Tenable Nessus 和思科身份服务集成

目录

关于本文档

本文档适用于部署 Tenable Nessus 和思科身份服务引擎 (ISE) 1.3 或思科身份服务引擎 (ISE) 1.2 的思科工程师、合作伙伴和客户。读者应熟悉 Tenable Nessus 和 ISE。

Tenable Nessus 和 ISE 集成可基于漏洞扫描结果提供会话记录信息，并通过思科 ISE RESTful 服务 API 对终端执行自适应网络控制 (ANC) 隔离/非隔离缓解操作。

Nessus Enterprise 6.1.x 和 6.2x、Nessus Manager 6.3 及更高版本将与 ISE 集成。无需特殊许可。请注意，Nessus Manager 将取代 Nessus Enterprise，Nessus Enterprise 并未停售，但实行按主机许可证模式，这不会对 ISE 集成产生任何影响。

.

简介

Tenable Nessus 是一款可提供漏洞发现、合规性审核、控制系统审核及敏感内容审核等功能的漏洞扫描工具。Tenable 能够根据扫描结果使用思科身份服务引擎 (ISE) 外部 RESTful 服务 API 在终端上提供缓解操作。

ISE 外部 RESTful 服务基于 HTTPS 和 REST 方法，并被 Tenable 用于从终端获取更多情景信息。此类情景信息包括用户名、设备信息、隔离/非隔离状态及最后更新记录。

本文档包括初始的 Tenable 和 ISE 配置，并提供了一个扫描示例，其中包括 Tenable 和 ISE 中显示的各种结果。

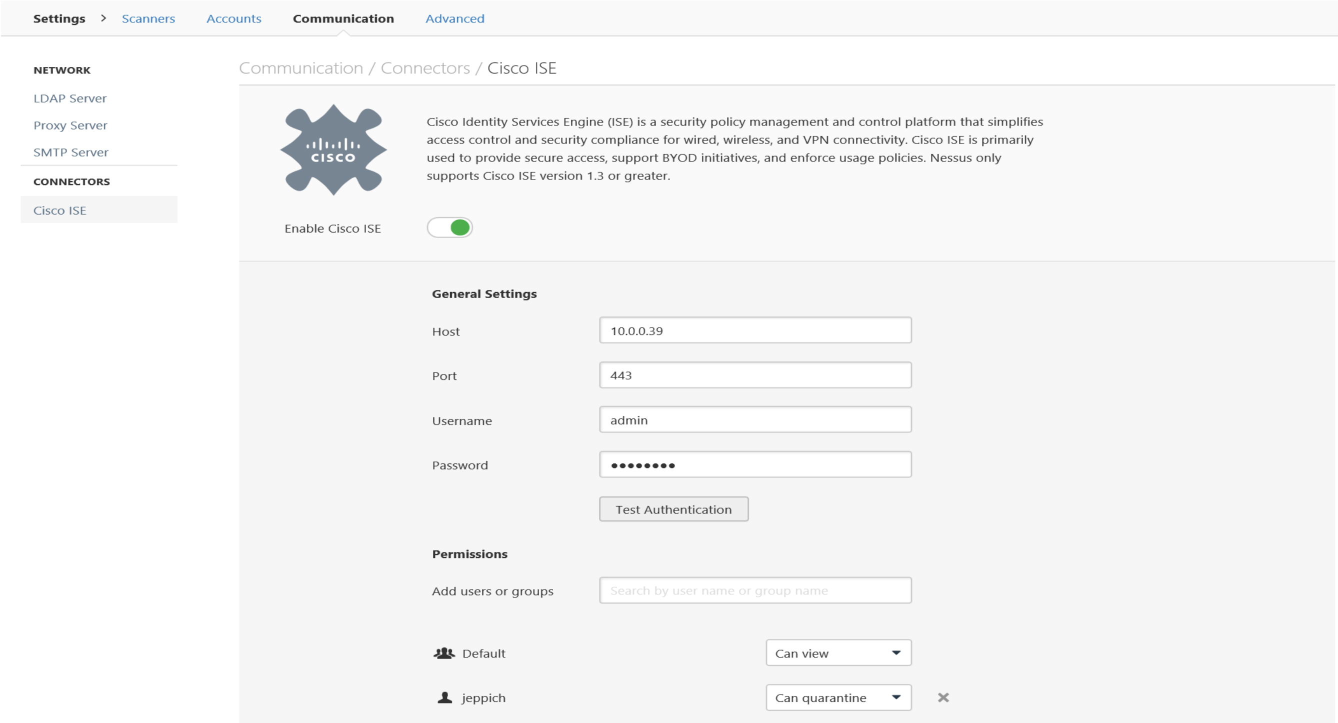
Tenable Nessus 配置

思科 ISE 连接参数可在“Settings”-> “Communication”视图下访问。

“General Settings”参数用于 ISE。ISE 主机是指 ISE MnT 节点 IP 地址。 “ISE Username”和“Password”属于 ISE ERS 或 ISE 管理员组。您可以在具有已安装的 Nessus 和 ISE 的 Web 客户端之间进行身份验证测试，以确保不存在连接问题。

“Permissions”参数用于 Nessus 帐户。下图所示的“Default”组可以查看扫描结果。Nessus 用户“jeppich”能够根据漏洞扫描结果隔离和不隔离主机。

步骤 1. 下面列出的是初始 ISE 连接参数。
“Settings”-> “Communication”。


Settings > Scanners Accounts Communication Advanced
NETWORK
LDAP Server
Proxy Server
SMTP Server
CONNECTORS
Cisco ISE
Communication / Connectors / Cisco ISE
CISCO
Test Authentication
Search by user name or group name

Cisco Identity Services Engine (ISE) is a security policy management and control platform that simplifies access control and security compliance for wired, wireless, and VPN connectivity. Cisco ISE is primarily used to provide secure access, support BYOD initiatives, and enforce usage policies. Nessus only supports Cisco ISE version 1.3 or greater.

Enable Cisco ISE ●

General Settings

Host: 10.0.0.39

Port: 443

Username: admin

Password: ••••••••

Permissions

Add users or groups

Default: Can view

jeppich: Can quarantine ✕

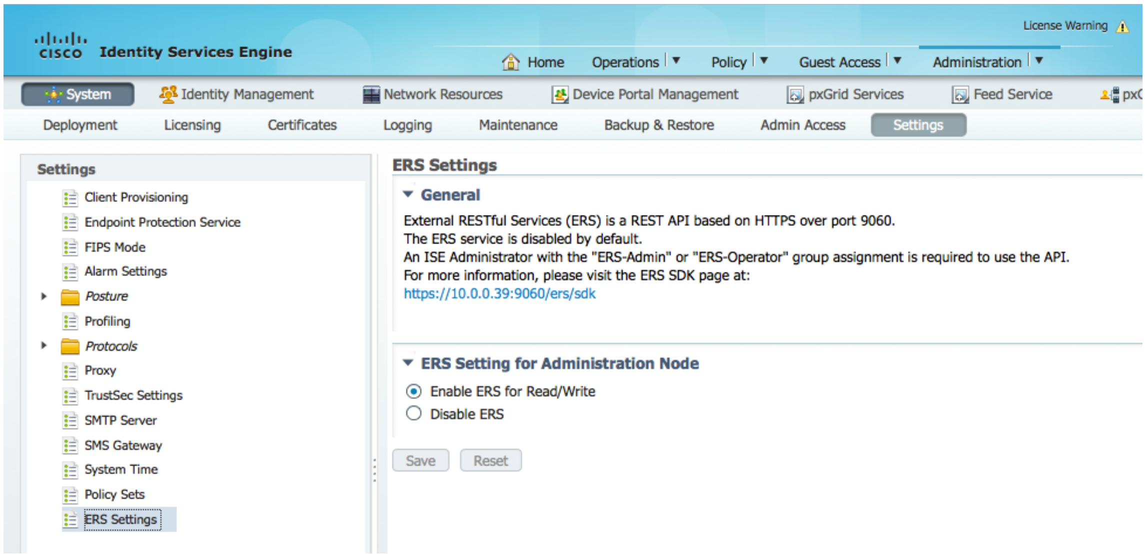
思科 ISE 身份引擎 1.3 配置

ISE 将配置为启用 RESTful API 和终端保护服务。此外，系统还会创建授权配置文件以及用于隔离终端的授权配置文件。

启用 ISE RESTful API

步骤 1. 启用 ERS 设置。
依次点击“Administration” -> “System” -> “Settings” -> “ERS Settings”，然后点击“Save”。

注：在分布式 ISE 环境中，您还需要为其他节点“启用”ERS 设置。



ERS Settings

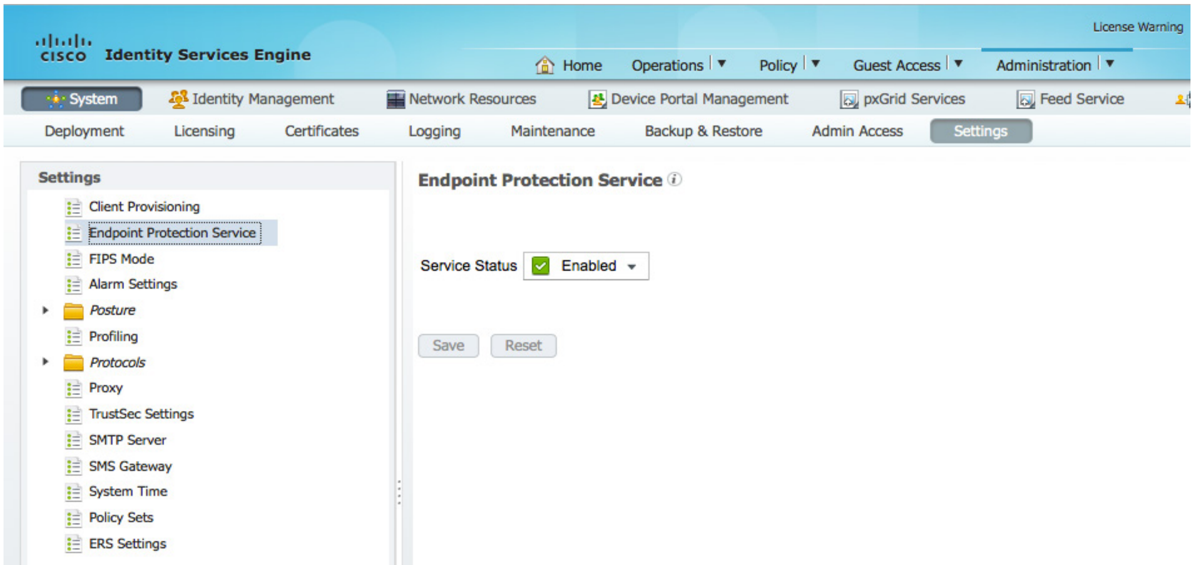
General

External RESTful Services (ERS) is a REST API based on HTTPS over port 9060.
The ERS service is disabled by default.
An ISE Administrator with the "ERS-Admin" or "ERS-Operator" group assignment is required to use the API.
For more information, please visit the ERS SDK page at:
https://10.0.0.39:9060/ers/sdk

ERS Setting for Administration Node

● Enable ERS for Read/Write
○ Disable ERS

步骤 2. 启用终端保护服务。
依次点击“Administration” -> “System” -> “Settings” -> “enable Service Status”，然后点击“Save”。



Endpoint Protection Service

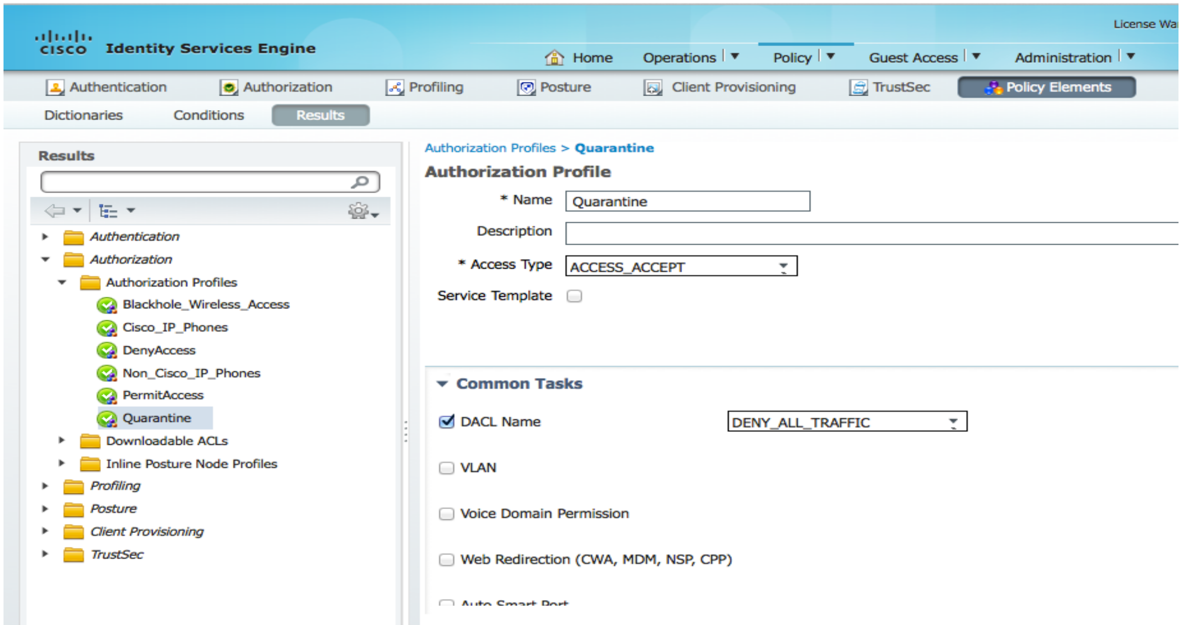
Service Status ✓ Enabled

创建用于隔离的授权策略

此处，我们将创建 EPS 隔离授权配置文件和用于隔离终端的授权配置文件。

步骤 1. 创建隔离授权配置文件。
依次点击“Policy”->“Policy Elements”->“Results”->“Authorization”->“Authorization Profiles”，添加 Quarantine 配置文件，然后点击“Submit”。

注：您可以选择“DENY”或“ALLOW”测试所有流量。授权策略配置文件结果在 ISE 运行身份验证视图下仍将为“Quarantine”。



Authorization Profiles > Quarantine

Authorization Profile

* Name: Quarantine

Description:

* Access Type: ACCESS_ACCEPT

Service Template ☐

Common Tasks

☑ DACL Name: DENY_ALL_TRAFFIC

☐ VLAN

☐ Voice Domain Permission

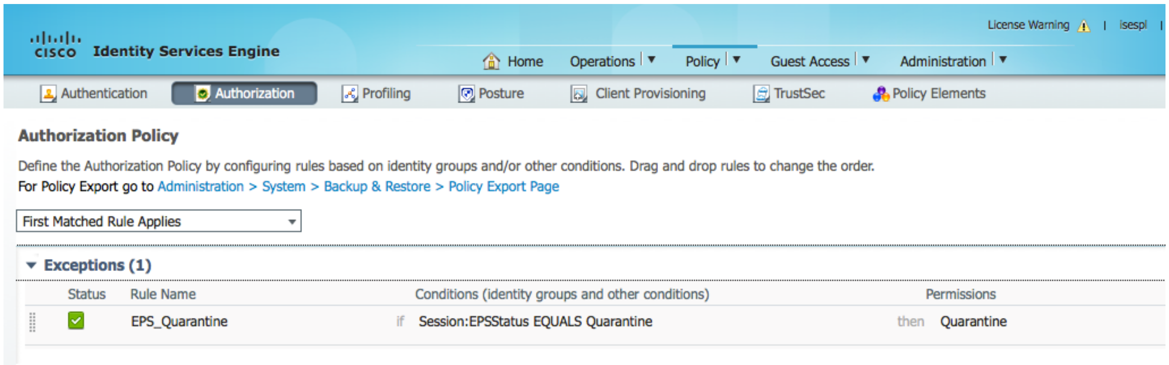
☐ Web Redirection (CWA, MDM, NSP, CPP)

☐ Auto Smart Port

步骤 2. 创建 EPS 隔离授权策略。
点击“Policy”->“Authorization”->“Exceptions”，然后按照以下说明创建新规则：

- 提供规则名称：EPS_Quarantine
- 创建新条件：Session:Equals:Quarantine
- 权限：基于标准配置文件的隔离

“Click”->“Done”->“Save”。



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (1)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	EPS_Quarantine	if	Session:EPSStatus EQUALS Quarantine	then	Quarantine

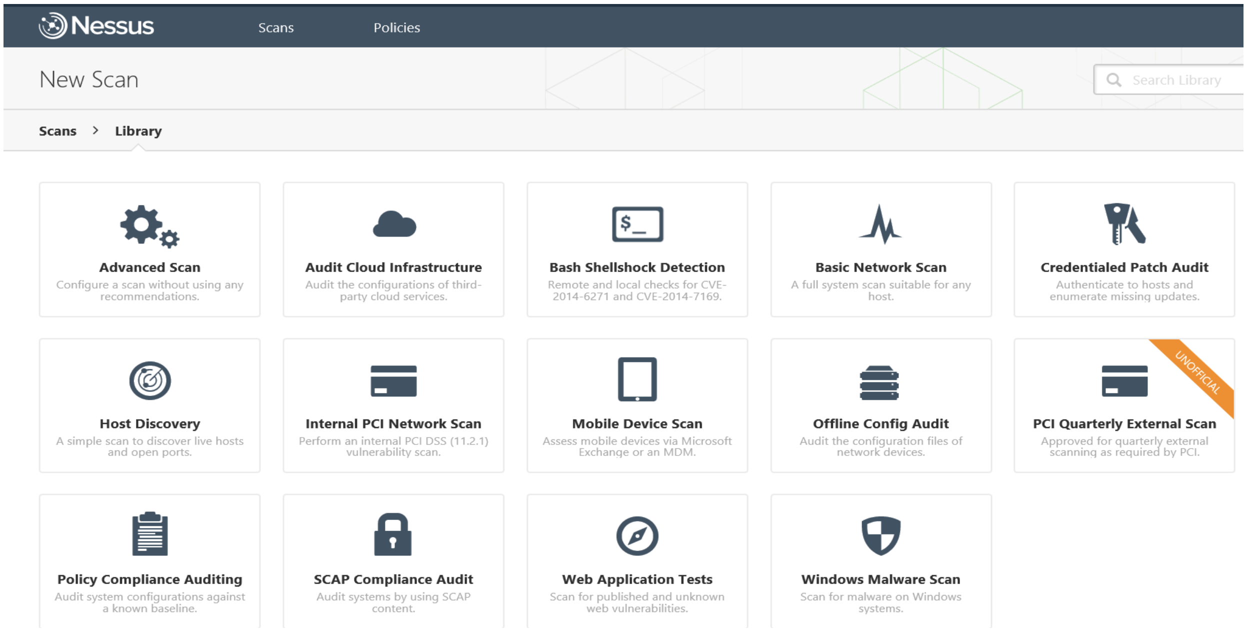
运行 Nessus 扫描并执行 ISE 缓解操作

以下步骤提供有关运行“Basic Network Scan”和根据扫描结果隔离/不隔离终端的详细信息。

步骤 1. 运行“Basic Network Scan”。
“New Scan”->“Scans”->“Basic Network Scan”。

注：假定 Nessus 用户帐户具有“quarantine”权限，则所显示的 ISE 缓解操作可运行任何 Nessus 扫描。

虽然对于所有的扫描，都可能会显示思科 ISE 连接器，但“Audit Cloud Infrastructure”扫描和“Offline Config Audit”扫描不可能生成与隔离相关的数据，因为它们均不用于主机。



Advanced Scan
Configure a scan without using any recommendations.

Audit Cloud Infrastructure
Audit the configurations of third-party cloud services.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan
A full system scan suitable for any host.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Host Discovery
A simple scan to discover live hosts and open ports.

Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit
Audit the configuration files of network devices.

PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

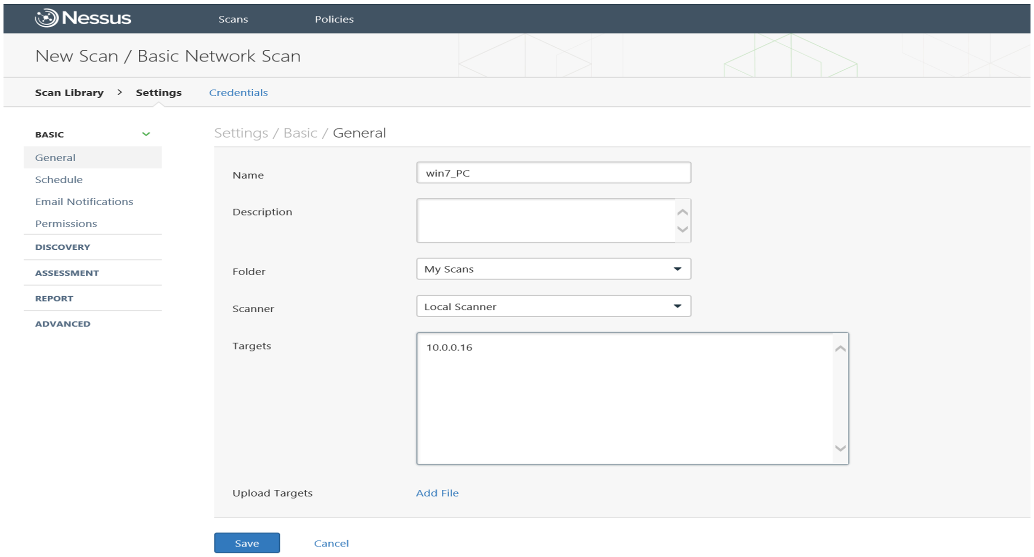
Policy Compliance Auditing
Audit system configurations against a known baseline.

SCAP Compliance Audit
Audit systems by using SCAP content.

Web Application Tests
Scan for published and unknown web vulnerabilities.

Windows Malware Scan
Scan for malware on Windows systems.

步骤 2. 提供主机名和目标信息，然后保存，此操作将启动扫描。

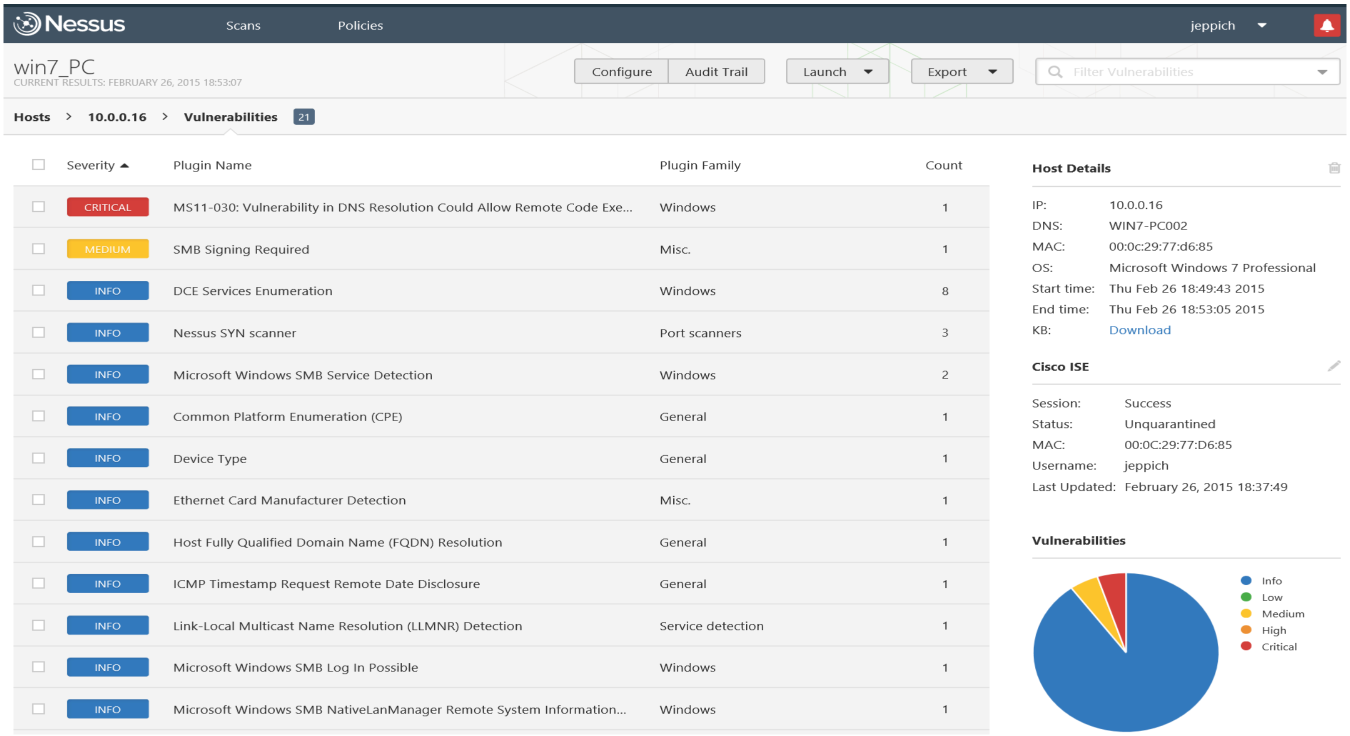


New Scan / Basic Network Scan

Settings / Basic / General

Name	win7_PC
Description	
Folder	My Scans
Scanner	Local Scanner
Targets	10.0.0.16
Upload Targets	Add File

步骤 3. 扫描完成后，选择主机名以查看扫描结果。
思科 ISE 会话记录提供 IEE 802.1X 经过身份验证的主机的缓解状态信息。



win7_PC
CURRENT RESULTS: FEBRUARY 26, 2015 18:53:07

Hosts > 10.0.0.16 > Vulnerabilities 21

Severity ▲	Plugin Name	Plugin Family	Count
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Exe...	Windows	1
MEDIUM	SMB Signing Required	Misc.	1
INFO	DCE Services Enumeration	Windows	8
INFO	Nessus SYN scanner	Port scanners	3
INFO	Microsoft Windows SMB Service Detection	Windows	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
INFO	Microsoft Windows SMB Log In Possible	Windows	1
INFO	Microsoft Windows SMB NativeLanManager Remote System Information...	Windows	1

Host Details

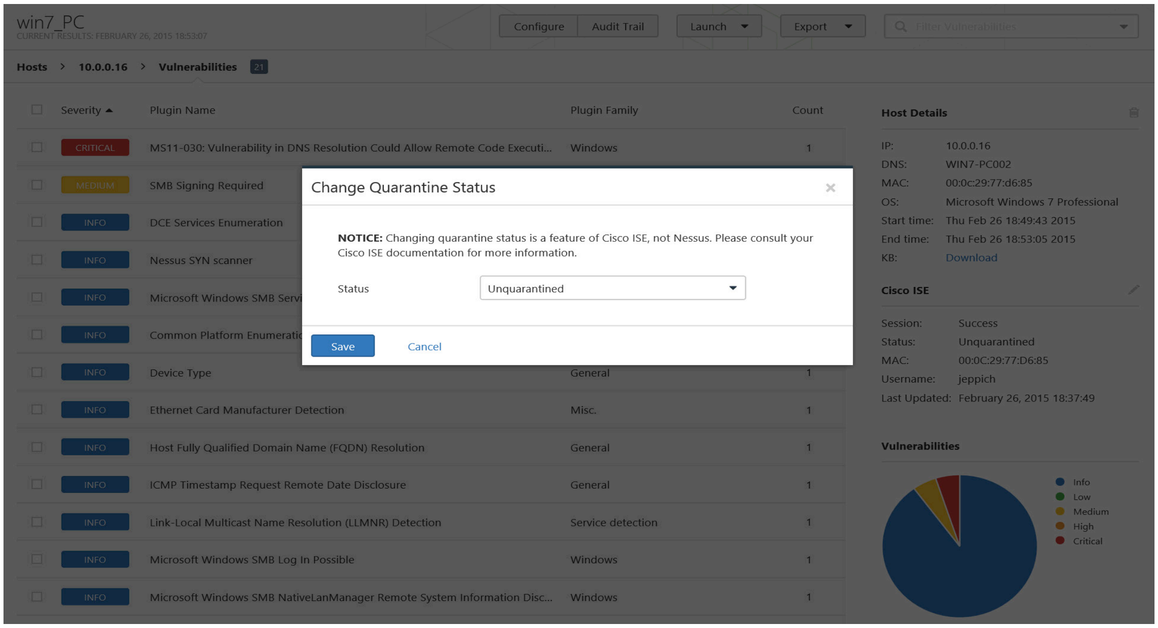
IP:	10.0.0.16
DNS:	WIN7-PC002
MAC:	00:0c:29:77:d6:85
OS:	Microsoft Windows 7 Professional
Start time:	Thu Feb 26 18:49:43 2015
End time:	Thu Feb 26 18:53:05 2015
KB:	Download

Cisco ISE

Session:	Success
Status:	Unquarantined
MAC:	00:0C:29:77:D6:85
Username:	jeppich
Last Updated:	February 26, 2015 18:37:49

Vulnerabilities

步骤 4. 要隔离终端，请点击思科 ISE 旁边的铅笔图标，此操作可显示缓解操作窗口。



win7_PC
CURRENT RESULTS: FEBRUARY 26, 2015 18:53:07

Hosts > 10.0.0.16 > Vulnerabilities 21

□	Severity ▲	Plugin Name	Plugin Family	Count
□	CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Executi...	Windows	1
□	MEDIUM	SMB Signing Required		
□	INFO	DCE Services Enumeration		
□	INFO	Nessus SYN scanner		
□	INFO	Microsoft Windows SMB Servi		
□	INFO	Common Platform Enumeratio		
□	INFO	Device Type	General	1
□	INFO	Ethernet Card Manufacturer Detection	Misc.	1
□	INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
□	INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
□	INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
□	INFO	Microsoft Windows SMB Log In Possible	Windows	1
□	INFO	Microsoft Windows SMB NativeLanManager Remote System Information Disc...	Windows	1

Change Quarantine Status ×

NOTICE: Changing quarantine status is a feature of Cisco ISE, not Nessus. Please consult your Cisco ISE documentation for more information.

Status: Unquarantined

Host Details

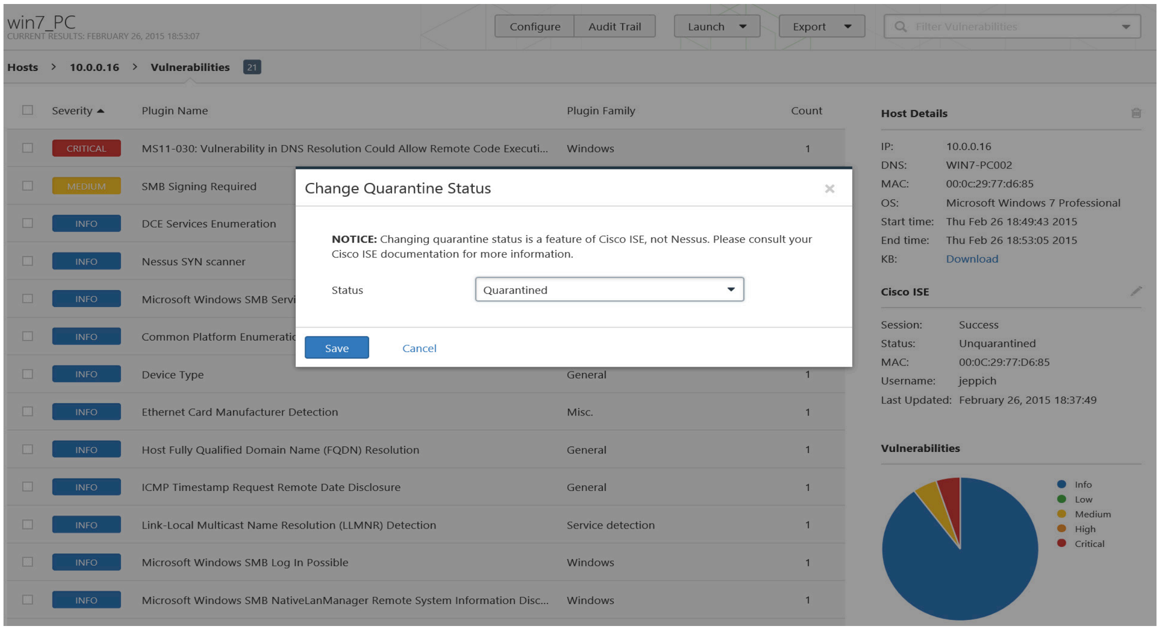
IP: 10.0.0.16
DNS: WIN7-PC002
MAC: 00:0c:29:77:d6:85
OS: Microsoft Windows 7 Professional
Start time: Thu Feb 26 18:49:43 2015
End time: Thu Feb 26 18:53:05 2015
KB: Download

Cisco ISE

Session: Success
Status: Unquarantined
MAC: 00:0C:29:77:D6:85
Username: jeppich
Last Updated: February 26, 2015 18:37:49

Vulnerabilities

步骤 5. 点击下拉菜单并选择“Quarantined”。



win7_PC
CURRENT RESULTS: FEBRUARY 26, 2015 18:53:07

Hosts > 10.0.0.16 > Vulnerabilities 21

□	Severity ▲	Plugin Name	Plugin Family	Count
□	CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Executi...	Windows	1
□	MEDIUM	SMB Signing Required		
□	INFO	DCE Services Enumeration		
□	INFO	Nessus SYN scanner		
□	INFO	Microsoft Windows SMB Servi		
□	INFO	Common Platform Enumeratio		
□	INFO	Device Type	General	1
□	INFO	Ethernet Card Manufacturer Detection	Misc.	1
□	INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
□	INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
□	INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
□	INFO	Microsoft Windows SMB Log In Possible	Windows	1
□	INFO	Microsoft Windows SMB NativeLanManager Remote System Information Disc...	Windows	1

Change Quarantine Status ×

NOTICE: Changing quarantine status is a feature of Cisco ISE, not Nessus. Please consult your Cisco ISE documentation for more information.

Status: Quarantined

Host Details

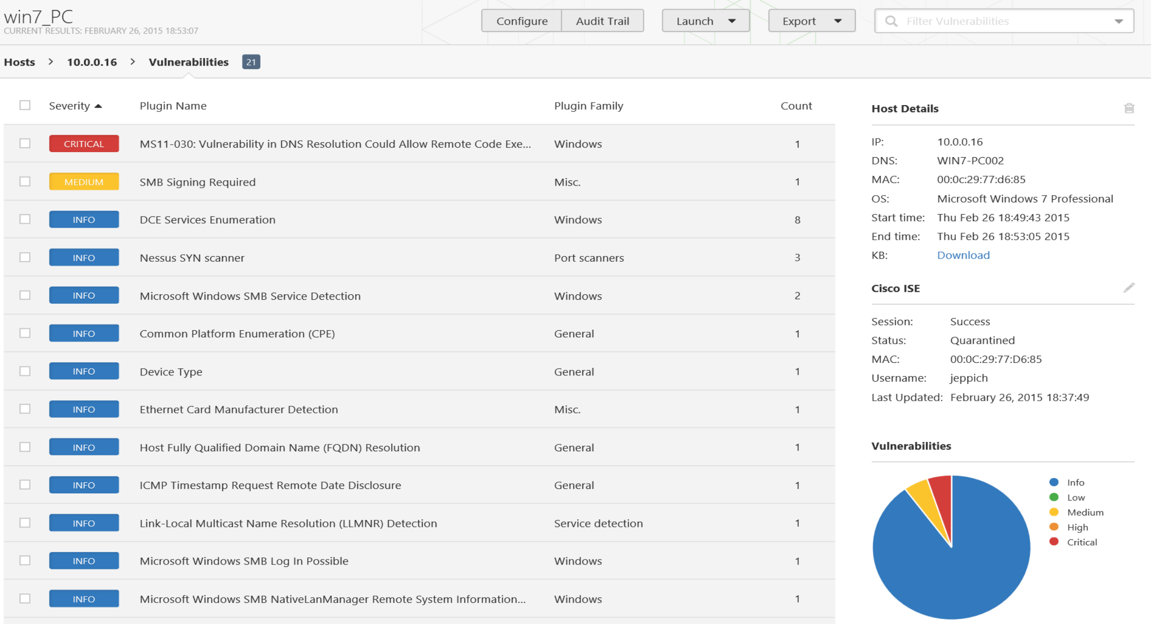
IP: 10.0.0.16
DNS: WIN7-PC002
MAC: 00:0c:29:77:d6:85
OS: Microsoft Windows 7 Professional
Start time: Thu Feb 26 18:49:43 2015
End time: Thu Feb 26 18:53:05 2015
KB: Download

Cisco ISE

Session: Success
Status: Unquarantined
MAC: 00:0C:29:77:D6:85
Username: jeppich
Last Updated: February 26, 2015 18:37:49

Vulnerabilities

步骤 6. 您应该会注意到设备已处于“Quarantined”状态。



win7_PC
CURRENT RESULTS: FEBRUARY 26, 2015 18:53:07

Hosts > 10.0.0.16 > Vulnerabilities 21

□	Severity ▲	Plugin Name	Plugin Family	Count
□	CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Exe...	Windows	1
□	MEDIUM	SMB Signing Required	Misc.	1
□	INFO	DCE Services Enumeration	Windows	8
□	INFO	Nessus SYN scanner	Port scanners	3
□	INFO	Microsoft Windows SMB Service Detection	Windows	2
□	INFO	Common Platform Enumeration (CPE)	General	1
□	INFO	Device Type	General	1
□	INFO	Ethernet Card Manufacturer Detection	Misc.	1
□	INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
□	INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
□	INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
□	INFO	Microsoft Windows SMB Log In Possible	Windows	1
□	INFO	Microsoft Windows SMB NativeLanManager Remote System Information...	Windows	1

Host Details

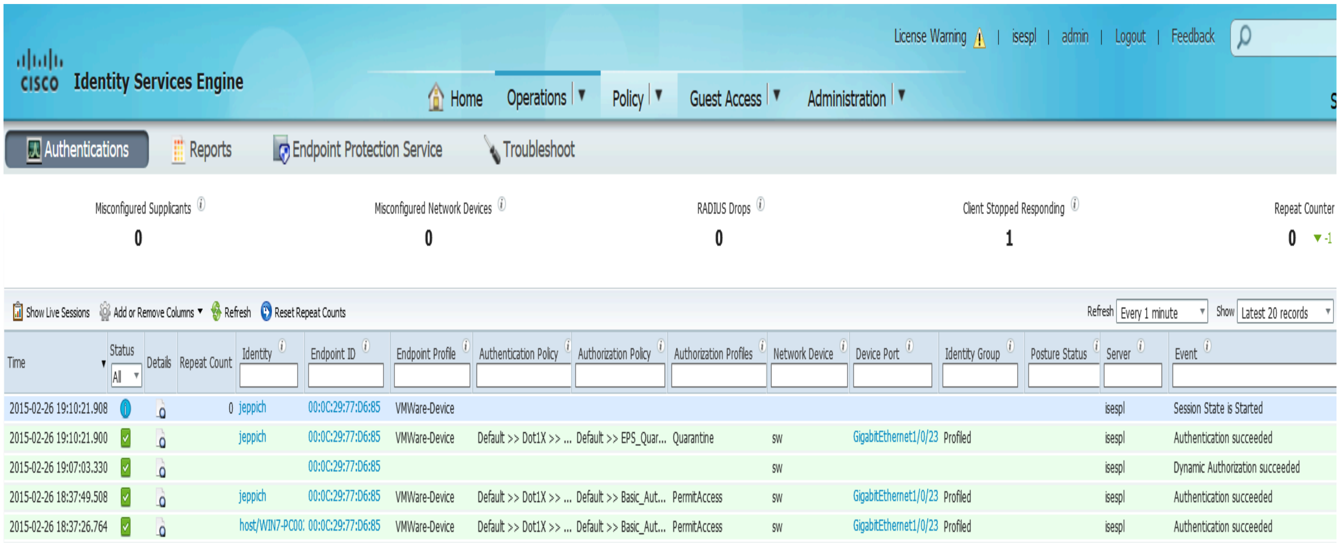
IP:	10.0.0.16
DNS:	WIN7-PC002
MAC:	00:0c:29:77:d6:85
OS:	Microsoft Windows 7 Professional
Start time:	Thu Feb 26 18:49:43 2015
End time:	Thu Feb 26 18:53:05 2015
KB:	Download

Cisco ISE

Session:	Success
Status:	Quarantined
MAC:	00:0C:29:77:D6:85
Username:	jeppich
Last Updated:	February 26, 2015 18:37:49

Vulnerabilities

步骤 7. 在 ISE 中查看。
“Operations” -> “Authentications”。
您会看到终端已被隔离。



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	1	0 ▼-1

Refresh: Every 1 minute　Show: Latest 20 records

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port	Identity Group	Posture Status	Server	Event
	All														
2015-02-26 19:10:21.908	ⓘ		0	jeppich	00:0C:29:77:D6:85	VMWare-Device								isespl	Session State is Started
2015-02-26 19:10:21.900	✓			jeppich	00:0C:29:77:D6:85	VMWare-Device	Default >> Dot1X >> ...	Default >> EPS_Quar...	Quarantine	sw	GigabitEthernet1/0/23	Profiled		isespl	Authentication succeeded
2015-02-26 19:07:03.330	✓				00:0C:29:77:D6:85					sw				isespl	Dynamic Authorization succeeded
2015-02-26 18:37:49.508	✓			jeppich	00:0C:29:77:D6:85	VMWare-Device	Default >> Dot1X >> ...	Default >> Basic_Aut...	PermitAccess	sw	GigabitEthernet1/0/23	Profiled		isespl	Authentication succeeded
2015-02-26 18:37:26.764	✓			host/WIN7-PC00:	00:0C:29:77:D6:85	VMWare-Device	Default >> Dot1X >> ...	Default >> Basic_Aut...	PermitAccess	sw	GigabitEthernet1/0/23	Profiled		isespl	Authentication succeeded

故障排除

Tenable Nessus 扫描完成后显示 Cannot“Open Session”Records

如果您在 Tenable Nessus 扫描完成后收到 cannot“Open Session”records 消息，而且您已验证了 ISE 连接参数，请检查交换机配置并确保您已进行以下设置：

```
# aaa accounting system default start-stop group radius
```

```
# aaa accounting update periodic {value in minutes}
```

有关参考资料，请参阅：http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xe-3s/sec-usr-aaa-xe-3s-book/sec-cfg-accountg.html

参考资料

思科身份服务引擎 ISE 1.3 管理指南：http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13.html

启用 ISE 1.3 RESTful API：http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/api_ref_guide/api_ref_book/ise_api_ref_ers1.html

启用 ISE 1.2 RESTful API：http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/api_ref_guide/api_ref_book/ise_api_ref_ers1.html

Nessus 6.3 安装和配置指南：http://static.tenable.com/documentation/nessus_6.3_installation_guide.pdf