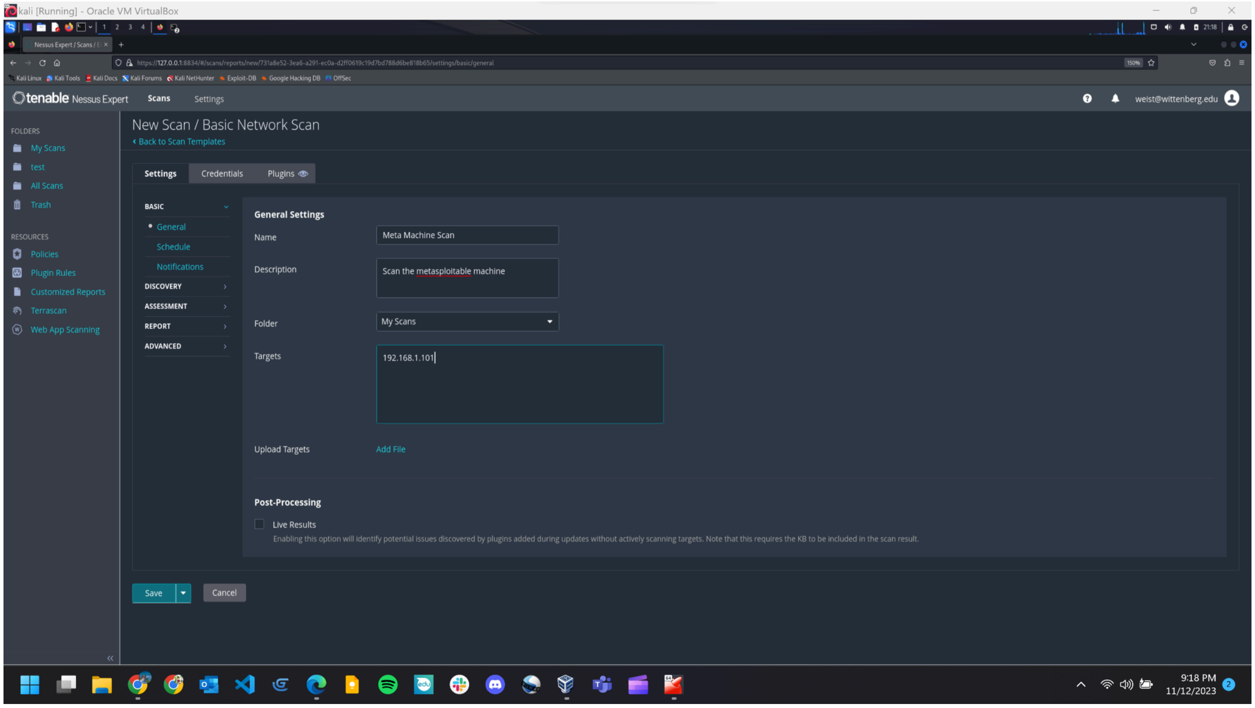
I received additional help from the article at:
https://community.tenable.com/s/article/Nessus-scanner-is-stuck-in-the-Initializing-process?language=en_US

This helped get the "New Scan" button to run. I used the following commands to get the initializing process to work.

```
# sudo service nessusd stop
# sudo /opt/nessus/sbin/nessusd -R
# sudo service nessusd start
```

Part 2 Capture: Setting up and running the scan on the Metasploitable machine.



https://127.0.0.1:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general

New Scan / Basic Network Scan

‹ Back to Scan Templates

General Settings

Name: Meta Machine Scan

Description: Scan the metasploitable machine

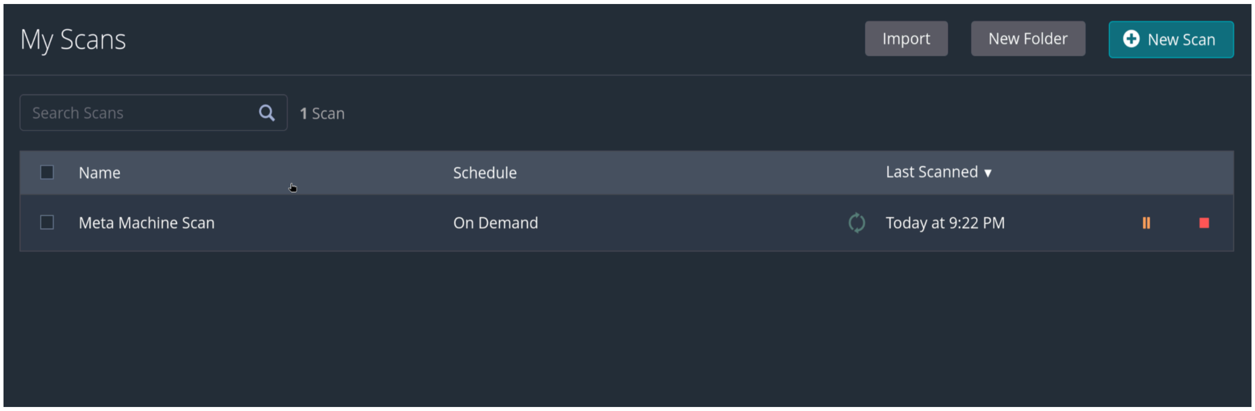
Folder: My Scans

Targets: 192.168.1.101

Upload Targets: Add File

Post-Processing

□ Live Results
Enabling this option will identify potential issues discovered by plugins added during updates without actively scanning targets. Note that this requires the KB to be included in the scan result.



My Scans

1 Scan

□	Name	Schedule	Last Scanned ▾
□	Meta Machine Scan	On Demand	Today at 9:22 PM

Part 3:
How many critical vulnerabilities are there? 12 critical

Drill down into each critical vulnerability discovered and provide a description of each.

1. **NFS Exported Share Information Disclosure**
   - **Description:** At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.
   - **Solution:** Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
2. **Unix Operating System Unsupported Version Detection**
   - **Description:** According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
   - Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
   - **Solution:** Upgrade to a version of the Unix operating system that is currently supported.
3. **InrealIRCd Backdoor Detection**
   - **Description:** The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.
   - **Solution:** Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.
4. **VNC Server 'password' Password**
   - **Description:** The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.
   - **Solution:** Secure the VNC service with a strong password.

5 & 6. **SSL Version 2 and 3 Protocol Detection**
   - **Description:** The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:
     - An insecure padding scheme with CBC ciphers.
     - Insecure session renegotiation and resumption schemes.
   - An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.
   - Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.
   - NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

  - **Solution:** Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

7. **Bind Shell Backdoor Detection**
   - **Description:** A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.
   - **Solution:** Verify if the remote host has been compromised, and reinstall the system if necessary.

8. **Apache Tomcat SEoL (<= 5.5.x)**
   - **Description:** According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.
   - Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.
   - **Solution:** Upgrade to a version of Apache Tomcat that is currently supported.

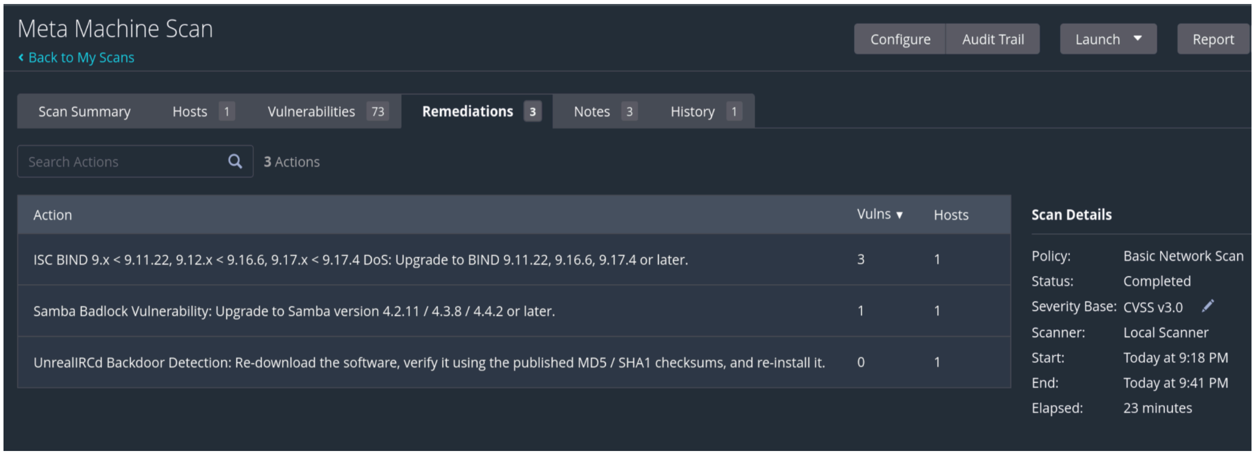
9. **Apache Tomcat AJP Connector Request Injection (Ghostcat)**
   - **Description:** A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).
   - **Solution:** Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

10 & 11. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**
   - **Description:** The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.
   - The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
   - An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man-in-the-middle attack.
   - **Solution:** Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL, and OpenVPN key materials should be re-generated.

12. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**
   - **Description:** The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.
   - The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
   - An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man-in-the-middle attack.
   - **Solution:** Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL, and OpenVPN key materials should be re-generated.

Check out the Remediations tab and write a brief list of recommended actions you would provide to a system administrator maintaining the Metasploitable server.

- ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.
- Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
- UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

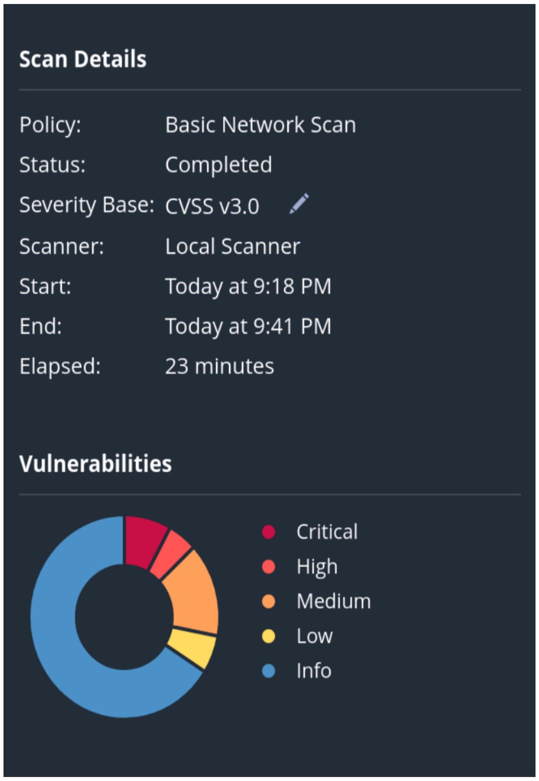


3 Actions

Action	Vulns ▾	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 9:18 PM
End:	Today at 9:41 PM
Elapsed:	23 minutes



Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 9:18 PM
End:	Today at 9:41 PM
Elapsed:	23 minutes

Vulnerabilities