ID	A.	Description	Severity	Type	Files	Superseded	Conditions
55	Vendor ID# 104849-09	2003/04/01	solaris-sparc	5.5.1	104849-09		/kernel/fs/c...	3	Mandatory	0	1	3
56	Vendor ID# 104873-08	2001/10/22	solaris-sparc	5.5.1	104873-08		/usr/bin/uu...	3	Mandatory	0	1	1
57										0	0	1
58										0	0	2
59										0	0	2
60										0	0	1
61										0	0	2
62										0	0	2
63										0	0	2
64										0	0	1
65										0	0	1
66										0	0	1
67										0	0	4
68										0	0	1
69												
70												
71												
72												
73	Vendor ID# 106160-02	2001/12/13	solaris-sparc	5.5.1								
74	Vendor ID# 106224-01	1998/04/28	solaris-sparc	5.5.1								
75	Vendor ID# 106382-01	1998/05/18	solaris-sparc	5.5.1								
76	Vendor ID# 106396-02	2002/06/19	solaris-sparc	5.5.1								
77	Vendor ID# 106411-06	1999/04/05	solaris-sparc	5.5.1								
78	Vendor ID# 106441-02	1999/01/27	solaris-sparc	5.5.1								
79	Vendor ID# 106602-01	1998/09/22	solaris-sparc	5.5.1								
80	Vendor ID# 106662-01	1998/09/02	solaris-sparc	5.5.1								
81	Vendor ID# 106663-01	1998/09/02	solaris-sparc	5.5.1								
82	Vendor ID# 106689-01	1998/09/22	solaris-sparc	5.5.1								

Patch – Solaris (patch.pso) Version: 3248

	Severity	Type	Files	Supersede
1	3	Mandatory	0	0
2	3		0	1
3	3		0	0
4	3		0	1
5	3		0	0
6	3	Mandatory		

Key	Value	Explanation
O	Feature-specific	Patch is needed if feature is supported
P	Optional	Patch is optional
F	Forbidden	Patch is forbidden

	File	Date/Version
1	%systemroot%\system32\msgsvc.dll	2003/10/23
2	%systemroot%\system32\msgsvc.dll	v5.2.3790.90
3	%systemroot%\system32\wkssvc.dll	2003/10/23
4	%systemroot%\system32\wkssvc.dll	v5.2.3790.90

Figure 1 – ESM Patch Template Editor

References

- Web Advisories of patch template updates:
  http://securityresponse.symantec.com → Symantec ESM → Patch Policies
- Email Notifications of patch template updates:
  http://www.symantec.com/techsupp/bulletin/enterprise.html
- Microsoft Security Bulletins
  http://www.microsoft.com/security

Remediation Capabilities

Overview

A “fix it” capability was introduced in 1999 in ESM SU1 and significantly updated in mid-2002 in ESM SU12. This feature allows you to correct some policy violations from within the ESM console. It provides end-to-end policy compliance with separation of duties enforced.

Practical Uses

Some Symantec ESM users find it convenient to both identify and correct non-compliant messages from a single console.

From the ESM console, you can use the “Correct” feature to correct agent rights or settings. For example, in the Account Integrity module, the “Generate security audits” check reports accounts with rights to generate entries in the security log. If you correct a reported user account, the right is revoked. You can restore the right by repeating the same process that you used to revoke it.

You can also use the “Correct” feature to disable a vulnerable account. In the Password Strength module, for example, you can immediately disable an account that has no password.

Using Remediation

The built-in remediation capability in Symantec ESM is limited to mostly file and registry key permissions and attributes. These include:

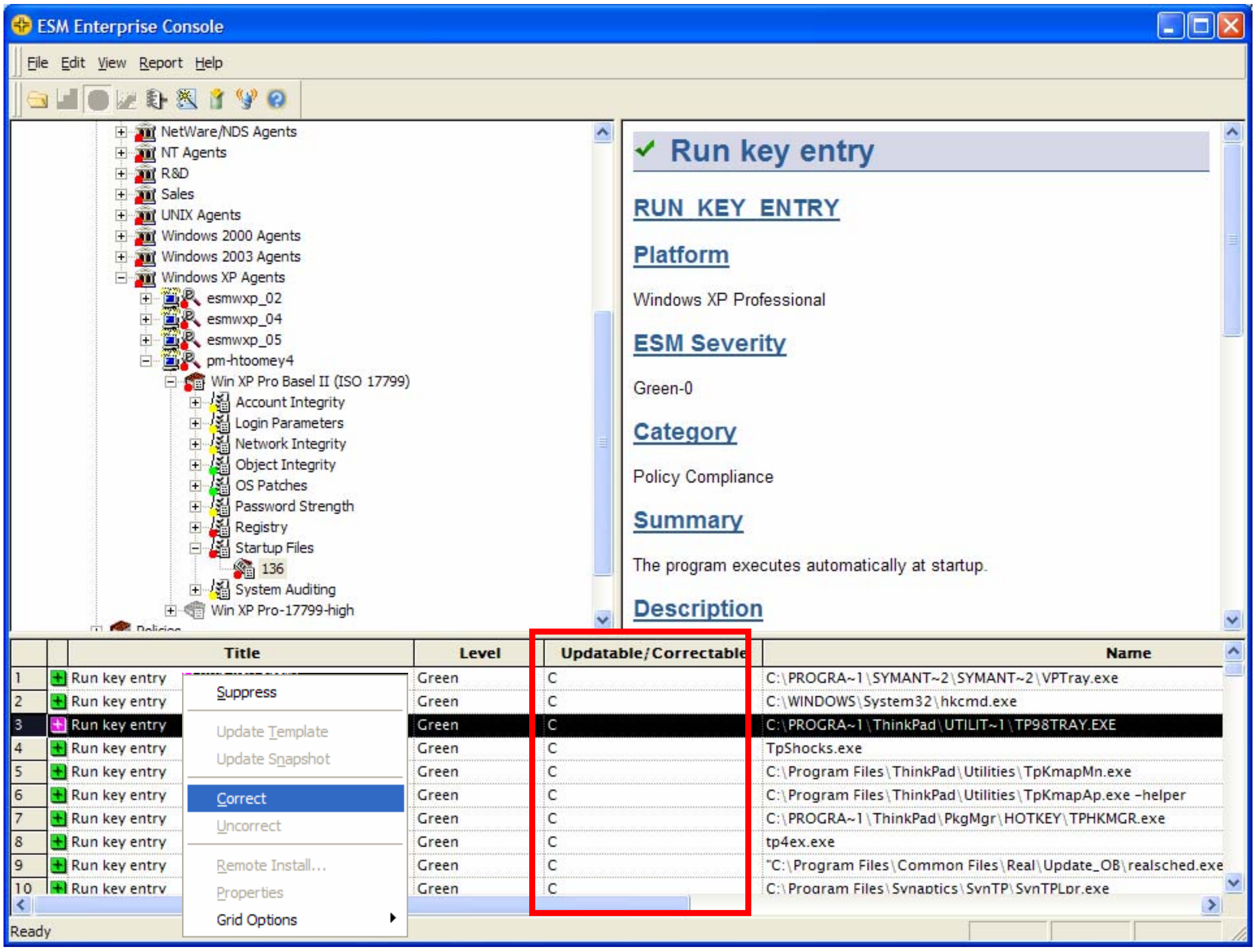
- Registry Keys
- File Permissions
- File Attributes
- Startup Files
- Account Integrity (to snapshot)
- Network Integrity (to snapshot)
- Password Strength (to snapshot)
- System Auditing (to snapshot)

Correctable messages are displayed in the ESM console grid with a letter “C” in the “Updateable / Correctable” column (see Figure 2). Messages that need correcting can be remediated either individually or more efficiently as a group. This is done simply by right clicking the message and choosing “Correct”. After re-authentication, the message is then updated to match either the template data or the baseline snapshot.

To maintain separation of duties, users must re-authenticate in the ESM console before correcting a non-compliant ESM message. This maintains the proper balance between the needs of the security administrator (security) and the IT manager (operational).

More extensive remediation through integration with a patch management system can be done by Symantec Services for many corporate environments.

The Symantec ESM SU17 User’s Guides for Windows and UNIX contain remediation steps for many policy checks. This information was included in the rich content introduced in Symantec ESM 6.5. The vulnerability messages generated from the ESM Network Assessment module also contain rich content that includes detailed steps to remediate. This information is included as part of the Bugtraq vulnerability database information.



✓ Run key entry

RUN_KEY_ENTRY

Platform

Windows XP Professional

ESM Severity

Green-0

Category

Policy Compliance

Summary

The program executes automatically at startup.

Description

		Title	Level	Updatable/Correctable	Name
1	✚	Run key entry	Green	C	C:\PROGRA~1\SYMANT~2\SYMANT~2\VPTray.exe
2	✚	Run key entry	Green	C	C:\WINDOWS\System32\hkcmd.exe
3	✚	Run key entry	Green	C	C:\PROGRA~1\ThinkPad\UTILIT~1\TP98TRAY.EXE
4	✚	Run key entry	Green	C	TpShocks.exe
5	✚	Run key entry	Green	C	C:\Program Files\ThinkPad\Utilities\TpKmapMn.exe
6	✚	Run key entry	Green	C	C:\Program Files\ThinkPad\Utilities\TpKmapAp.exe -helper
7	✚	Run key entry	Green	C	C:\PROGRA~1\ThinkPad\PkgMgr\HOTKEY\TPHKMGR.exe
8	✚	Run key entry	Green	C	tp4ex.exe
9	✚	Run key entry	Green	C	"C:\Program Files\Common Files\Real\Update_OB\realsched.exe
10	✚	Run key entry	Green	C	C:\Program Files\Synaptics\SynTP\SynTPLpr.exe

Figure 2 – ESM Correctable Messages

References

- ESM SU17 User's Guides for Windows, p. 41
  http://securityresponse.symantec.com/avcenter/security/Content/2005.12.22a.html
  This document is provided in each Security Update advisory.
- ESM SU17 User's Guides for UNIX, p. 42
  http://securityresponse.symantec.com/avcenter/security/Content/2005.12.22a.html
  This document is provided in each Security Update advisory.

Command Line Interface (CLI)

Overview

The ESM console is an interactive GUI. The ESM CLI is a text-based console. Both are valid ways to communicate with ESM managers. Both have been part of Symantec ESM since the beginning. Currently the ESM console has more capabilities than the CLI. The ESM CLI currently has 49 unique commands (see Table 1).

You can run batch files with the CLI to automate some Symantec ESM processes. You can also run the CLI in interactive mode.

Practical Uses

Many large Symantec ESM customers use the CLI to provide automation through scripts. Once developed, these scripts can run all Symantec ESM audits and maintenance tasks automatically and unattended.

The CLI allows for NMS / management framework integration with BMC PATROL, Tivoli TMS, CA Unicenter, and HP OpenView. These frameworks can launch an ESM policy run using the CLI. The on-demand audit can be triggered by other network events, such as a network attack or the availability of a new critical patch. The policy results can then be viewed in the NMS console or from within the Symantec ESM console.

The CLI is more efficient for repetitive operations. For example, to insert a dozen new ESM agents into a domain, an ESM batch file can be generated to perform this task very quickly.

Using the CLI

Symantec ESM batch files contain each CLI command that is needed to accomplish a task. For example, a batch file can contain the CLI commands that are needed to run a policy on specific agents in a selected manager domain and write the required reports. For example:

```
% esmc -t -p 5600 -m my_manager -U ESM -P my_password -b my_batch_file.esm
```

Where my_batch_file.esm contains:

```
run job “Phase 3:c Strict” “Windows XP Agents”
sleep -j 0
view report “Phase 3:c Strict” my_agent account 0
```

In this example, the Run command initiates a policy run on the Windows XP Agent domain. The Sleep command makes the CLI wait for each policy run to complete before continuing. The View report command displays the resulting security information for policy “Phase 3:c Strict” on agent “my_agent” from the Account Integrity (account.m) module for job ID 0.

CLI scripts can be run on either a Windows or a UNIX system. The CLI can even be run interactively using the login and logout commands.

Several examples are provided in the Symantec Enterprise Security Manager™ Administrator's Guide, Version 6.5, starting at page 107. This document is on the Symantec ESM 6.5 CD #1 as the file name esm65adminguide.pdf.

CLI Command	CLI Command Options
Create	Create access Create agent Create domain Create policy
Delete	Delete access Delete agent Delete domain Delete job Delete module Delete policy
Insert	Insert agent Insert module Insert name
Login	Login
Logout	Logout
Ping	Ping
Query	Query
Quit	Quit
Remove	Remove agent Remove module Remove name
Run	Run
Set	Set config Set license Set variable
Show	Show access Show agent Show config Show domain Show job Show license Show module Show policy Show sumfinal Show summary Show variable
Shutdown (UNIX only)	Shutdown
Sleep	Sleep
Status	Status
Stop	Stop
Version	Version
View	View agent View audit View checks View custom View differences View domain View policy View report View summary

Table 1 – ESM 6.5 CLI Commands

References

- Symantec Enterprise Security Manager™ Administrator's Guide, Version 6.5, p. 107 - 152. (file name: esm65adminguide.pdf)
- Symantec Enterprise Security Manager™ Administrator's Guide, Version 6.5, p. 109. Provides a list of all ESM module short and long names.

ICE Module

Overview

ICE is an abbreviation for Integrated Command Engine. It was introduced in 1999 with ESM SU2 and updated in ESM SU24 and SU25. ICE templates add new checks to Symantec ESM. The ICE module integrates user provided programs or scripts into Symantec ESM and maps their output to security messages. ICE script results are returned to the ESM manager for reporting.

The ICE module provides another means to perform security checks; complimenting agent and agentless architectures (see Table 2).

Operation **Architecture**	**Policy Compliance (PC)**	**Vulnerability Assessment (VA)**
Host-Based (Agent)	ESM Agents	
Network-Based (Agentless)	*ESM 7 Agentless (to ship in 2006)* BindView bv-Control *(acquired by Symantec in Jan. 2006)*	ESM 6.5 Network Assessment Module*
Remote Execution (Scripts)	ESM ICE Module	N/A

Table 2 – Security Technologies and Remote Script Execution

NOTE: *The NA module of Symantec ESM covers the host-based vulnerabilities as well.

Practical Uses

The ICE module was originally developed to extend the capabilities of Symantec ESM by the customer. For example, a system administrator could write a script or provide an executable to check the settings of a custom application. The script / executable could perform several operations on the agent system, and then return a value back to ESM for compliance reporting.

Many IT managers don't trust agents running on their servers and they don't want the network traffic generated by a network-based approach. Their objective is to keep their servers up and performing at their peak at all times. This requirement is often at odds with security requirements. These same IT managers are more likely to trust scripts running on these servers. They are the predominant users of the ICE module to do security "their way" rather than strictly with a Symantec ESM agent.

Using ICE

Symantec ESM does not provide ICE templates or scripts out-of-the-box. You must create your own. An ICE Module Training Guide is available for download on the SU16 Web page. It contains many examples on how to effectively utilize this module for both Windows and UNIX.

Newly introduced in September 2005 with ESM SU24 is the ability to automatically push scripts / executables to all servers running a Symantec ESM agent before running the scripts. The copy scripts and overwrite scripts checks solves the management nightmare of deploying multiple scripts to multiple ESM agents. It also makes for more consistent configuration management, since different versions of the same script will now be updated with the same and most current script.

This new option to push scripts is securely implemented. Many security precautions were taken before adding this new capability. See user permissions and ownership security setting recommendations in the release notes for the most secure use. As an added precaution, scripts can be pushed only to the ESM installation directory structure on the agent. ESM SU25 in December 2005 added a new option to block the copying of scripts to individual ESM agents as an added precaution to avoid the potential for abuse.

References

- Symantec ESM SU25 Release Notes, p. 8 - 9, 21 - 23
  http://securityresponse.symantec.com/avcenter/security/Content/2005.12.22a.html
- ESM SU17 User's Guides for Windows, p. 267 - 283
  http://securityresponse.symantec.com/avcenter/security/Content/2005.12.22a.html
  This document is provided in each Security Update advisory.
- ESM SU17 User's Guides for UNIX, p. 225 - 240
  http://securityresponse.symantec.com/avcenter/security/Content/2005.12.22a.html
  This document is provided in each Security Update advisory.
- ESM SU16 ICE Module Training Guide Demonstration
  http://securityresponse.symantec.com/avcenter/security/Content/2003.07.30b.html
- ESM SU16 ICE Module Training Guide for Windows and UNIX
  http://securityresponse.symantec.com/avcenter/security/Content/2003.07.30b.html

Network Assessment Module

Overview

The network assessment (NA) module was introduced in June 2005 with ESM 6.5. The NA module tightly integrates network vulnerability scans from Symantec ESM agents. Policy audits can now include checks for vulnerabilities.

The NA module compliments Symantec ESM's policy checks, providing wider security coverage. For example, Symantec ESM agents cannot be placed on many network devices, such as Cisco routers and wireless access points. These devices can now be scanned over the network for vulnerabilities.

Vulnerability assessments and policy compliance checks both arrive at the need to deploy the same mitigating controls, such as applying a patch or making a configuration change (see Figure 3). Both approach the same security problem from differing viewpoints. A combination of the two is considered to be best practice.

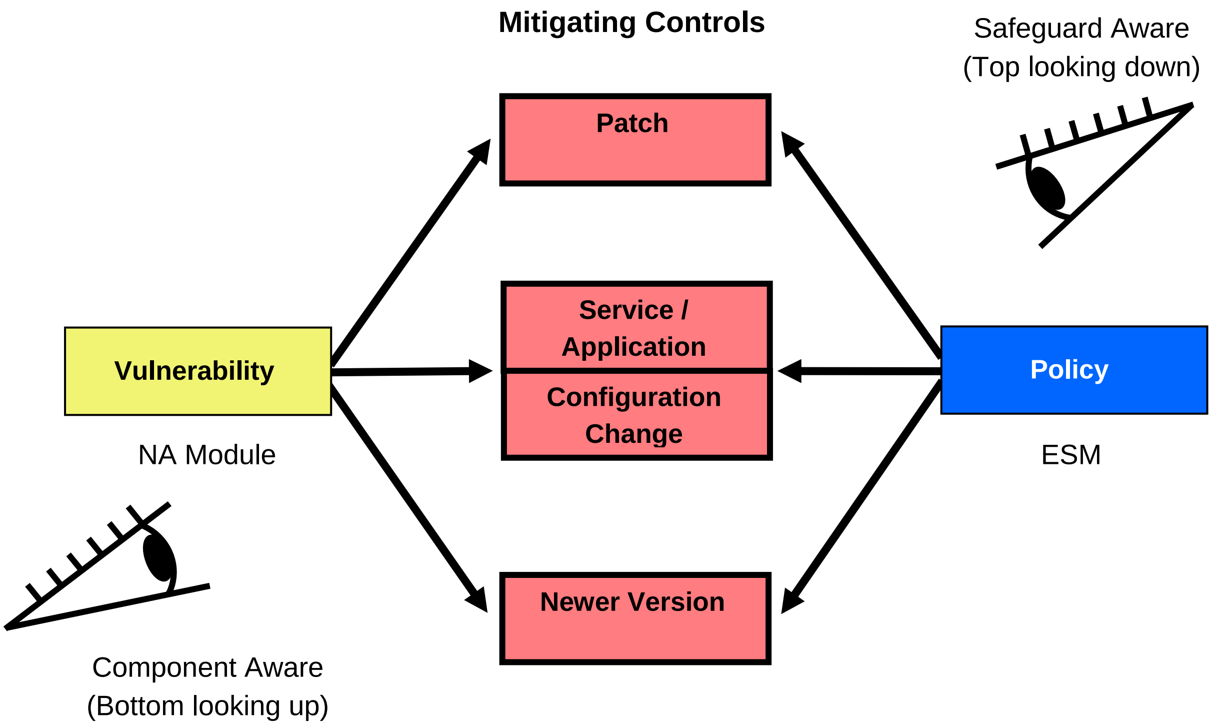


Figure 3 – Vulnerability vs. Policy View

Diagram © Copyright 2005 Symantec Corporation. All rights reserved.

As of December 2005, the Network Assessment module had the equivalent number of signatures as Symantec NetRecon, a since retired stand-alone vulnerability scanner whose major capabilities are now integrated into Symantec ESM 6.5 as the Network Assessment module. The vulnerability and exposure content is growing rapidly, and is updated monthly via LiveUpdate.

Practical Uses

Use the NA module to scan 50 network segments from a single ESM console. You can create customized Network Assessment policies to split up the scanning of an enterprise in logical ways and assign them to one or more ESM agents. This is far more efficient than scanning each network segment with a stand-alone, non-distributed scanning tool.

The NA module provides the benefits of distributed scans with central administration from a single console. Unlike other vulnerability scanners, scan data from multiple agents is automatically consolidated into the same data store. The scan data is also integrated into Symantec ESM's advanced enterprise reporting, with two predefined reports included in Symantec ESM 6.5.

The NA messages reference Bugtraq vulnerability IDs. This detailed information can be used to better understand the vulnerabilities and how to best remediate them. Vulnerabilities can also be manually correlated with similar host-based ESM checks, such as missing patches, for a more comprehensive view of security.

Using the NA Module

The Network Assessment module is tightly integrated into Symantec ESM. Network assessments are managed from the Symantec ESM console. It uses the same module format, and data is displayed in the ESM console and reports along side policy compliance messages. The ESM console policy wizard is used to run scans immediately or scheduled. This lets you schedule scans for devices such as laptops that can be accessed on the network at specific times.

To create a NA scan policy you simply need to specify the ESM agent and the range of IPs to scan.

References

- Symantec™ ESM 6.5 Network Assessment Implementation Guide
  Ships on the ESM 6.5 Windows CD
- Web Advisories of Network Assessment security updates:
  http://securityresponse.symantec.com → Symantec ESM → ESM Network Assessment module Security Updates → Network Assessment Security Updates

The Final Word

Sometimes, just being aware of some of the more advanced features of a product like Symantec ESM can provide an avenue to make the job of a security manager easier. This paper introduced several key and often unknown features of Symantec ESM. It detailed each capability and provided information on their practical use. Additional references where provided to allow you to research each capability further and in more depth.

After over 12 years of development, it is no wonder that very few people really know all of the capabilities of Symantec ESM. It is a powerful and mature policy compliance and vulnerability assessment solution. As a customer and market driven solution, we can expect to see new capabilities added and integrated both quarterly with the ESM SUs as well as annually with each new point release.

The advanced features outlined in this paper are just the tip of the iceberg. Part 2 of this white paper will address another set of practical advanced uses of Symantec ESM.

This white paper was sponsored by Symantec Corporation.

While every care has been taken during the preparation of this document to ensure accurate information, the publishers cannot accept responsibility for any errors or omissions.

About Toomey.org Consulting

With a belief that information security is a necessary and critical business process, Toomey.org Consulting works with clients to identify risks, assess controls, plan, prioritize and remediate security vulnerabilities and policy non-compliance to achieve regulatory compliance.

http://www.toomey.org

About the Author

Harold Toomey has over 17 years experience in information technology. He has eight years of experience in the information security space working closely with Fortune 100 companies to assess their security compliance needs. Previously Toomey held positions as a Technical Product Manager at AXENT Technologies and as a Product Manager at Symantec for Symantec ESM and Symantec NetRecon. Earlier in his career he held engineering and development management positions with CallWare Technologies, Novell Inc., and the US Air Force Systems Command.

He is a frequent presenter on various security topics from wireless security to policy compliance and vulnerability assessment. Toomey holds a master’s in electrical and computer engineering from Brigham Young University. He is certified as a CISSP, CISA, CISM, NSA IAM and Novell Master CNE. He is the proud father of four beautiful children: 3 boys and 1 little princess.

harold@toomey.org