INTRO TO ETHICAL HACKING

MIS 5211.701

Week 5

Site:

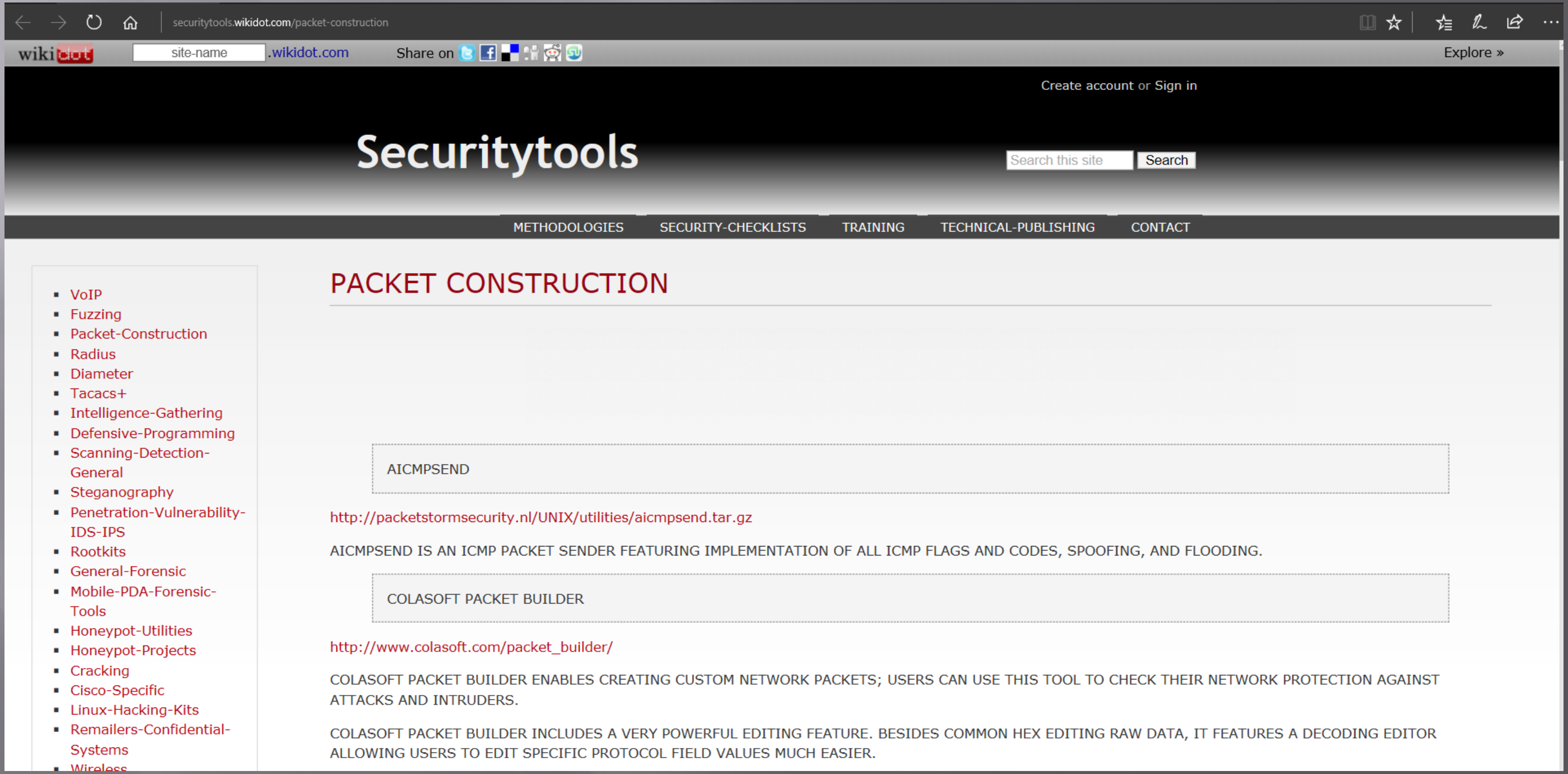
http://community.mis.temple.edu/mis5211sec701fall2018/

Tonight's Plan

- Odds and Ends
- Nessus
- Next Week

Packet Construction Tools

- http://securitytools.wikidot.com/packet-construction



PACKET CONSTRUCTION

AICMPSEND

http://packetstormsecurity.nl/UNIX/utilities/aicmpsend.tar.gz

AICMPSEND IS AN ICMP PACKET SENDER FEATURING IMPLEMENTATION OF ALL ICMP FLAGS AND CODES, SPOOFING, AND FLOODING.

COLASOFT PACKET BUILDER

http://www.colasoft.com/packet_builder/

COLASOFT PACKET BUILDER ENABLES CREATING CUSTOM NETWORK PACKETS; USERS CAN USE THIS TOOL TO CHECK THEIR NETWORK PROTECTION AGAINST ATTACKS AND INTRUDERS.

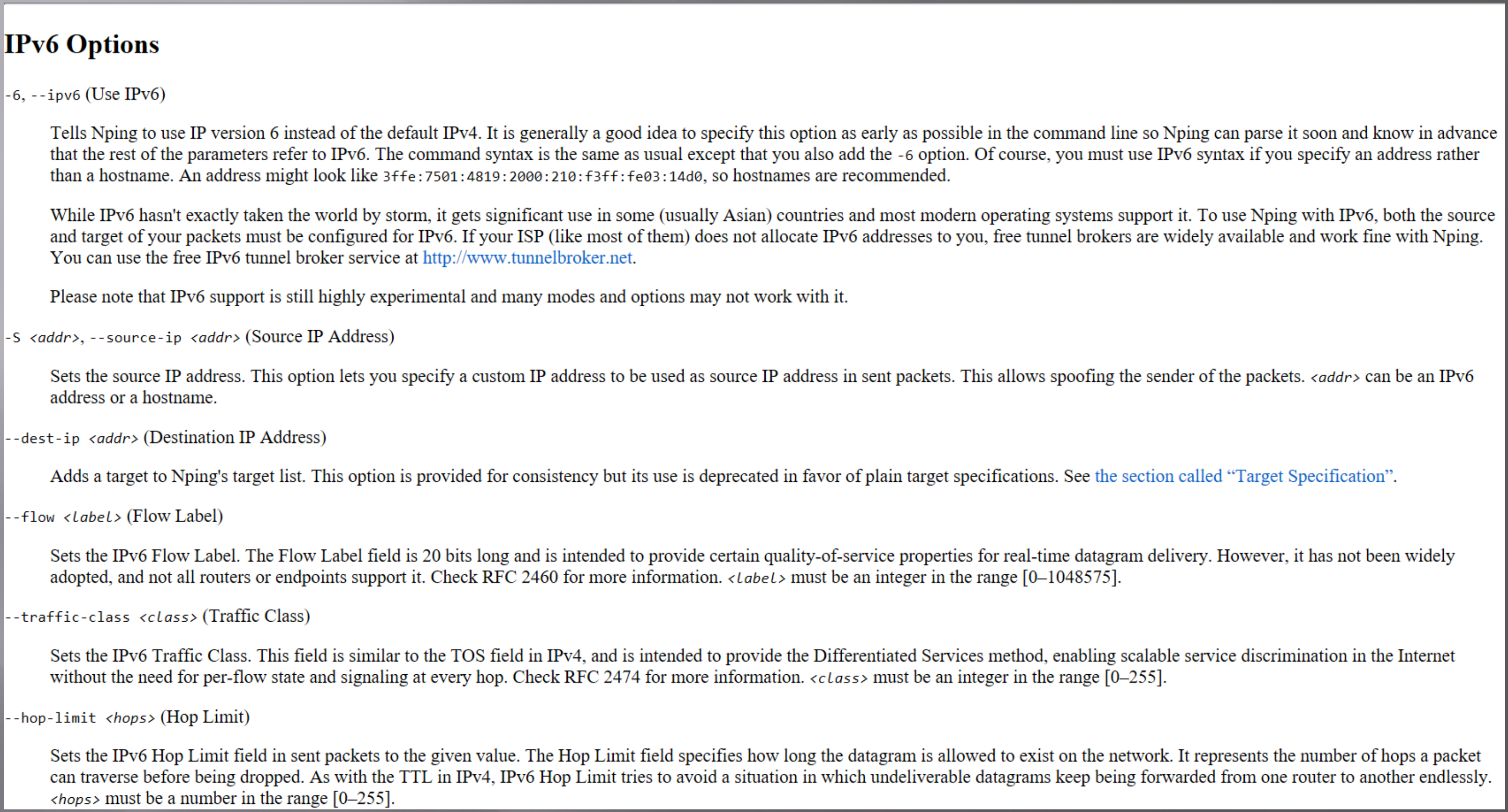
COLASOFT PACKET BUILDER INCLUDES A VERY POWERFUL EDITING FEATURE. BESIDES COMMON HEX EDITING RAW DATA, IT FEATURES A DECODING EDITOR ALLOWING USERS TO EDIT SPECIFIC PROTOCOL FIELD VALUES MUCH EASIER.

IPv6 Scanning

- IPv6 fingerprinting
- Nmap has a similar but separate OS detection engine specialized for IPv6
  - Use the -6 and –O options

IPv6 Scanning

- Nping – Comes with Nmap
- https://nmap.org/book/nping-man-ip6-options.html
- From the site
  - Nping is an open-source tool for network packet generation, response analysis and response time measurement. Nping allows users to generate network packets of a wide range of protocols, letting them tune virtually any field of the protocol headers. While Nping can be used as a simple ping utility to detect active hosts, it can also be used as a raw packet generator for network stack stress tests, ARP poisoning, Denial of Service attacks, route tracing, and other purposes.



IPv6 Options

`-6`, `--ipv6` (Use IPv6)

Tells Nping to use IP version 6 instead of the default IPv4. It is generally a good idea to specify this option as early as possible in the command line so Nping can parse it soon and know in advance that the rest of the parameters refer to IPv6. The command syntax is the same as usual except that you also add the `-6` option. Of course, you must use IPv6 syntax if you specify an address rather than a hostname. An address might look like `3ffe:7501:4819:2000:210:f3ff:fe03:14d0`, so hostnames are recommended.

While IPv6 hasn't exactly taken the world by storm, it gets significant use in some (usually Asian) countries and most modern operating systems support it. To use Nping with IPv6, both the source and target of your packets must be configured for IPv6. If your ISP (like most of them) does not allocate IPv6 addresses to you, free tunnel brokers are widely available and work fine with Nping. You can use the free IPv6 tunnel broker service at http://www.tunnelbroker.net.

Please note that IPv6 support is still highly experimental and many modes and options may not work with it.

`-S` *`<addr>`*, `--source-ip` *`<addr>`* (Source IP Address)

Sets the source IP address. This option lets you specify a custom IP address to be used as source IP address in sent packets. This allows spoofing the sender of the packets. *`<addr>`* can be an IPv6 address or a hostname.

`--dest-ip` *`<addr>`* (Destination IP Address)

Adds a target to Nping's target list. This option is provided for consistency but its use is deprecated in favor of plain target specifications. See the section called “Target Specification”.

`--flow` *`<label>`* (Flow Label)

Sets the IPv6 Flow Label. The Flow Label field is 20 bits long and is intended to provide certain quality-of-service properties for real-time datagram delivery. However, it has not been widely adopted, and not all routers or endpoints support it. Check RFC 2460 for more information. *`<label>`* must be an integer in the range [0–1048575].

`--traffic-class` *`<class>`* (Traffic Class)

Sets the IPv6 Traffic Class. This field is similar to the TOS field in IPv4, and is intended to provide the Differentiated Services method, enabling scalable service discrimination in the Internet without the need for per-flow state and signaling at every hop. Check RFC 2474 for more information. *`<class>`* must be an integer in the range [0–255].

`--hop-limit` *`<hops>`* (Hop Limit)

Sets the IPv6 Hop Limit field in sent packets to the given value. The Hop Limit field specifies how long the datagram is allowed to exist on the network. It represents the number of hops a packet can traverse before being dropped. As with the TTL in IPv4, IPv6 Hop Limit tries to avoid a situation in which undeliverable datagrams keep being forwarded from one router to another endlessly. *`<hops>`* must be a number in the range [0–255].

Nessus

- Started in 1998 as an open source security scanning tool
- Changed to a close sourced tool in 2005, but has remained “free” for personal use.
- Surveys by sectools.org indicate Nessus remains the most popular vulnerability scanners
- Not installed with Kali

The Nessus Server

- Four basic parts to the Nessus server:
  - Nessus-core
  - Nessus-libraries
  - Libnasl
  - Nessus-plugins

Plugins

- Plugins are the scripts that perform the vulnerability tests.
- NASL – This is the Nessus Attack Scripting Language which can be used to write your own plugins.

Defining Targets

- Hosts
  - Server.domain.edu
  - 172.21.1.2
- Subnet
  - 192.168.100.0
- Address range
  - 192.168.1.1-192.168.1.10

Vulnerability Scanning

- Scanning methods:
  - Safe
  - Destructive
- Service recognition – Will determine what service is actually running on a particular port.
- Handle multiple services – Will test a service if it appears on more then one port.
- Will test multiple systems at the same time.

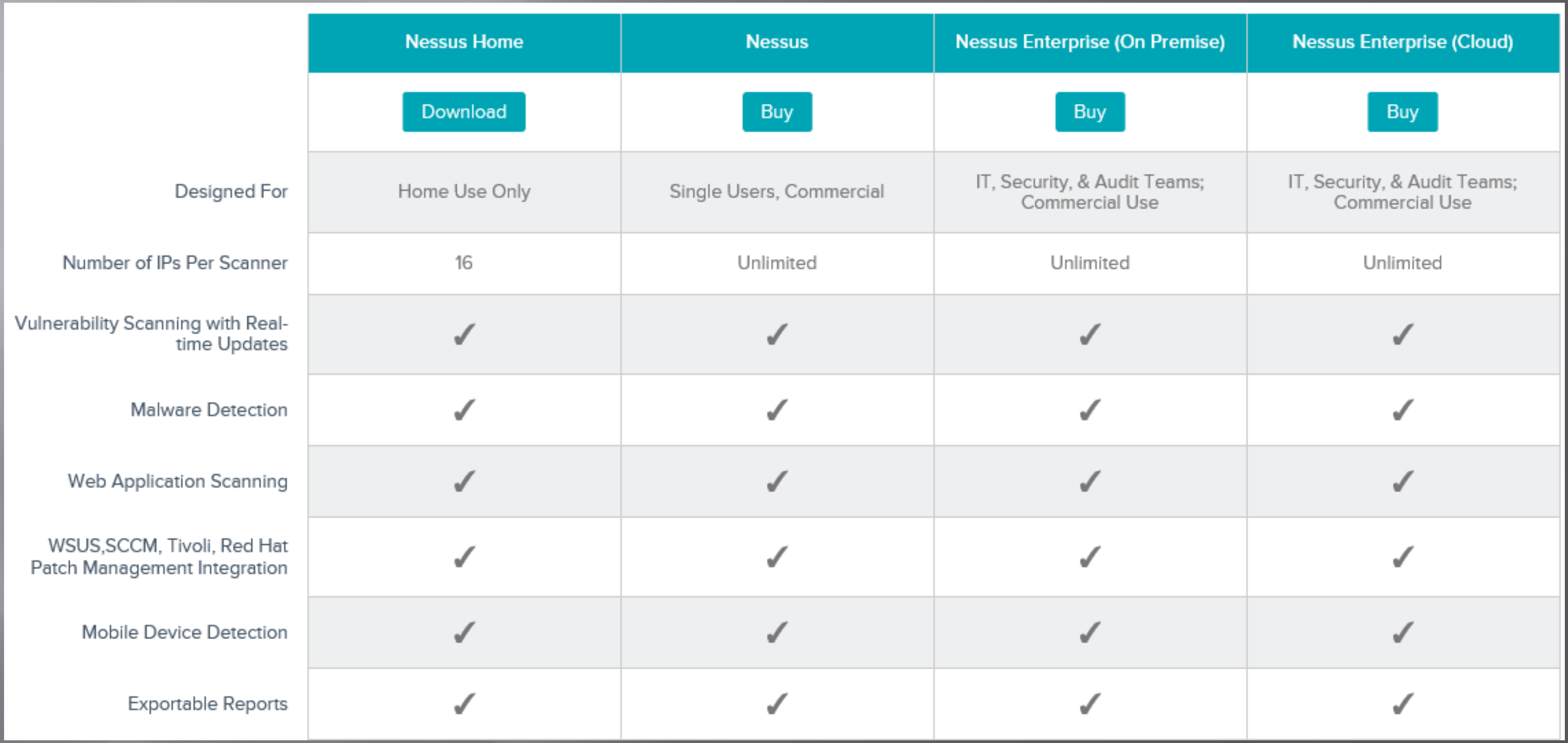
Viewing Reports

- Nessus will indicate the threat level for services or vulnerabilities it detects:
  - Critical
  - High
  - Medium
  - Low
  - Informational
- Description of vulnerability
- Risk factor
- CVE number

Common Vulnerabilities and Exposures

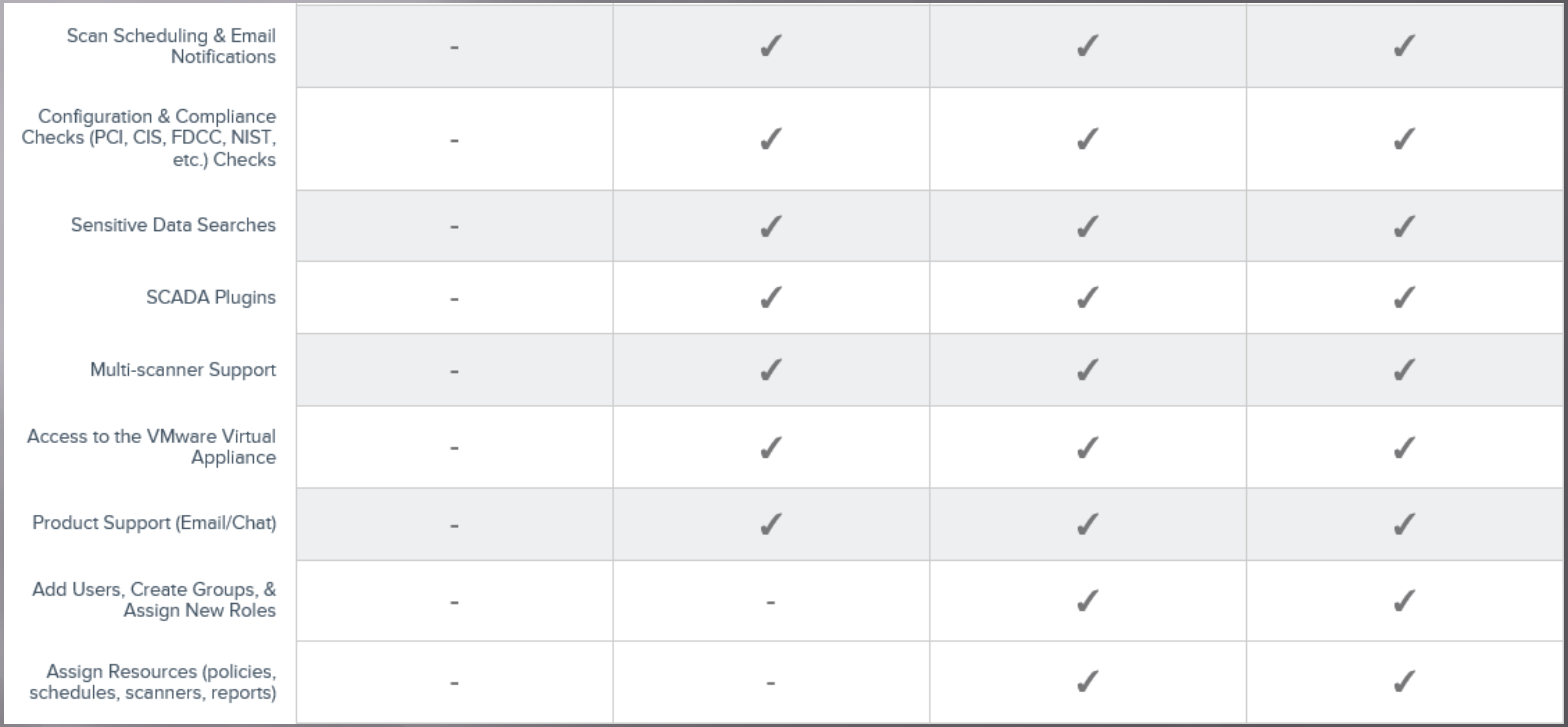
- CVE created by http://www.cve.mitre.org/
  - Attempting to standardize the names for vulnerabilities.
- CVE search engine at http://icat.nist.gov/

Options



	Nessus Home	Nessus	Nessus Enterprise (On Premise)	Nessus Enterprise (Cloud)
	Download	Buy	Buy	Buy
Designed For	Home Use Only	Single Users, Commercial	IT, Security, & Audit Teams; Commercial Use	IT, Security, & Audit Teams; Commercial Use
Number of IPs Per Scanner	16	Unlimited	Unlimited	Unlimited
Vulnerability Scanning with Real-time Updates	✓	✓	✓	✓
Malware Detection	✓	✓	✓	✓
Web Application Scanning	✓	✓	✓	✓
WSUS,SCCM, Tivoli, Red Hat Patch Management Integration	✓	✓	✓	✓
Mobile Device Detection	✓	✓	✓	✓
Exportable Reports	✓	✓	✓	✓

Options

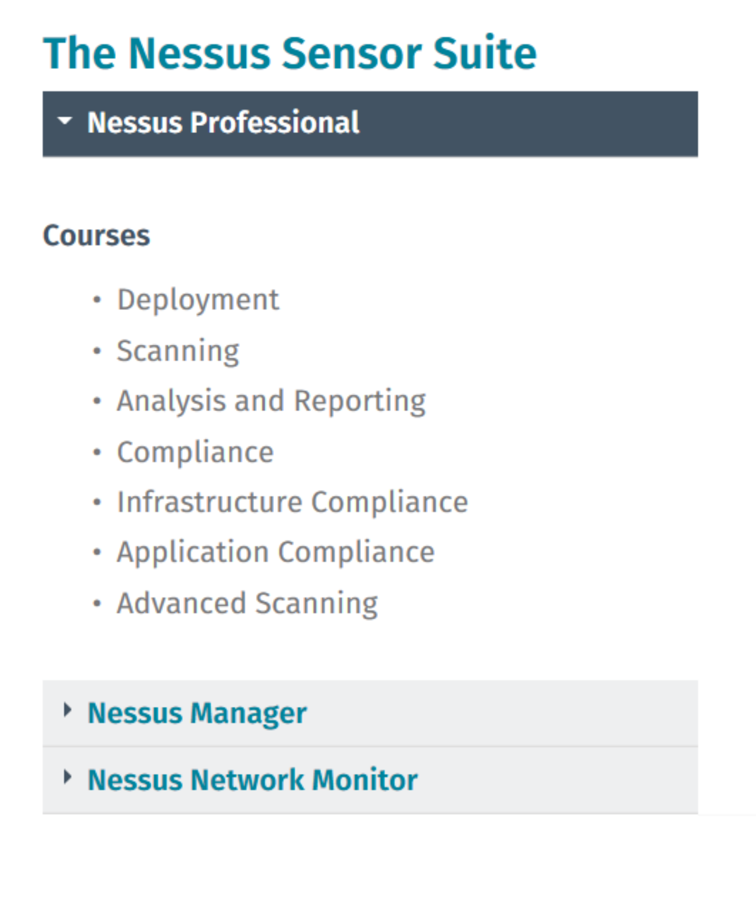


Scan Scheduling & Email Notifications	-	✓	✓	✓
Configuration & Compliance Checks (PCI, CIS, FDCC, NIST, etc.) Checks	-	✓	✓	✓
Sensitive Data Searches	-	✓	✓	✓
SCADA Plugins	-	✓	✓	✓
Multi-scanner Support	-	✓	✓	✓
Access to the VMware Virtual Appliance	-	✓	✓	✓
Product Support (Email/Chat)	-	✓	✓	✓
Add Users, Create Groups, & Assign New Roles	-	-	✓	✓
Assign Resources (policies, schedules, scanners, reports)	-	-	✓	✓

http://www.tenable.com/products/nessus/select-your-operating-system

Free Training

- http://www.tenable.com/education/on-demand-courses



The Nessus Sensor Suite

▾ Nessus Professional

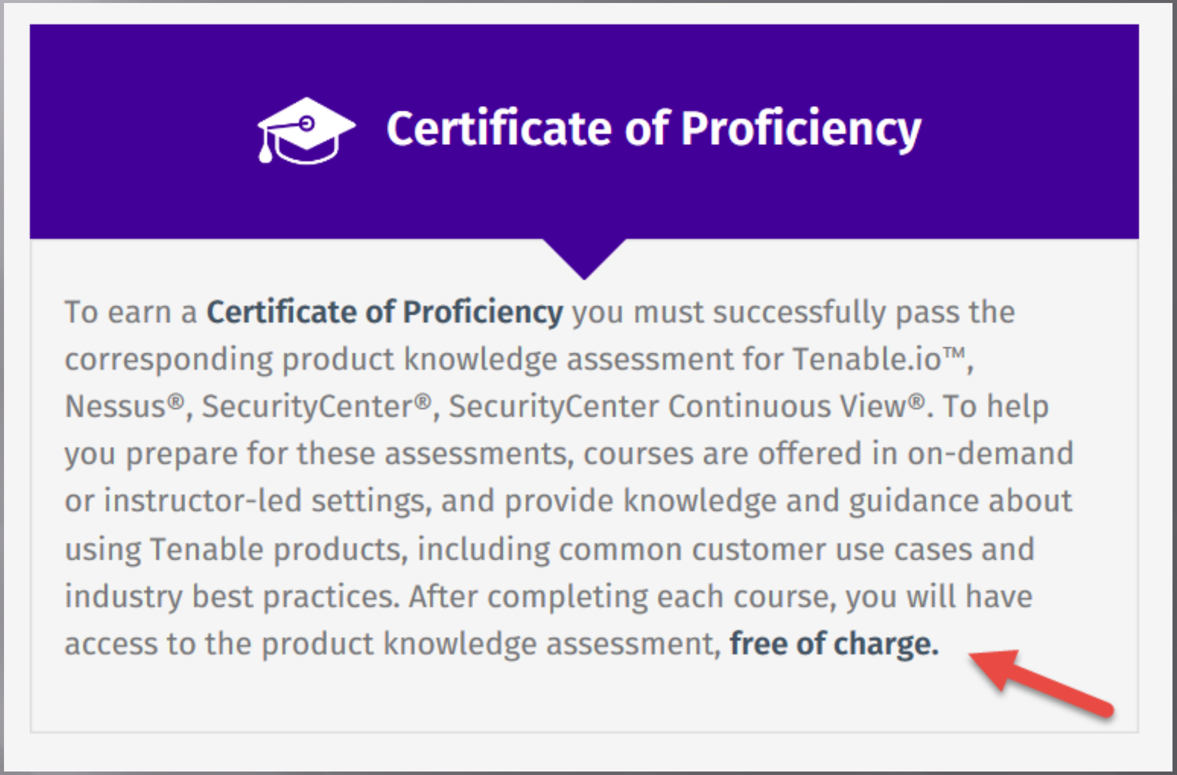
Courses

- Deployment
- Scanning
- Analysis and Reporting
- Compliance
- Infrastructure Compliance
- Application Compliance
- Advanced Scanning

▸ Nessus Manager

▸ Nessus Network Monitor

Certification Options



Certificate of Proficiency

To earn a **Certificate of Proficiency** you must successfully pass the corresponding product knowledge assessment for Tenable.io™, Nessus®, SecurityCenter®, SecurityCenter Continuous View®. To help you prepare for these assessments, courses are offered in on-demand or instructor-led settings, and provide knowledge and guidance about using Tenable products, including common customer use cases and industry best practices. After completing each course, you will have access to the product knowledge assessment, **free of charge.**

http://www.tenable.com/education/certification

Architecture

- Nessus is built on a classic client/server model.
- The server portion may reside on a separate machine, or on the same machine as the client
- The client is the interface that you will interact with to execute scans

Getting Nessus

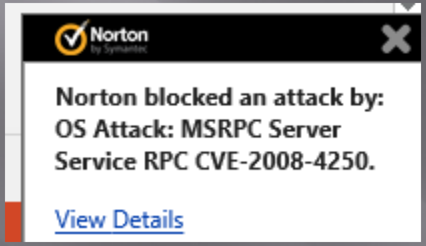
- Download from Tenable Security
  - http://www.tenable.com/products/nessus/select-your-operating-system
  - Before installing, go to registration page and get the activation code
  - http://www.tenable.com/products/nessus-home
- Run the MSI package and follow the prompts
- Install will also install PCAP and then take you to the registration page.
- Enter activation code and follow the prompts to get updates and plugins

Documentation

- Documentation for Nessus is available here:
  - http://static.tenable.com/documentation/nessus_4.2_user_guide.pdf
- You will also get a link to this location during the install.

AV and Firewalls

- You will need to turn off Anti-Virus and Firewall in order to get an effective scan or you will see this:

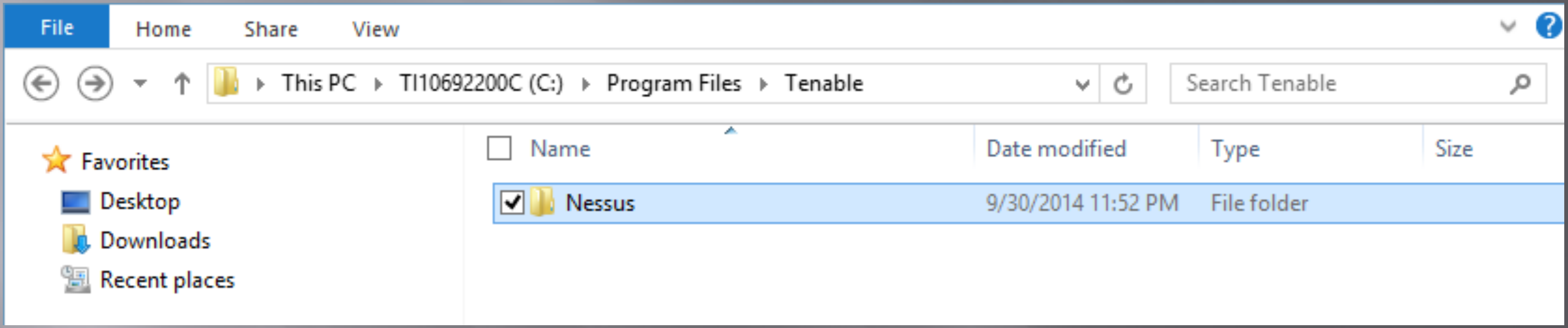


Norton blocked an attack by: OS Attack: MSRPC Server Service RPC CVE-2008-4250.

- Before you do this, disconnect from any and all networks.
- You will likely still get some blocking as AV doesn't like to give up.

Location

- Nessus is installed here:



This PC ▸ TI10692200C (C:) ▸ Program Files ▸ Tenable

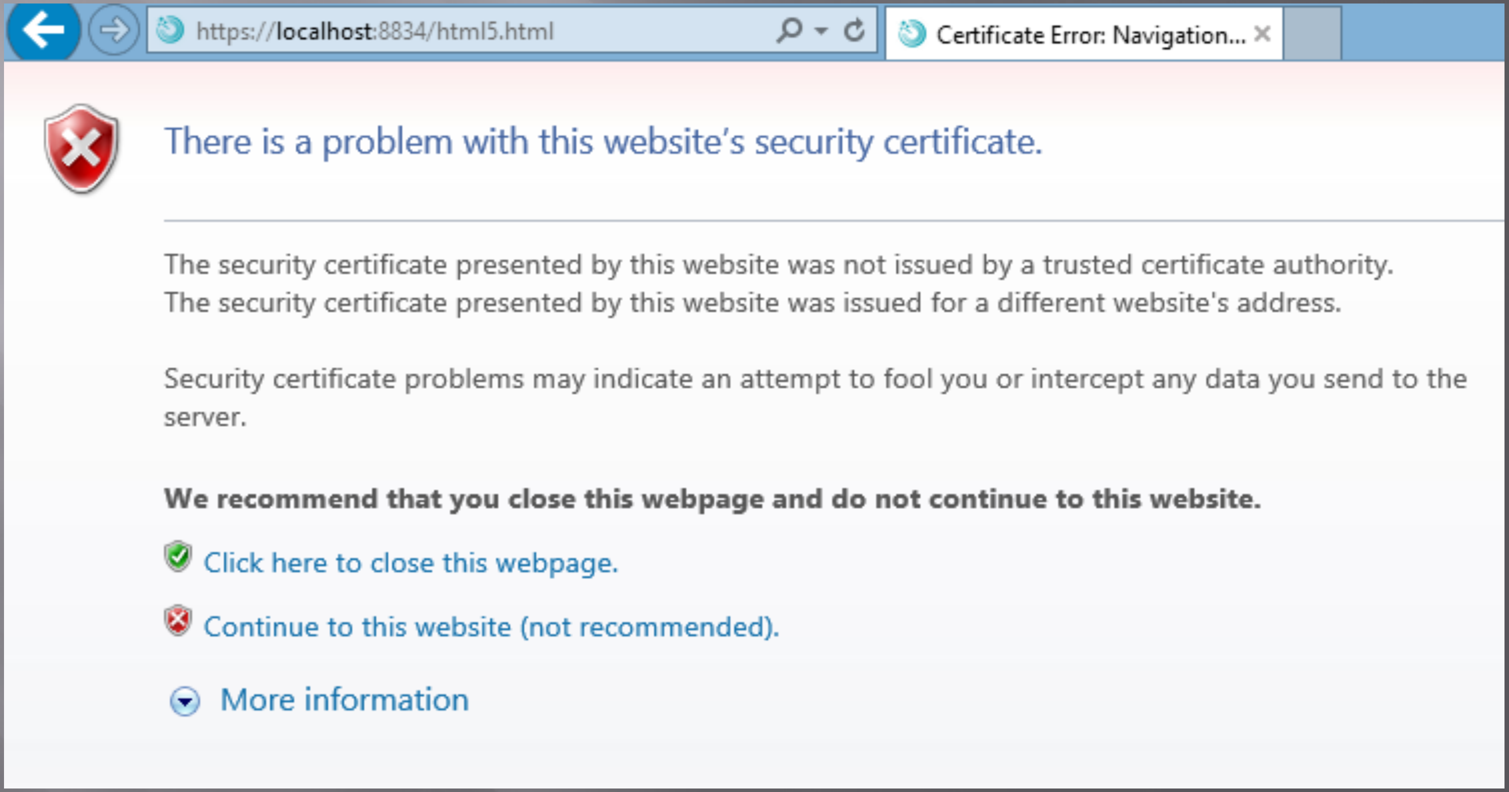
☐ Name	Date modified	Type	Size
☑ Nessus	9/30/2014 11:52 PM	File folder	

Getting Started

- You should end up looking at web page hosted from your machine.
- Book mark the page to save time getting back
- URL will look like this:
  - https://localhost:8834/html5.html

SSL Warning

- When you first go to site, you will need to click on continue to the website.:



https://localhost:8834/html5.html
Certificate Error: Navigation...

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

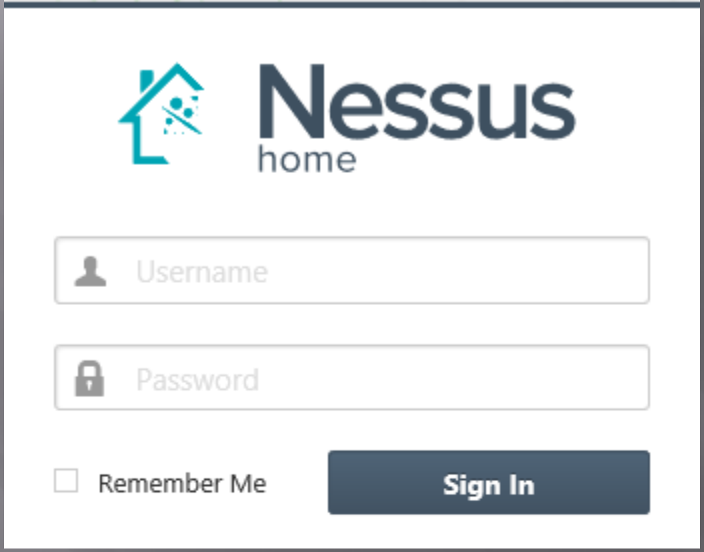
Click here to close this webpage.

Continue to this website (not recommended).

More information

Logging In

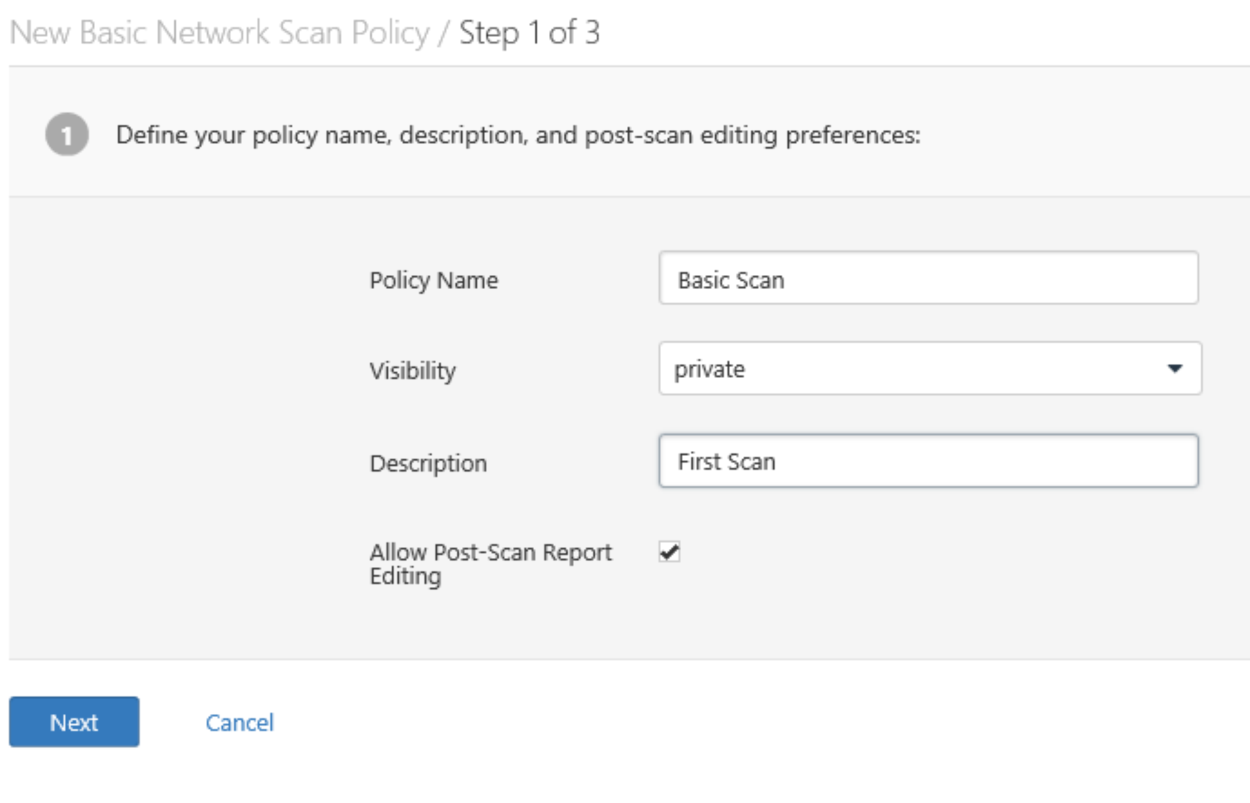
- Start



Nessus home

Policies

- Scans are based on policies, you will need to create that first.



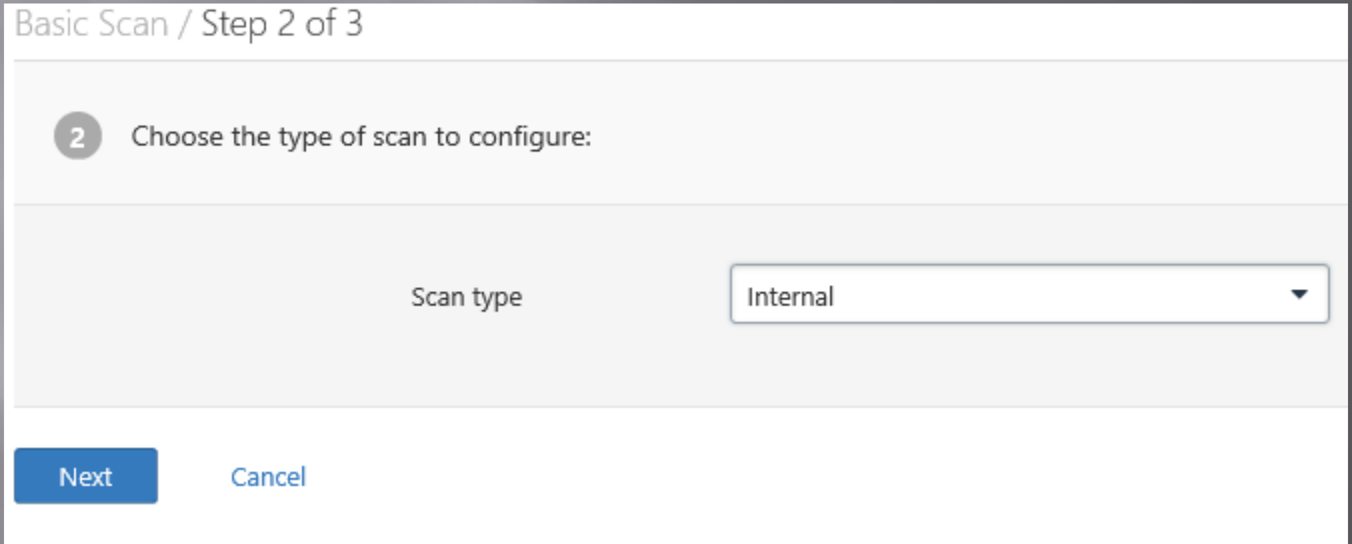
New Basic Network Scan Policy / Step 1 of 3

1 Define your policy name, description, and post-scan editing preferences:

Policy Name	Basic Scan
Visibility	private
Description	First Scan
Allow Post-Scan Report Editing	☑

Policies 2

- Next

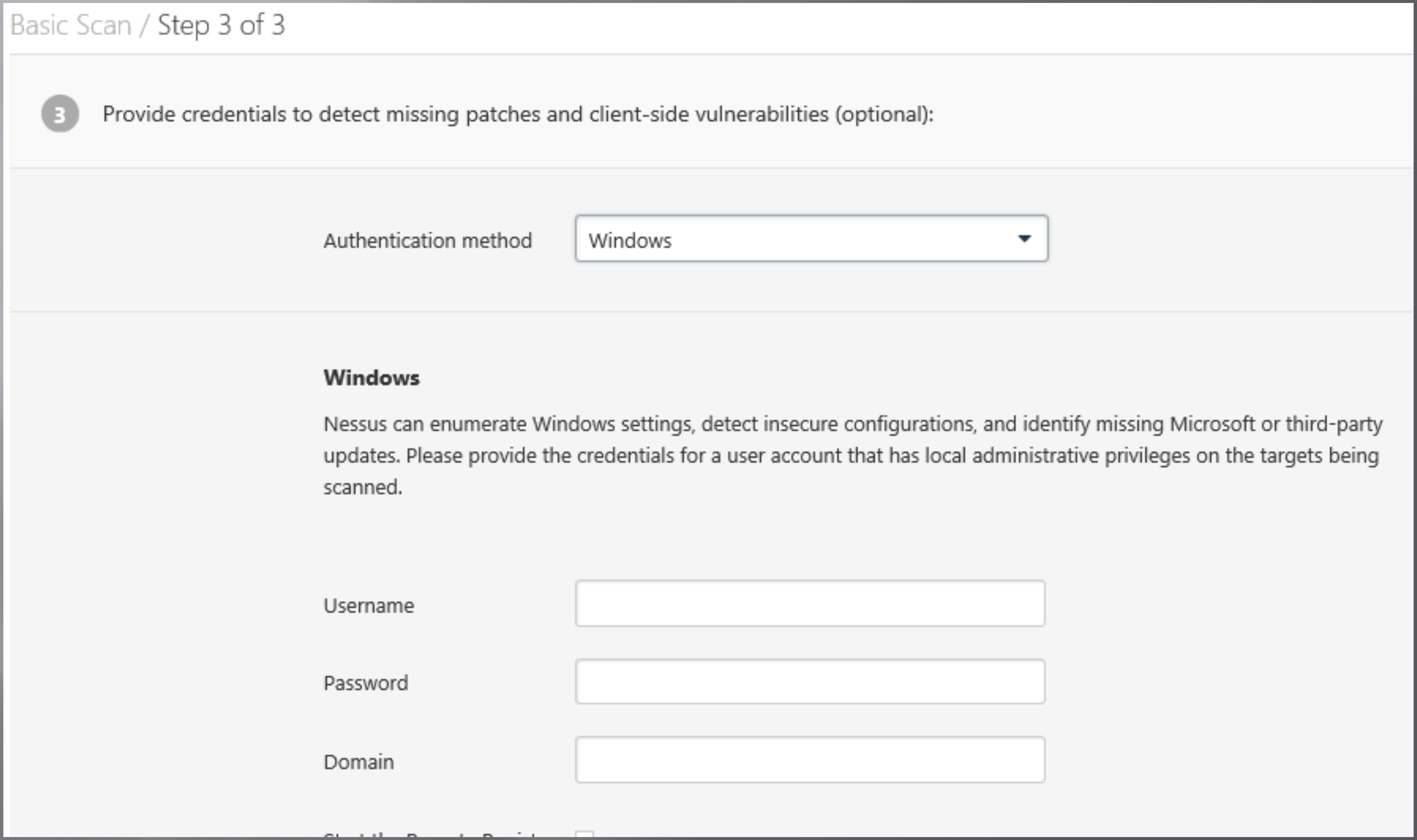


Basic Scan / Step 2 of 3

2 Choose the type of scan to configure:

Scan type: Internal

Policies 3



Basic Scan / Step 3 of 3

3 Provide credentials to detect missing patches and client-side vulnerabilities (optional):

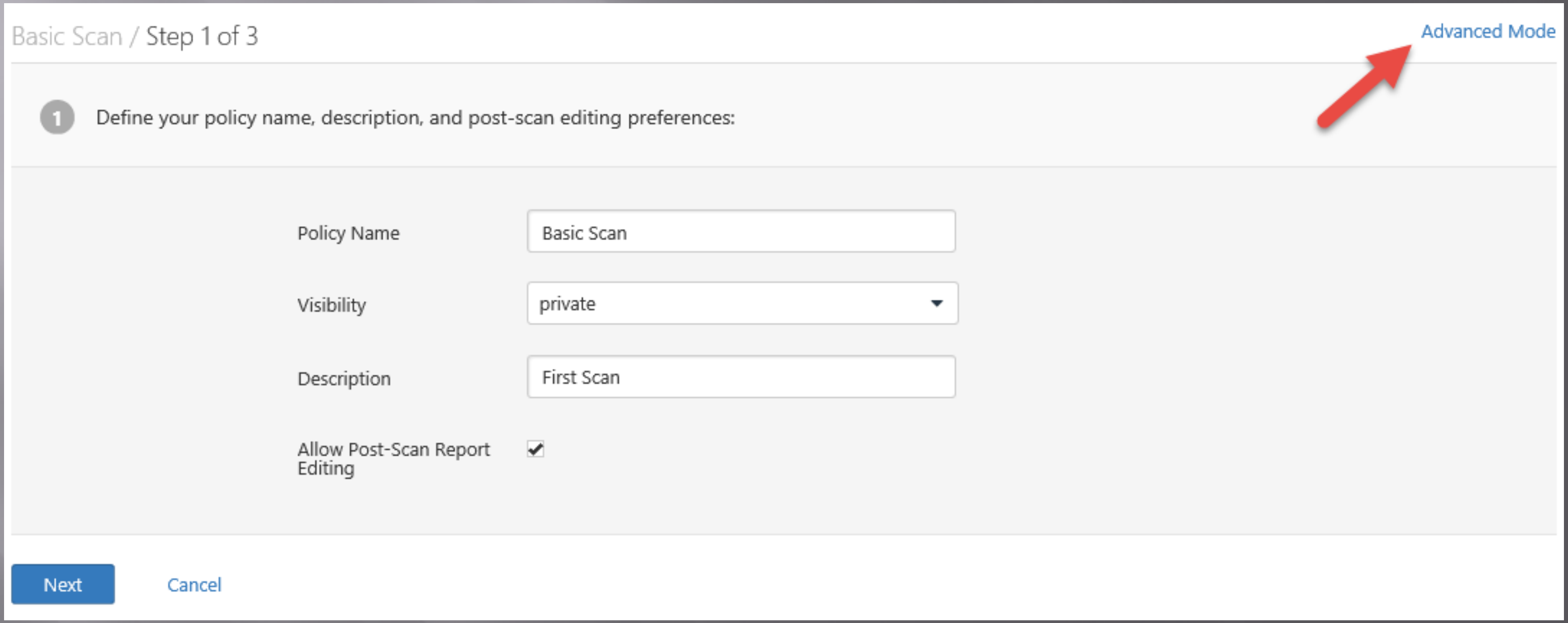
Authentication method: Windows

Windows

Nessus can enumerate Windows settings, detect insecure configurations, and identify missing Microsoft or third-party updates. Please provide the credentials for a user account that has local administrative privileges on the targets being scanned.

Username	
Password	
Domain	

There are many more options



Basic Scan / Step 1 of 3

1 Define your policy name, description, and post-scan editing preferences:

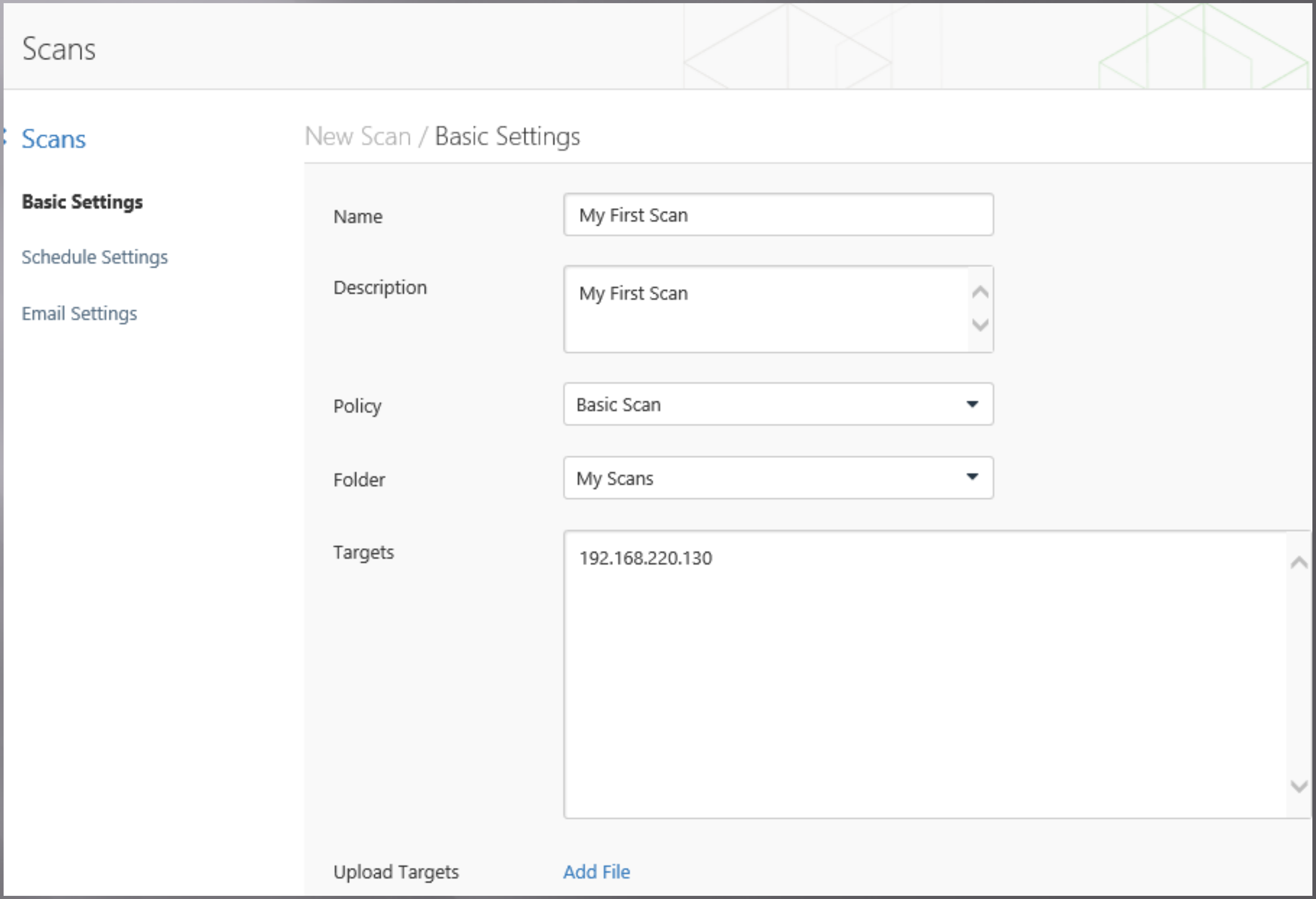
Policy Name: Basic Scan

Visibility: private

Description: First Scan

Allow Post-Scan Report Editing ☑

Creating A Scan



Name: My First Scan

Description: My First Scan

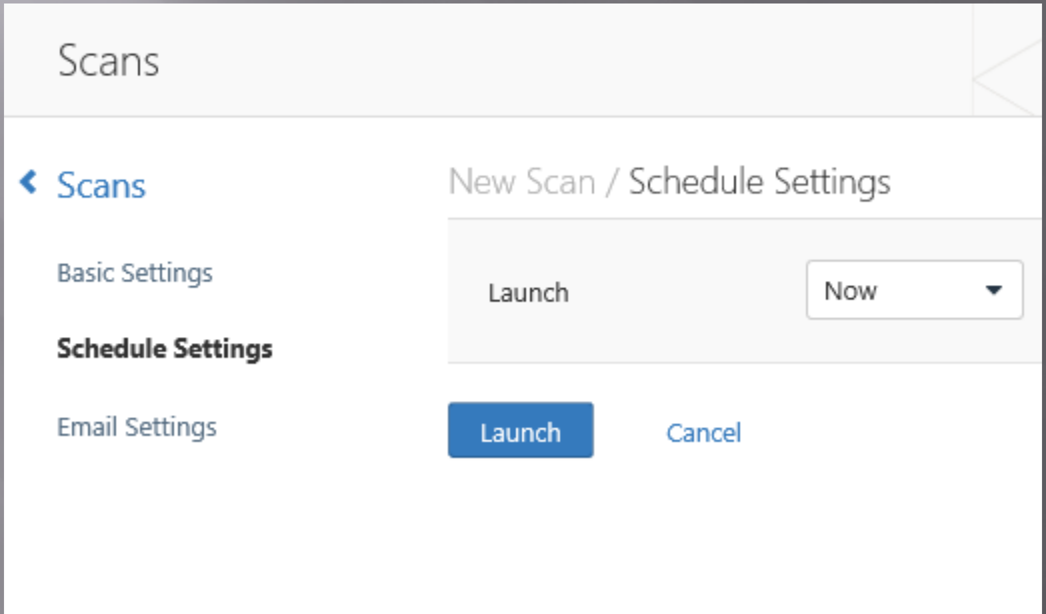
Policy: Basic Scan

Folder: My Scans

Targets: 192.168.220.130

Upload Targets: Add File

Scheduling A Scan

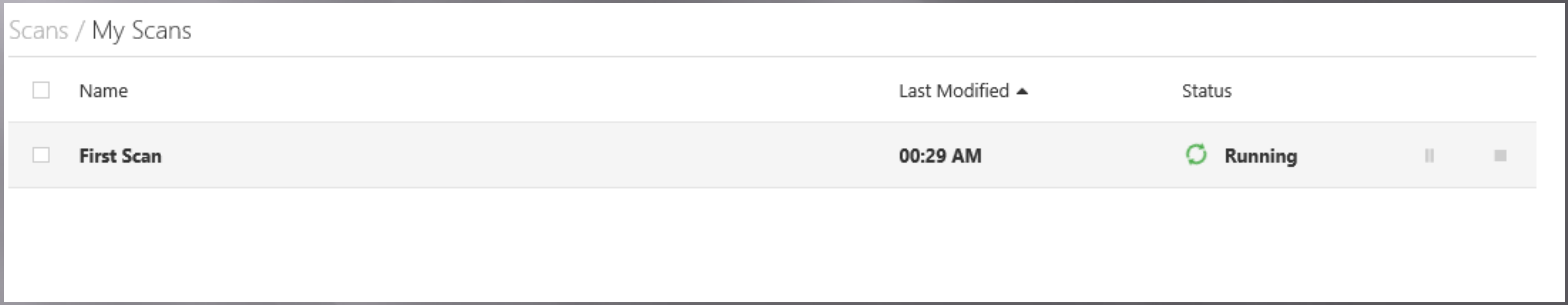


New Scan / Schedule Settings

Launch: Now

Scan Status

- Once your scan has started you will see a status field like this:

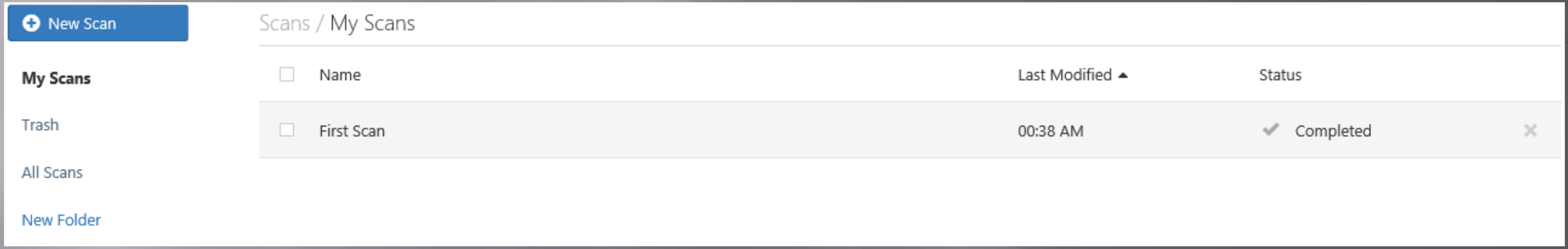


Scans / My Scans

□	Name	Last Modified ▲	Status
□	**First Scan**	**00:29 AM**	**Running**

Scan Status

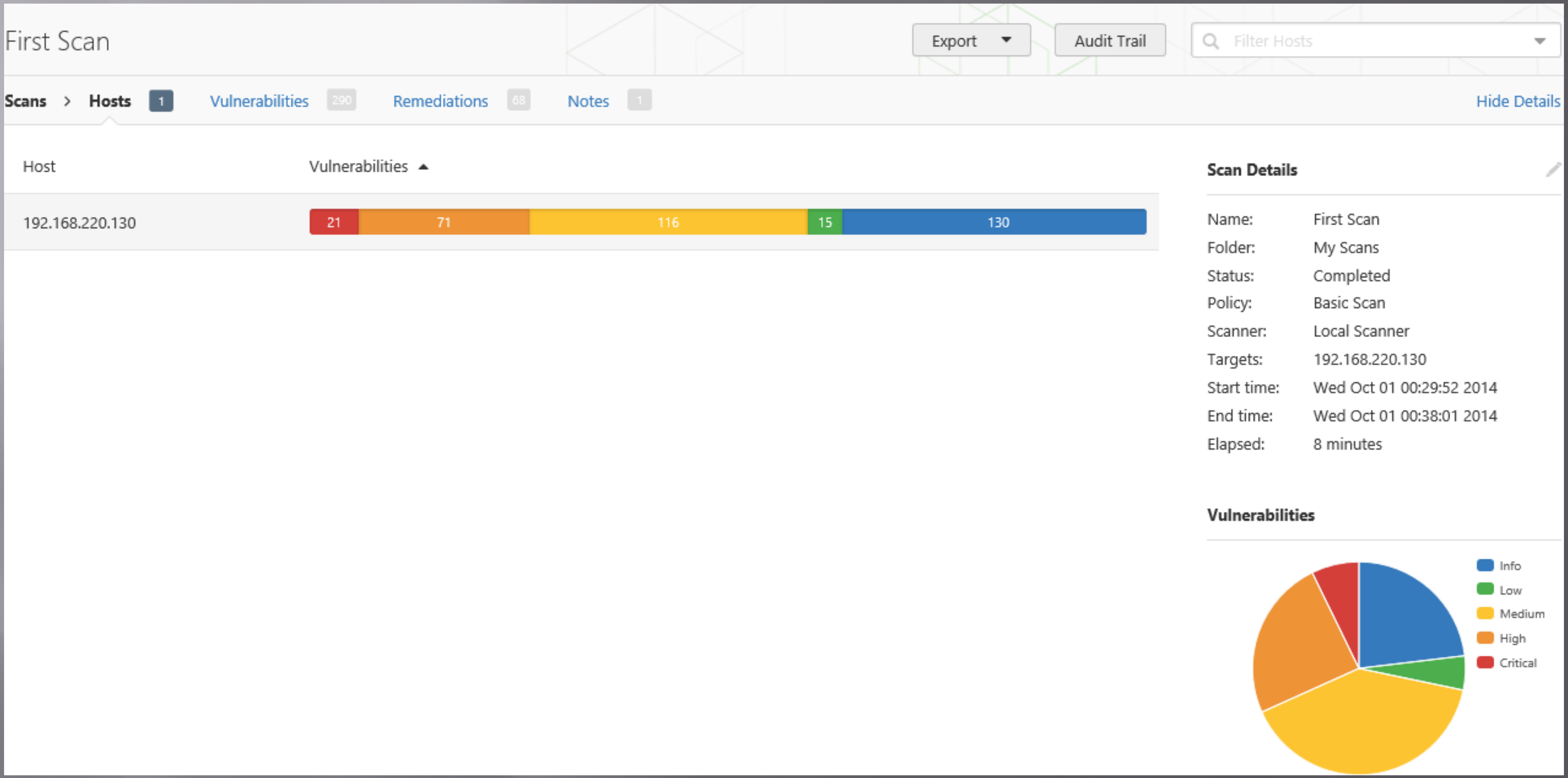
- Once completed you will get the following notification:



Scans / My Scans

□	Name	Last Modified ▲	Status	
□	First Scan	00:38 AM	✓ Completed	×

Output From First Scan



First Scan

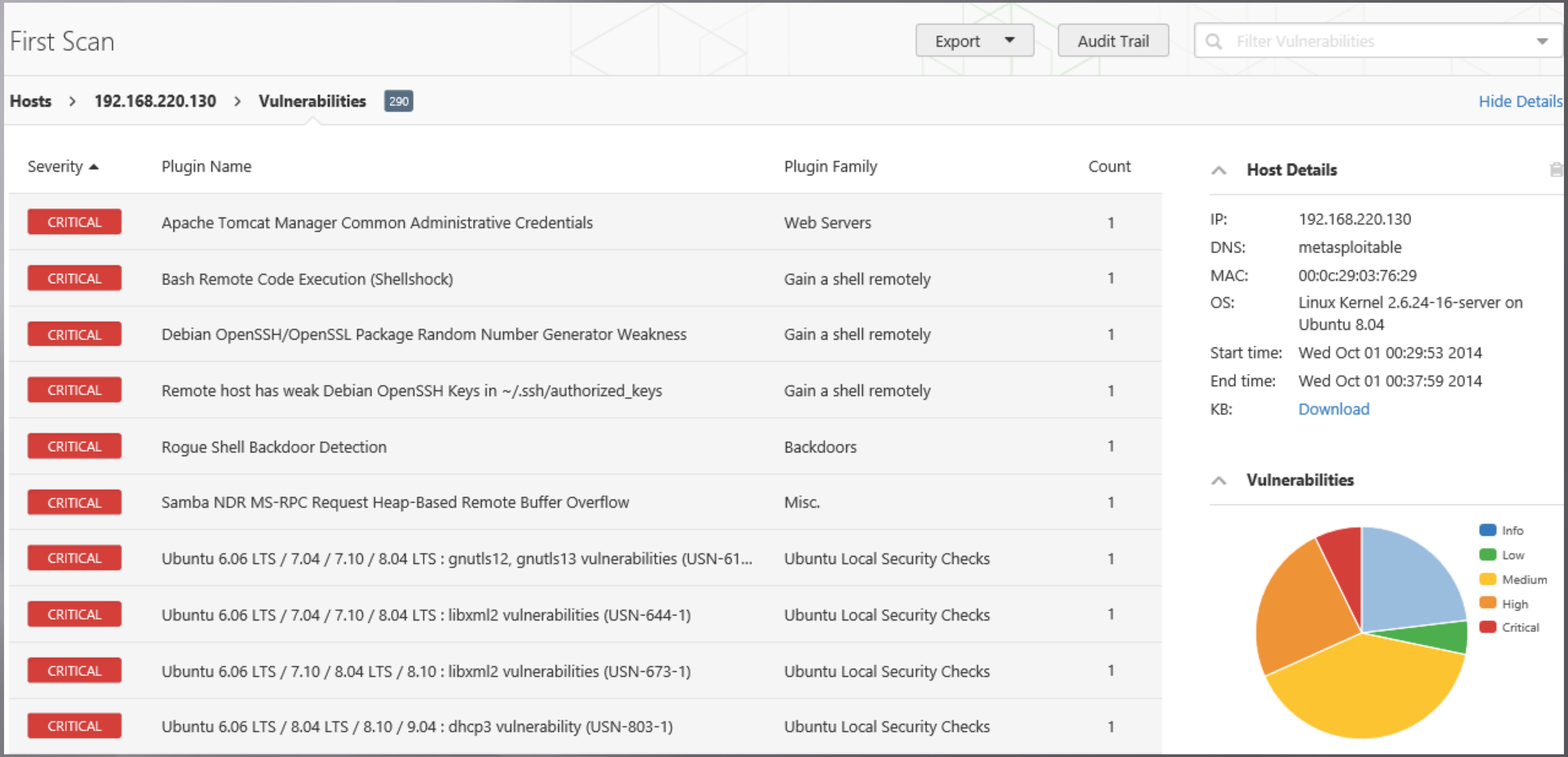
Host	Vulnerabilities
192.168.220.130	21 71 116 15 130

Scan Details

Name:	First Scan
Folder:	My Scans
Status:	Completed
Policy:	Basic Scan
Scanner:	Local Scanner
Targets:	192.168.220.130
Start time:	Wed Oct 01 00:29:52 2014
End time:	Wed Oct 01 00:38:01 2014
Elapsed:	8 minutes

Vulnerabilities

Clicking on scan gives details



First Scan

Export ▾ | Audit Trail | Filter Vulnerabilities

Hosts > 192.168.220.130 > Vulnerabilities 290

Hide Details

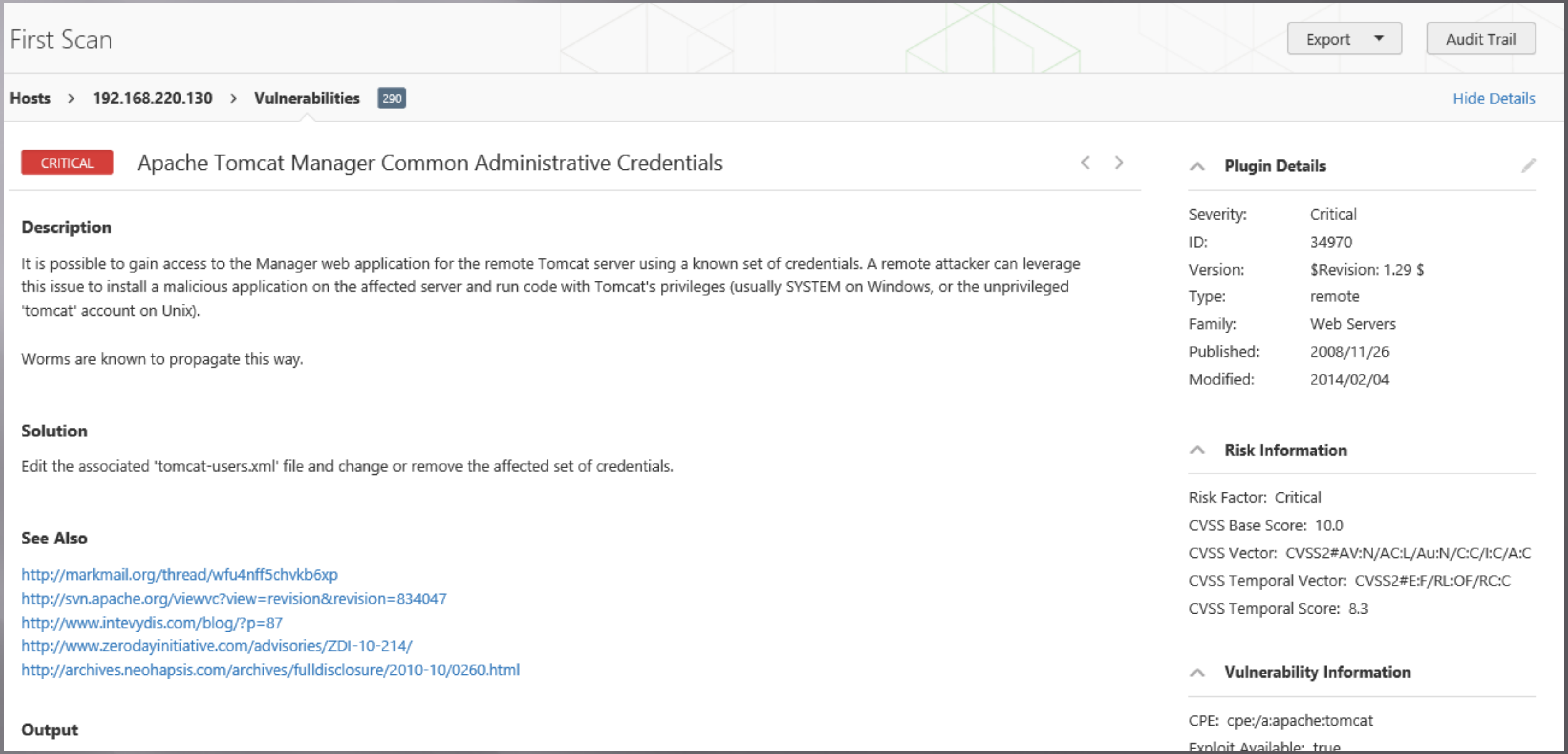
Severity ▲	Plugin Name	Plugin Family	Count
CRITICAL	Apache Tomcat Manager Common Administrative Credentials	Web Servers	1
CRITICAL	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	1
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1
CRITICAL	Remote host has weak Debian OpenSSH Keys in ~/.ssh/authorized_keys	Gain a shell remotely	1
CRITICAL	Rogue Shell Backdoor Detection	Backdoors	1
CRITICAL	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow	Misc.	1
CRITICAL	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gnutls12, gnutls13 vulnerabilities (USN-61...	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerabilities (USN-644-1)	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : libxml2 vulnerabilities (USN-673-1)	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : dhcp3 vulnerability (USN-803-1)	Ubuntu Local Security Checks	1

Host Details

IP:	192.168.220.130
DNS:	metasploitable
MAC:	00:0c:29:03:76:29
OS:	Linux Kernel 2.6.24-16-server on Ubuntu 8.04
Start time:	Wed Oct 01 00:29:53 2014
End time:	Wed Oct 01 00:37:59 2014
KB:	Download

Vulnerabilities

Continuing to drill down



First Scan

Apache Tomcat Manager Common Administrative Credentials

Description

It is possible to gain access to the Manager web application for the remote Tomcat server using a known set of credentials. A remote attacker can leverage this issue to install a malicious application on the affected server and run code with Tomcat's privileges (usually SYSTEM on Windows, or the unprivileged 'tomcat' account on Unix).

Worms are known to propagate this way.

Solution

Edit the associated 'tomcat-users.xml' file and change or remove the affected set of credentials.

See Also

http://markmail.org/thread/wfu4nff5chvkb6xp
http://svn.apache.org/viewvc?view=revision&revision=834047
http://www.intevydis.com/blog/?p=87
http://www.zerodayinitiative.com/advisories/ZDI-10-214/
http://archives.neohapsis.com/archives/fulldisclosure/2010-10/0260.html

Output

Plugin Details

Severity:	Critical
ID:	34970
Version:	$Revision: 1.29 $
Type:	remote
Family:	Web Servers
Published:	2008/11/26
Modified:	2014/02/04

Risk Information

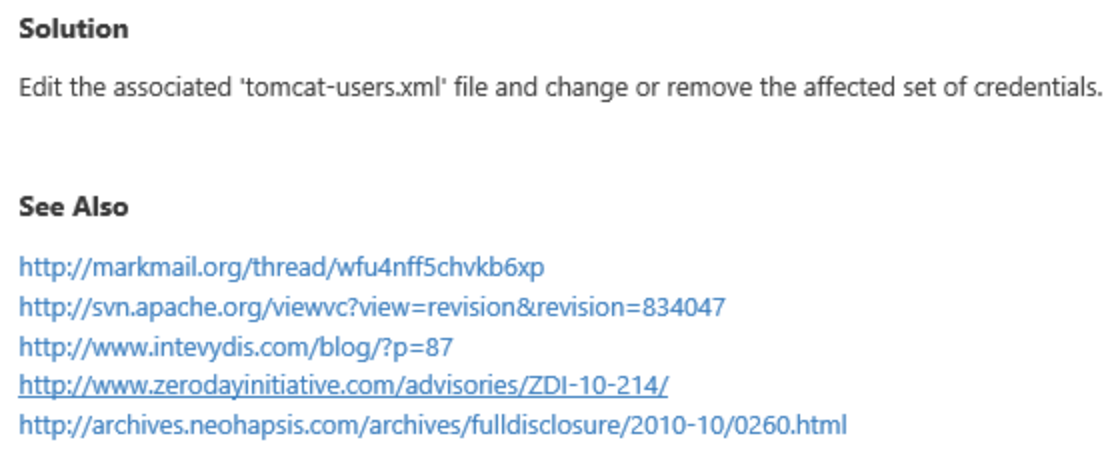
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
CVSS Temporal Score: 8.3

Vulnerability Information

CPE: cpe:/a:apache:tomcat
Exploit Available: true

Good Information

- Important to note:



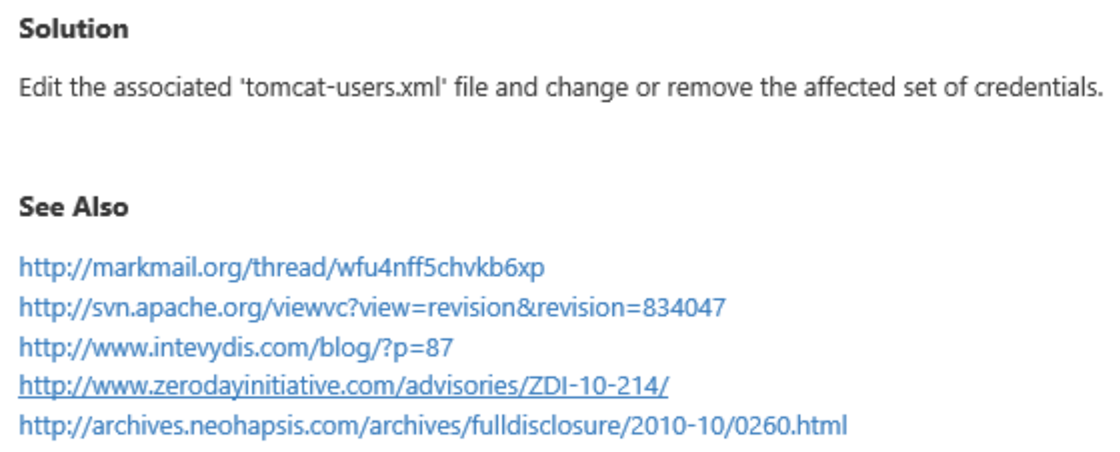
Solution

Edit the associated 'tomcat-users.xml' file and change or remove the affected set of credentials.

See Also

http://markmail.org/thread/wfu4nff5chvkb6xp
http://svn.apache.org/viewvc?view=revision&revision=834047
http://www.intevydis.com/blog/?p=87
http://www.zerodayinitiative.com/advisories/ZDI-10-214/
http://archives.neohapsis.com/archives/fulldisclosure/2010-10/0260.html

- Also



Solution

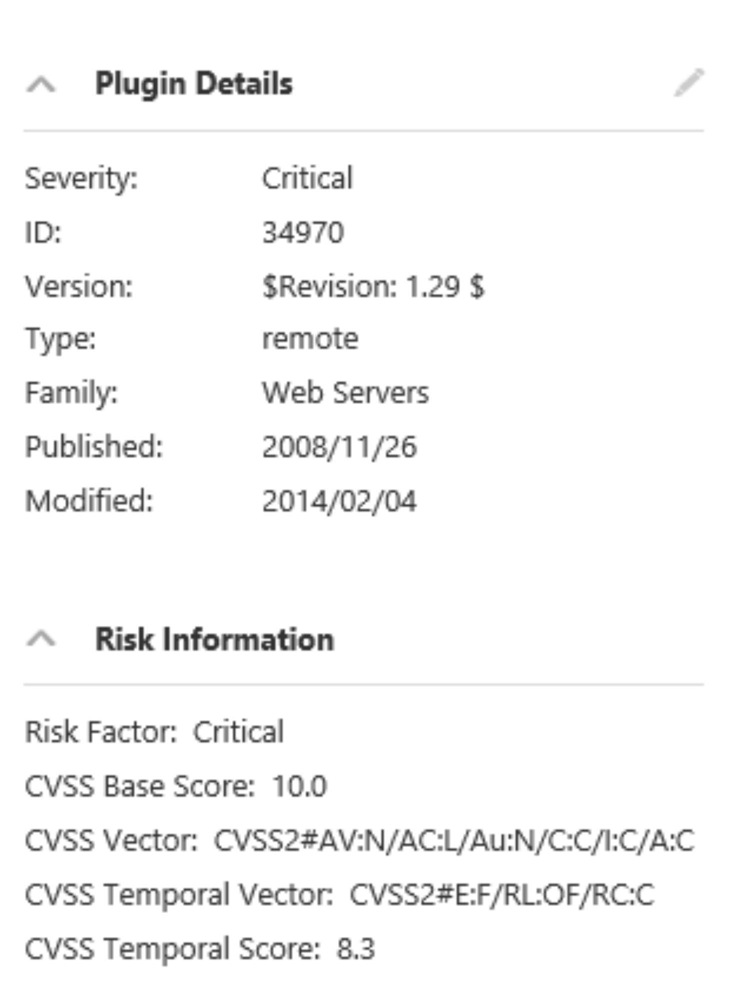
Edit the associated 'tomcat-users.xml' file and change or remove the affected set of credentials.

See Also

http://markmail.org/thread/wfu4nff5chvkb6xp
http://svn.apache.org/viewvc?view=revision&revision=834047
http://www.intevydis.com/blog/?p=87
http://www.zerodayinitiative.com/advisories/ZDI-10-214/
http://archives.neohapsis.com/archives/fulldisclosure/2010-10/0260.html

Criticality

- Note on criticality
- The "Critical" risk factor is without any mitigating controls being taken in to account
- Vulnerabilities need to be evaluated in context



Plugin Details

Severity:	Critical
ID:	34970
Version:	$Revision: 1.29 $
Type:	remote
Family:	Web Servers
Published:	2008/11/26
Modified:	2014/02/04

Risk Information

Risk Factor: Critical

CVSS Base Score: 10.0

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

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

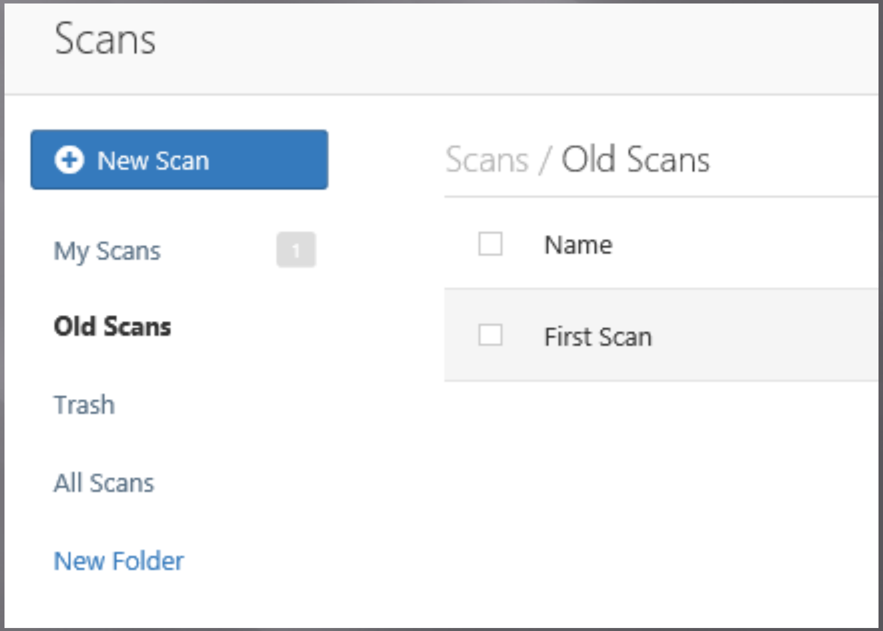
CVSS Temporal Score: 8.3

More on Results

- These results were obtained, even though Anti-Virus continued blocking multiple techniques.
- Consider setting up a scanning machine without any AV or Host Firewall.

Organizing Scans

- In short order you will gather a large collection of scans
- Use the built in folder system to move scans off of the main page

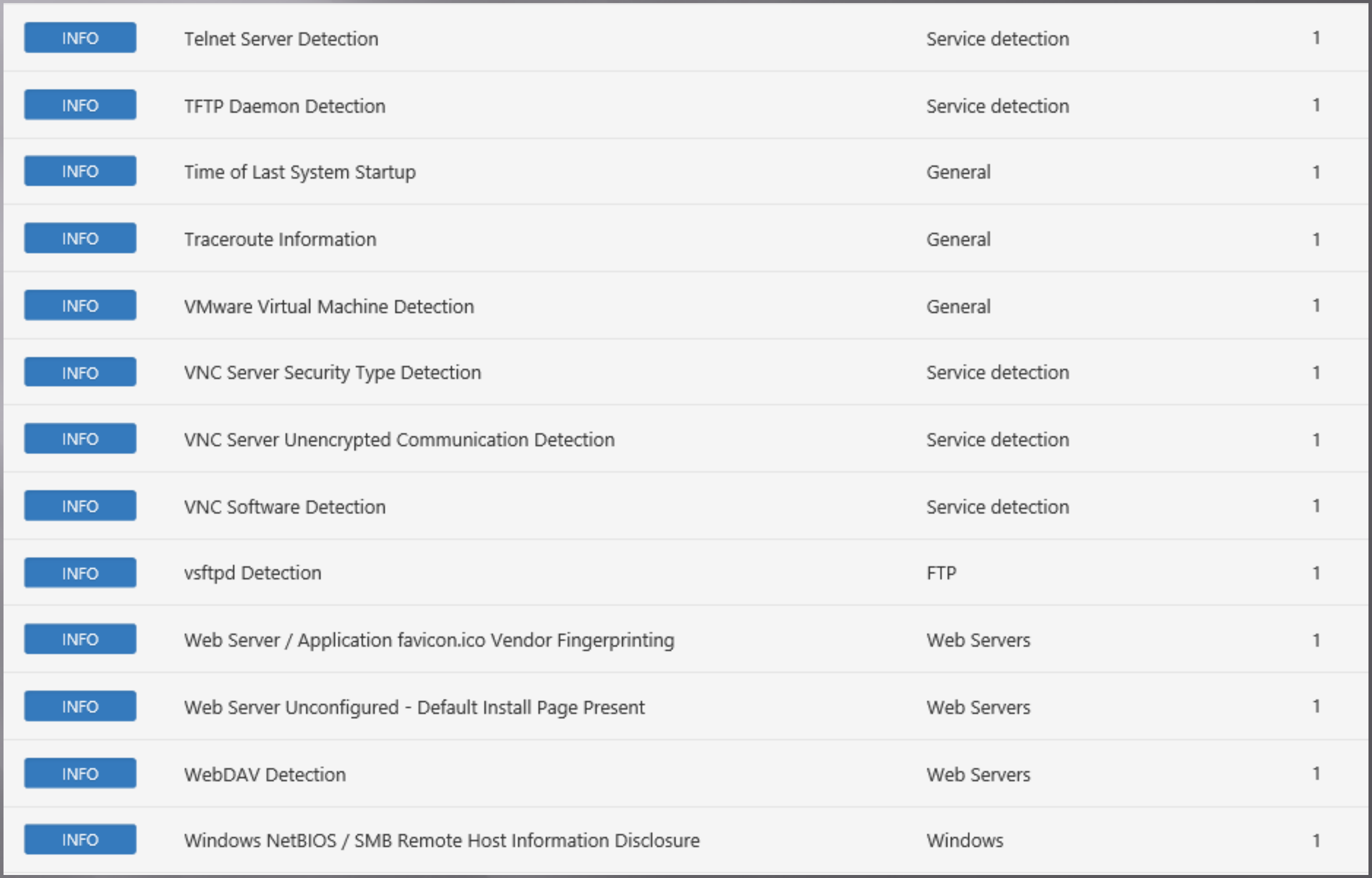


Scans / Old Scans

□ Name

□ First Scan

Don’t Forget the Info

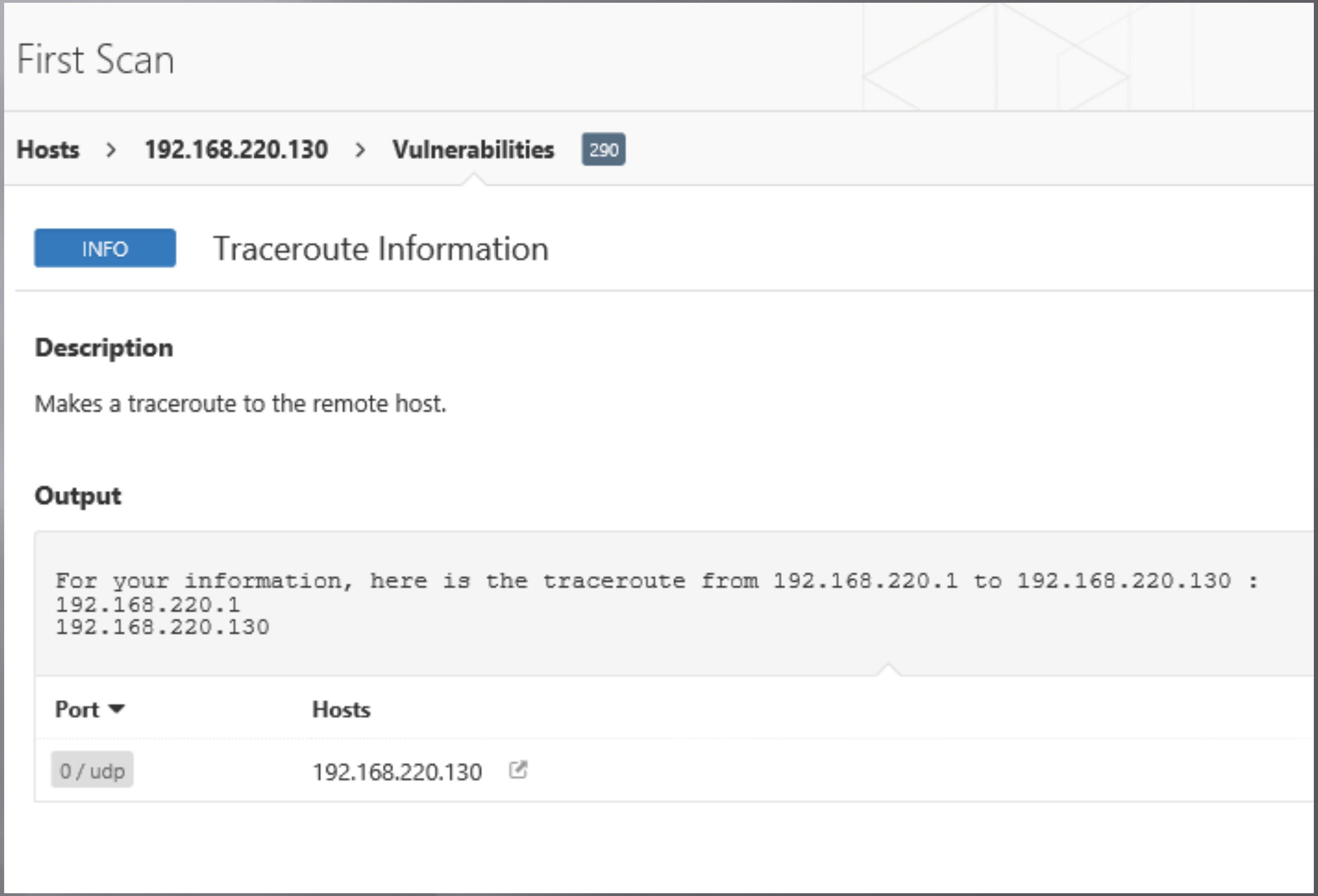


INFO	Telnet Server Detection	Service detection	1
INFO	TFTP Daemon Detection	Service detection	1
INFO	Time of Last System Startup	General	1
INFO	Traceroute Information	General	1
INFO	VMware Virtual Machine Detection	General	1
INFO	VNC Server Security Type Detection	Service detection	1
INFO	VNC Server Unencrypted Communication Detection	Service detection	1
INFO	VNC Software Detection	Service detection	1
INFO	vsftpd Detection	FTP	1
INFO	Web Server / Application favicon.ico Vendor Fingerprinting	Web Servers	1
INFO	Web Server Unconfigured - Default Install Page Present	Web Servers	1
INFO	WebDAV Detection	Web Servers	1
INFO	Windows NetBIOS / SMB Remote Host Information Disclosure	Windows	1

Info Vulnerabilities

- The least significant vulnerabilities are classified as "Info" or informational.
- These are often very useful in understanding details of the asset being scanned.

For Instance



First Scan

Hosts › 192.168.220.130 › Vulnerabilities 290

INFO Traceroute Information

Description

Makes a traceroute to the remote host.

Output

```
For your information, here is the traceroute from 192.168.220.1 to 192.168.220.130 :
192.168.220.1
192.168.220.130
```

Port ▾	Hosts
0 / udp	192.168.220.130

Ruby

- Link to Language
  - https://www.ruby-lang.org/en/
- Link to Interactive Ruby Website
  - https://ruby.github.io/TryRuby/
- Work through exercise section labeled “Of All the Summaries #3, is Here Now” down to “Have you got the time?”

Next Week

- NetCat
- DOS Batch

Questions

?