# V.M

# OPERATION CHIMERA

VULNERABILITY MANAGEMENT // SECURITY BLUE TEAM

## CONTENTS

This information has been gathered from public sources and combined with my own knowledge and experiences for the purpose of Operation Chimera, an online, live blue-team training operation conducted by myself under the alias Known Divide, for the SecurityBlueTeam community.

**Useful Links:**
**[1]** https://securitytrails.com/blog/top-20-intel-tools
**[2]** https://www.sans.org/course/open-source-intelligence-gathering
**[3]** https://securitytrails.com/blog/what-is-osint-how-can-i-make-use-of-it

Anything we've missed? Please let us know, so we can add it in here, and create a useful resource for security professionals worldwide!

**If you've enjoyed this event, please consider donating whatever you can spare to buy me pizza, coffee, and help fund future events!** (even £5/$5 will make a huge difference, and it only takes a few seconds).

PayPal.Me

**https://paypal.me/KDMentoring**

## OPERATION CHIMERA - VULNERABILITY MANAGEMENT

**This document is not 100% finished and will be updated throughout Chimera. Thank you for your patience.**

This module is designed to give a look into the world of Vulnerability Management. It is aimed at individuals who are moving in to Cyber, so the material is aimed at an entry-level student. We strongly encourage further reading using the provided sources and any that you find yourself. Want to talk to other hackers about this specific module? Join the discussion in the "vuln-mgmt-module" channel within the "Operation Chimera" category in the SBT Discord server. There is also a Chimera mega-thread on Reddit. Please make use of this to ask questions and talk to other participants!

## WHAT IS VULNERABILITY MANAGEMENT?

Vulnerability Management is the process of remediating vulnerabilities in software to reduce the risk and impact of cyber-attacks. The process includes the following steps:

- **Identification –** Using vulnerability scanners, manual techniques, and asset discovery methods to identify and record systems, along with any security issues they have.
- **Reporting –** Reporting these issues to appropriate stakeholders (such as system owners) so they can be addressed, and eventually resolved.
- **Remediation –** Having the security issues fixed by the system owner or technical owner.
- **Reassessment –** Scanning or manually checking to ensure the security issues have been successfully fixed.

## WHY IS IT USEFUL?

Vulnerabilities are announced constantly, and most of them affect software that is used on a mass scale. Examples include security flaws in Google Chrome, Windows operating system, and other programs such as Adobe Flash Player, and Adobe Shockwave Player. Being able to keep on top of these issues, and make sure products are patched as soon as possible (usually after testing, to ensure there's no unwanted effects from the patch), means that hackers have less time to attempt exploitation. By ensuring internet-facing systems are secure, it's harder for attackers to get in, and by ensuring internal systems are secure, it's harder for attackers to move around, and complete the actions they want to.

## ASSOCIATED ROLES

The below roles generally contain work that includes aspects of Vulnerability Management:

- **Threat Intelligence Analyst**
  Receiving and reporting on intelligence about newly released vulnerabilities, or vulnerabilities that are actively being exploited in the wild, and by which actors.
- **Vulnerability Analyst**
  Identifying, reporting on, and helping to remediate vulnerable assets to harden the estate and reduce risk from cyber-attacks.
- **Incident Responder**
  Knowledge about vulnerabilities, and how to deal with compromises as a result of successful exploitation.
- **Penetration Tester / Red Teamer**
  Knowing how to identify and scan for vulnerabilities and security flaws is key to this role, allowing you to exploit systems and gain access.

## A DAY IN THE LIFE

I'm responsible for ensuring that approximately 3000 endpoints around the world, including servers, clients, networking equipment, IoT, and mobile devices all stay secure. Sounds like fun, right? *Hmm… yeah.*
I'm kidding – I **love** it. In this role, you get a perfect mix of Red and Blue team. You get to hack stuff, but then get it fixed so some nasty threat actor can't do the same.

Over the past year we've had some pretty nasty vulnerabilities. Arguably the most important has been CVE-2019-0708, a zero-day vulnerability in Windows Remote Desktop Services (RDP). This remote code execution vulnerability could allow a hacker to bypass any authentication over RDP and connect directly to a system over the internet without valid credentials. This was BIG. I read some of the first public announcements on Twitter, and immediately set up some Tweetdeck columns to monitor for keywords such as "CVE-2019-0708", "RDP", "zeroday". I turned to the other analysts in the Vulnerability

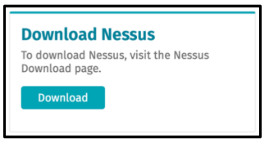
Management team and said, "guys, take a look at this", and sent them the details. At this point we genuinely laughed, because we knew this would be huge and we'd be *very* busy. I send an email to the wider Security Operations team providing everyone with a situational awareness update and inform the SOC Manger and SecOps Director. Next we draft up an email notification that is going to essentially every department we have, informing them to apply the Microsoft-issued security patches for everything back to Windows XP (yeah, it was so bad Microsoft brought out patches for end-of-life systems). Our email also mentioned that if anything didn't need RDP open, disable the service ASAP. We got our global DMZs patched the same day, and people began queueing patches for internal assets. Over the next few days we ran vulnerability scans against our internet-facing systems to see if RDP was still present anywhere. Other OSINT sources like Shodan helped us check for exposure. Throughout the week we also had Threat Intelligence analysts looking to see if any Public Exploit Code (also known as Proof of Concept code) or exploits were detected in the wild. I also shared any intelligence I discovered myself via a government-owned information sharing platform.

Although events like this aren't common, there's always work to do. Researching publicly announced vulnerabilities, checking them against the estate, getting systems patched, vulnerability scanning, manually checking and exploiting vulnerabilities, threat simulation attacks, analyzing reports generated by OSINT sources such as Shodan and ShadowServer, communicating with teams in other organizations, helping investigate SIEM alerts regarding vulnerability/system exploitation, web-app pentesting our sites, and much more.

## VULNERABILITY SCANNING

In this section, we'll be teaching you how to use Nessus Essentials, a free version of the enterprise-grade vulnerability scanning platform, Nessus. Please remember you may only use this version for personal projects at home, and using it in a business environment is a breach of Tenable's licensing. This tool is great to use during certification exams (*if it's permitted! Check before using it*), and pentesting systems on platforms such as HackTheBox.

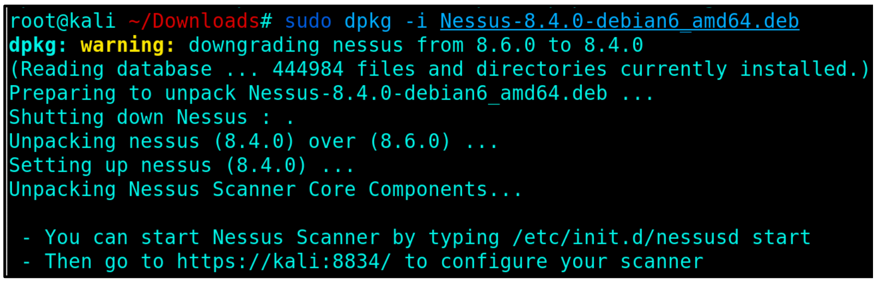
**You will want to do the next steps whilst in a Kali VM.**
Visit https://www.tenable.com/products/nessus/nessus-essentials and register for an activation code. Once you're taken to the next page, on the right-hand side you'll see this box, where you can download Nessus:



Download Nessus

To download Nessus, visit the Nessus Download page.

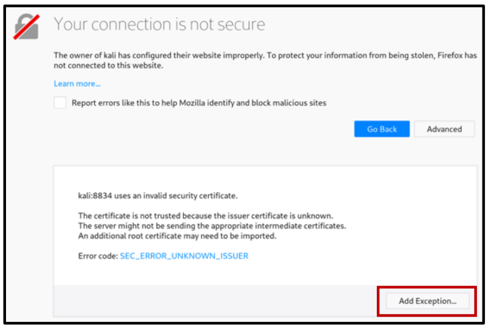
If you can't find that box, then visit https://www.tenable.com/downloads/nessus. Navigate to the directory you downloaded the file to (Most likely /root/Downloads) and use the following command to install Nessus from the .deb file:
sudo dpkg -i (Nessus .deb file name)
(run as super user) (Debian package tool) (install) (Nessus package)



```
root@kali ~/Downloads# sudo dpkg -i Nessus-8.4.0-debian6_amd64.deb
dpkg: warning: downgrading nessus from 8.6.0 to 8.4.0
(Reading database ... 444984 files and directories currently installed.)
Preparing to unpack Nessus-8.4.0-debian6_amd64.deb ...
Shutting down Nessus : .
Unpacking nessus (8.4.0) over (8.6.0) ...
Setting up nessus (8.4.0) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner
```

Next you'll need to run the Nessus service (also referred to as the Nessus Daemon), which starts everything up. Run service nessusd start, and once the service is running, go to your browser, and visit https://kali:8834/ - this is the local web GUI for Nessus. If you get an error similar to the below, you need to add an exception so you can view the site. Click "Add Exception" in the bottom right corner:



Your connection is not secure

The owner of kali has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

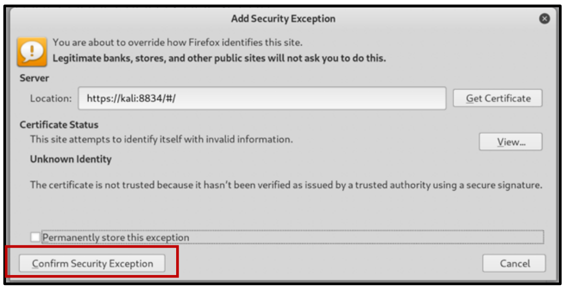
Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

kali:8834 uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

Error code: SEC_ERROR_UNKNOWN_ISSUER



Add Security Exception

You are about to override how Firefox identifies this site.
**Legitimate banks, stores, and other public sites will not ask you to do this.**

**Server**

Location: https://kali:8834/#/

**Certificate Status**

This site attempts to identify itself with invalid information.

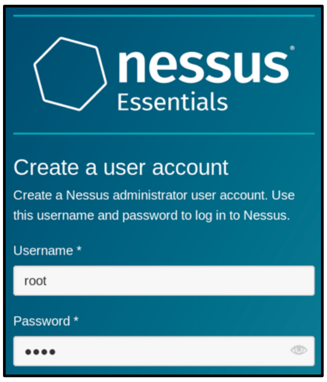
**Unknown Identity**

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

□ Permanently store this exception

(If you've previously used Nessus, you may get an error stating you have a corrupt database. To fix this, you need to kill the service (use service nessud stop), remove all Nessus files, download the latest version, and install it again. To delete all files for a clean re-install, use the command:
rm -rf /opt/nessus (recursively remove everything) (in opt/nessus).)

You should now be asked what product you want to use, select Nessus Essentials. You can either register here, or if you did it earlier, skip this step to submit your activation code which should've been emailed to you. Finally, you'll be asked to create a username and password to access Nessus locally within your VM. This form should inherit you Kali account details (in my case, 'root' and 'toor') however you are able to change them to anything you wish.



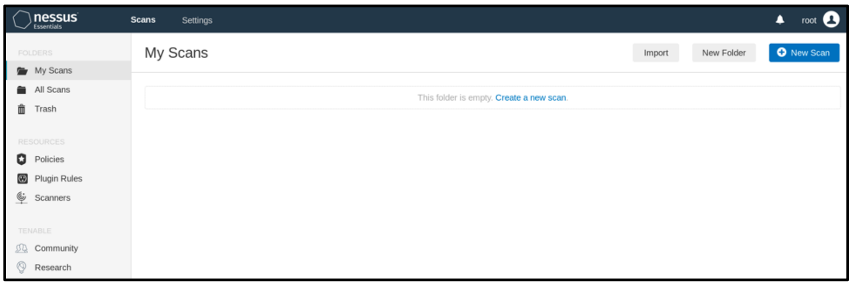
Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *
root

Password *
••••

Now Nessus will download plugins and other crucial files that it needs to function properly, so let it complete. Once that's done, you'll be presented with the Nessus dashboard. From here we can launch scans, create policies, review plugins, and more. For the scope of this module, we will only be looking briefly at plugins, and focusing on using a premade scan template. We strongly encourage you to explore Nessus, as it is widely used in industry and hands-on experience is a great thing to have.



This folder is empty. Create a new scan.

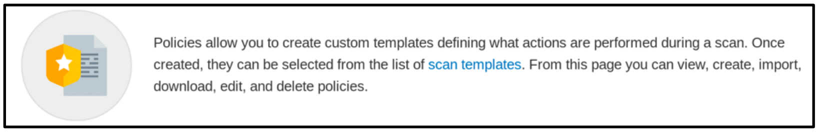
On the left-hand side we have a navigation menu, the following sections are interesting to us:

1. **My Scans** – Any scans that have been conducted by the currently signed-in user. This includes completed, scheduled, pending, and failed scans.

2. **All Scans** – Any scans that have been conducted by any users within an organisation. This includes completed, scheduled, pending, and failed scans.

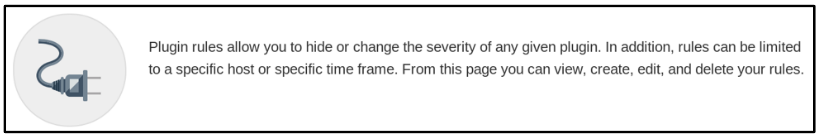
3. **Trash** – Once you've got a scan template, you can send it to the Trash, so that it is no longer in the "My Scans" or "All Scans" tabs.

4. **Policies** – Scans are conducted using a target and a policy, which is a list of settings and plugins that you use. Different plugins will identify and test different things.



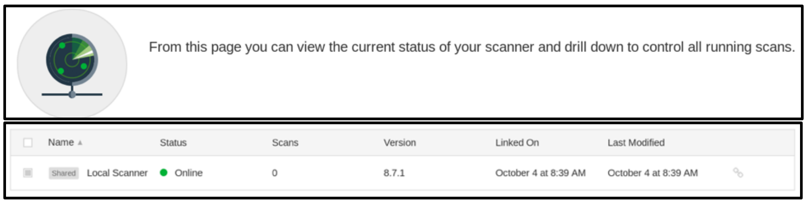
Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.

5. **Plugin Rules** – Plugins are the part of Nessus that actually conduct the scanning and enumeration. Using different ones will provide different results, so this is where you can fine tune the scan to look for specific security issues.



Plugin rules allow you to hide or change the severity of any given plugin. In addition, rules can be limited to a specific host or specific time frame. From this page you can view, create, edit, and delete your rules.

6. **Scanners** – Scanners are different hosts that are able to perform enumeration. This is useful if there are multiple V-LANs or physical networks that need to be scanned, and the hosts can't communicate directly. In our case, we only have one, the local scanner running in our VM.

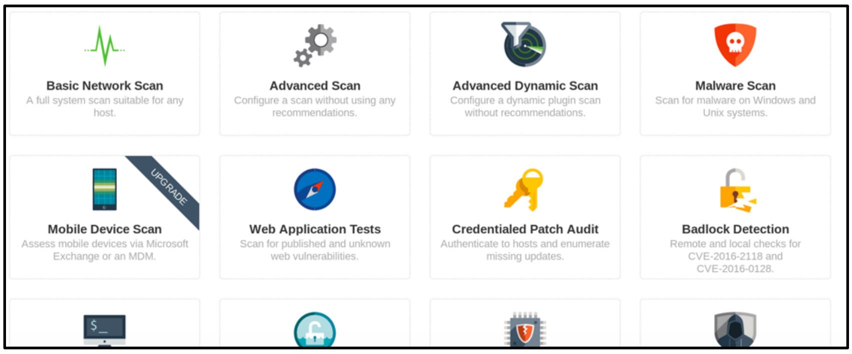


From this page you can view the current status of your scanner and drill down to control all running scans.

| Name | Status | Scans | Version | Linked On | Last Modified |
|---|---|---|---|---|---|
| Shared Local Scanner | ● Online | 0 | 8.7.1 | October 4 at 8:39 AM | October 4 at 8:39 AM |

Next we're going to perform a simple scan of own our machine to demonstrate how scans work, and what the results look like. You can use the following steps to scan any other hosts on your network (provided you have permission to do so).

1) Head over to the Policies tab on the left, and click "Scan Templates" in the description text (as seen above). We will now be able to choose from a list of pre-defined templates that can be used for specific actions, such as vulnerability scanning, and host discovery. We will be using the Basic Network Scan for this example.



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

**Advanced Scan**
Configure a scan without using any recommendations.

**Advanced Dynamic Scan**
Configure a dynamic plugin scan without recommendations.

**Malware Scan**
Scan for malware on Windows and Unix systems.

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

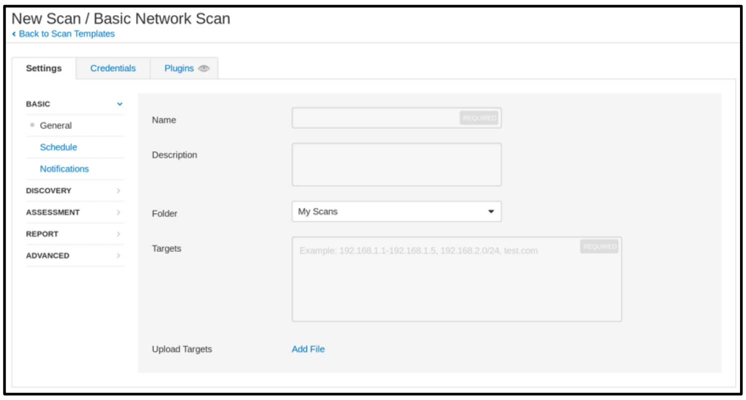
**Web Application Tests**
Scan for published and unknown web vulnerabilities.

**Credentialed Patch Audit**
Authenticate to hosts and enumerate missing updates.

**Badlock Detection**
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

2) After clicking on our scan template, we'll be able to customize the settings for this specific scan. Take a look at all of the settings you can change, as well as the Credentials tab, and Plugins tab. What are the credentials used for? They allow the scanner to log into the system, and collect much more valuable information, as opposed to being locked out and only being able to collect surface information. Companies will usually run credentialed scans internally to get the

most valuable information, whereas non-credentialed scans give an unauthenticated attacker’s view of the network.



Name: REQUIRED

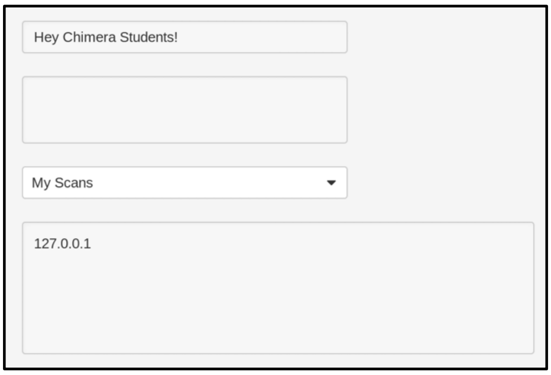
Description:

Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com REQUIRED

Upload Targets: Add File

For this example, you can name the scan anything you like, and we want to enter the localhost (127.0.0.1) as the target.

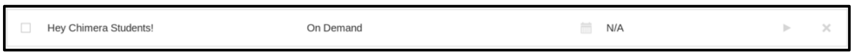


Hey Chimera Students!

My Scans

127.0.0.1

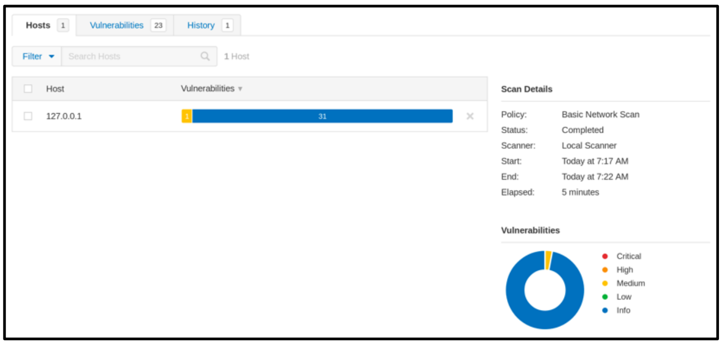
3) Click Save in the bottom left-hand corner, and you’ll be taken to the “My Scans” page. From here, we can launch our scan by pressing on the play icon to the right. Once clicked, the scan will get to work. Once it’s finished, a tick will appear, and we’ll be able to take a look at the results.



□ Hey Chimera Students! On Demand N/A

4) This is the results pane and provides us with all of the information the scan collected. On the left we have a list of hosts scanned, along with a summary of any vulnerabilities discovered. This would be full of different hosts if we were scanning an entire network and is arranged by criticality of vulnerability by default. On the right we have the Scan

Details, and below it we have a donut chart for the security issues identified. Click on the Vulnerabilities tab to see exactly what the scanner identified.



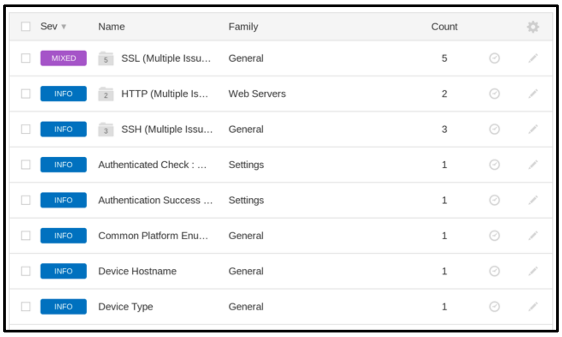
| Host | Vulnerabilities |
|---|---|
| 127.0.0.1 | 1 31 |

Scan Details

Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 7:17 AM
End: Today at 7:22 AM
Elapsed: 5 minutes

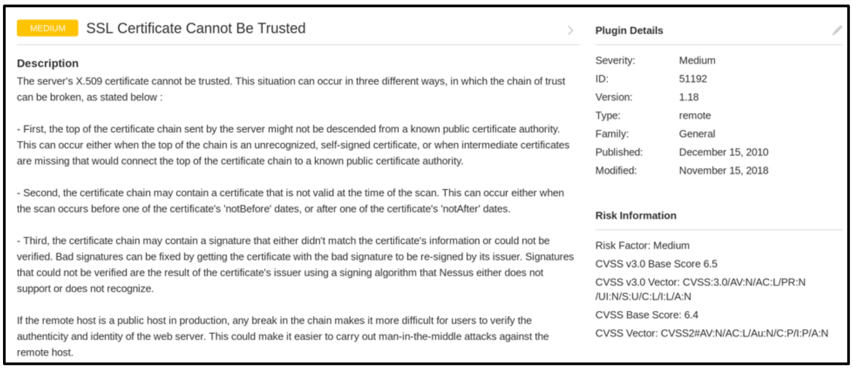
Vulnerabilities

5) In this example, we don't expect to see any major vulnerabilities. Here can see there some issues with SSL (this is because of the security exception we had to allow earlier when trying to open Nessus), and some informational issues. You can click on any of these rows in order to get more information and see how to fix them. Click on the SSL issues, then click on the medium-rated SSL issue.



| Sev | Name | Family | Count |
|---|---|---|---|
| MIXED | 5 SSL (Multiple Issu... | General | 5 |
| INFO | 2 HTTP (Multiple Is... | Web Servers | 2 |
| INFO | 3 SSH (Multiple Issu... | General | 3 |
| INFO | Authenticated Check : ... | Settings | 1 |
| INFO | Authentication Success ... | Settings | 1 |
| INFO | Common Platform Enu... | General | 1 |
| INFO | Device Hostname | General | 1 |
| INFO | Device Type | General | 1 |

6) This page shows us a description of the issue, the plugin that was used to detect it, and risk information. Below the description is a solution for how to address the issue. When contacting system owners after a scan, it is good practice to attach an export of the scan as a PDF, but also provide a concise summary in an email with a quick overview of the hosts, any issues, and how to fix them.



MEDIUM SSL Certificate Cannot Be Trusted

**Description**

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

**Plugin Details**

| | |
|---|---|
| Severity: | Medium |
| ID: | 51192 |
| Version: | 1.18 |
| Type: | remote |
| Family: | General |
| Published: | December 15, 2010 |
| Modified: | November 15, 2018 |

**Risk Information**

Risk Factor: Medium

CVSS v3.0 Base Score 6.5

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS Base Score: 6.4

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

Of course, Nessus is one of many different vulnerability scanners. Others include WPScan for scanning WordPress sites, OpenVAS for vulnerability scanning and vulnerability management, Nikto for scanning webservers, Nmap Scripting Engine for network scanning, and many more. We strongly advise that you become familiar with the other scanners mentioned if you are interested in a Vulnerability Management or Penetration Tester role.

## MODULE CHALLENGE

If you think you're ready for the module challenge, head over to the website and click on the 'Challenge Brief' under the Threat Intelligence module! Good luck.