Security Scanning Assignment

In this Scenario, a network Security Analyst is required to scan a host prior to onboarding

The target is meant to host the “Company’s” Business Critical Web Services.

Contents

[Scenario 4](#_Toc116996091)

[Methodology 5](#_Toc116996092)

[Network Discovery 6](#_Toc116996093)

[Non-Credentialed Scan 7](#_Toc116996094)

[Credentialed Scan 8](#_Toc116996095)

[Detailed Scanned Results and Priority 9](#_Toc116996096)

[APPENDIX 10](#_Toc116996097)

[REMEDIATION PLAN 11](#_Toc116996098)

# Scenario

A new Web Server hosting a Business Critical B2B order system is about to be put into production.

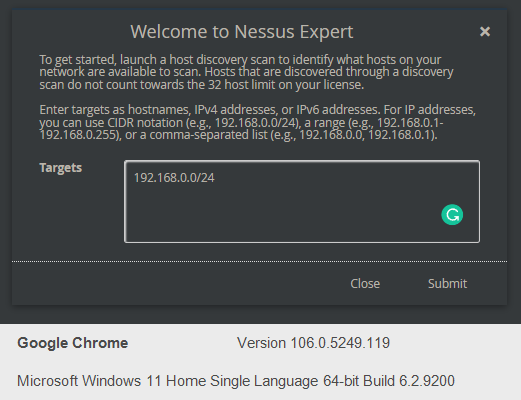
The CISO was unaware of this and was only informed about it 1 week prior to the roll-out.

The CISO quickly assigns a Security Analyst to perform an onboarding Vulnerability Scan.

# Methodology

The Security Analyst Performs the following Steps

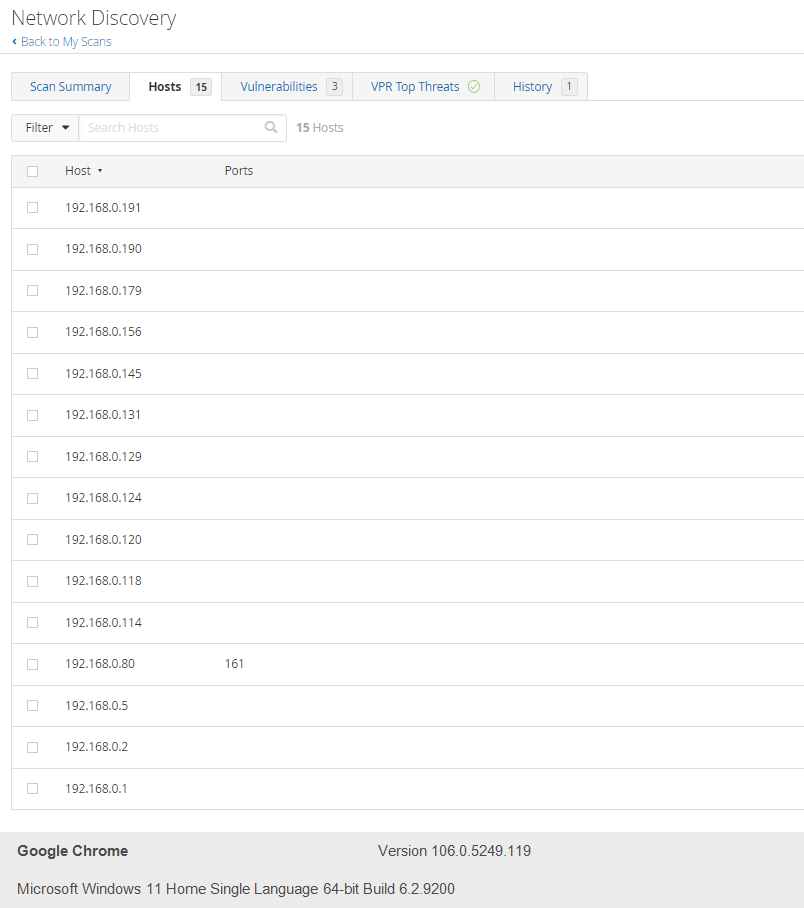
1. The Target host is paced on a private Network for scanning.
2. A non-intrusive discovery scan is performed on the Network
3. The target host is identified
4. A non-credentialed scan is performed on the target to determine the Basic Vulnerabilities
5. A credentialed scan is performed to determine al the Vulnerabilities based on the Plugins and Signature available on the scanning tool.
6. The Vulnerabilities are ranked based on Severity and Prioritised
7. A remediation plan is prepared and reviewed with the CISO and then with the Business Unit.
8. Progress of the remediation is tracked and reported until the CISO and Business units can agree that sufficient risk has been mitigated
9. Subsequent remediation is planned during patch and maintenance cycles.



## Network Discovery

The Security Analyst performs a discovery scan on the Test Network to verify that the Target system is visible on the Network and accessible for scanning.

In this Scenario the target host has an IP of 192. 168.0.145. This is a non-internet routable private IP address

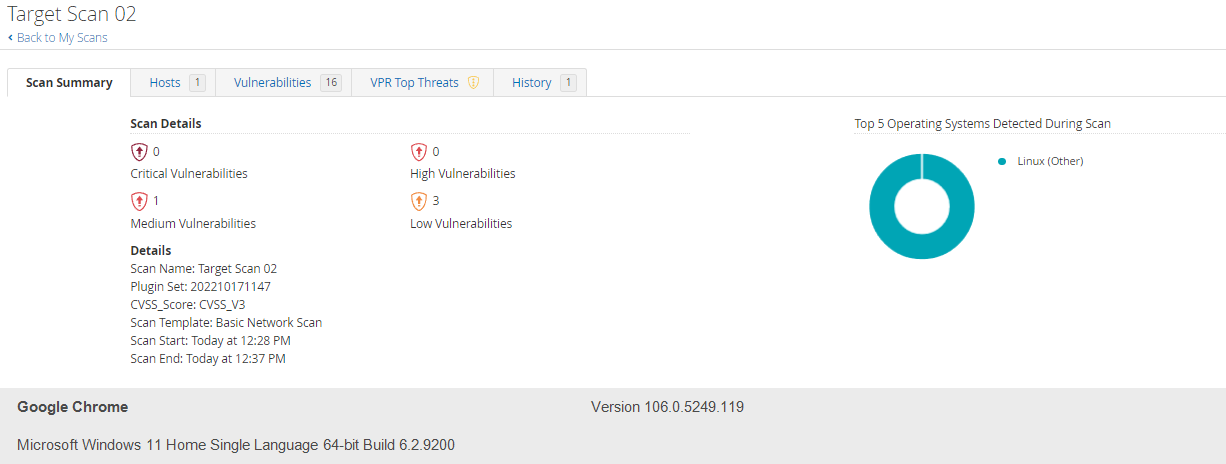


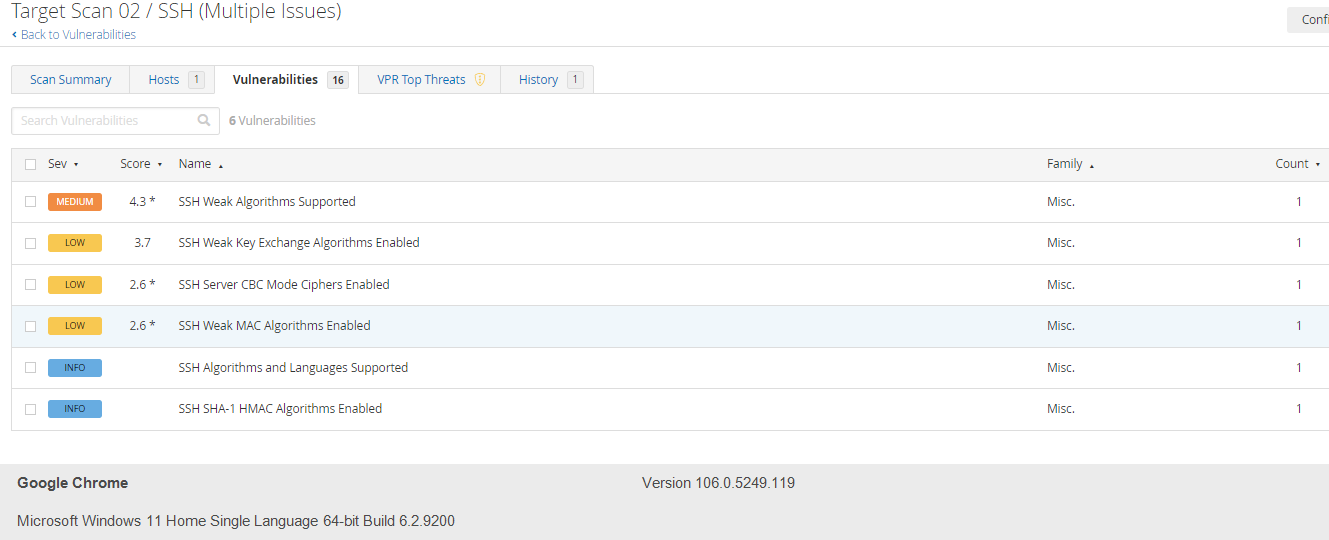
## Non-Credentialed Scan

Non-Credentialed scan is performed to determine the basic Vulnerabilities that exist on the host. Usually, these Vulnerabilities would be easily discoverable and exploited even by the most novice of hackers or malicious actors.

The Summary of the scans are:

* Number of CRITICAL severity Vulnerabilities: 0
* Number of HIGH severity Vulnerabilities: 0
* Number of MEDIUM severity Vulnerabilities: 1
* Number of LOW severity Vulnerabilities: 3





First Impressions:

Although No High or Critical Vulnerabilities were discovered, Weak SSH algorithms usually indicates either outdated Linux packages/distributions and/or Weak (unhardened) configurations of the services.

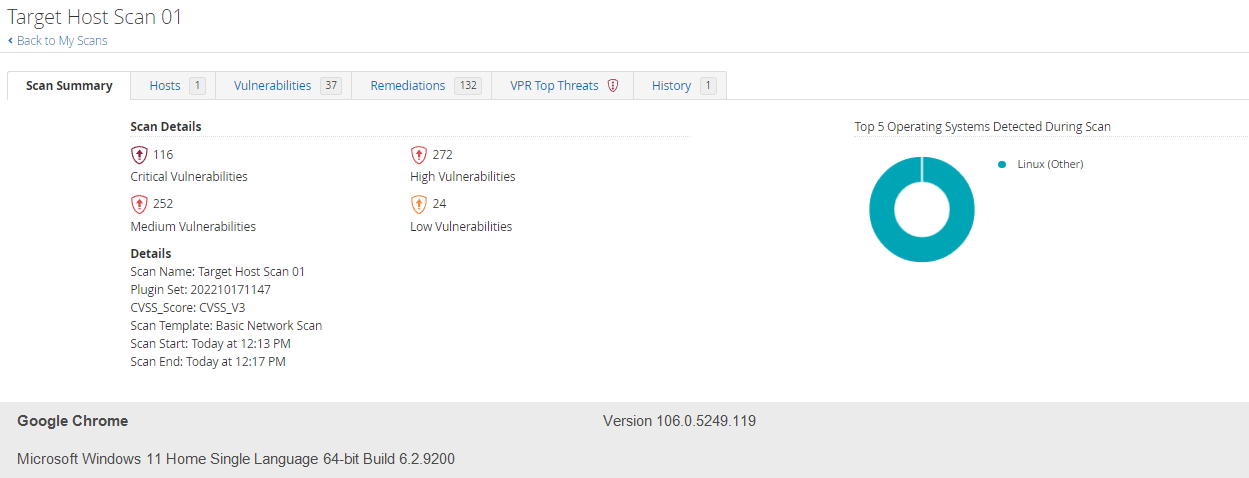
## Credentialed Scan

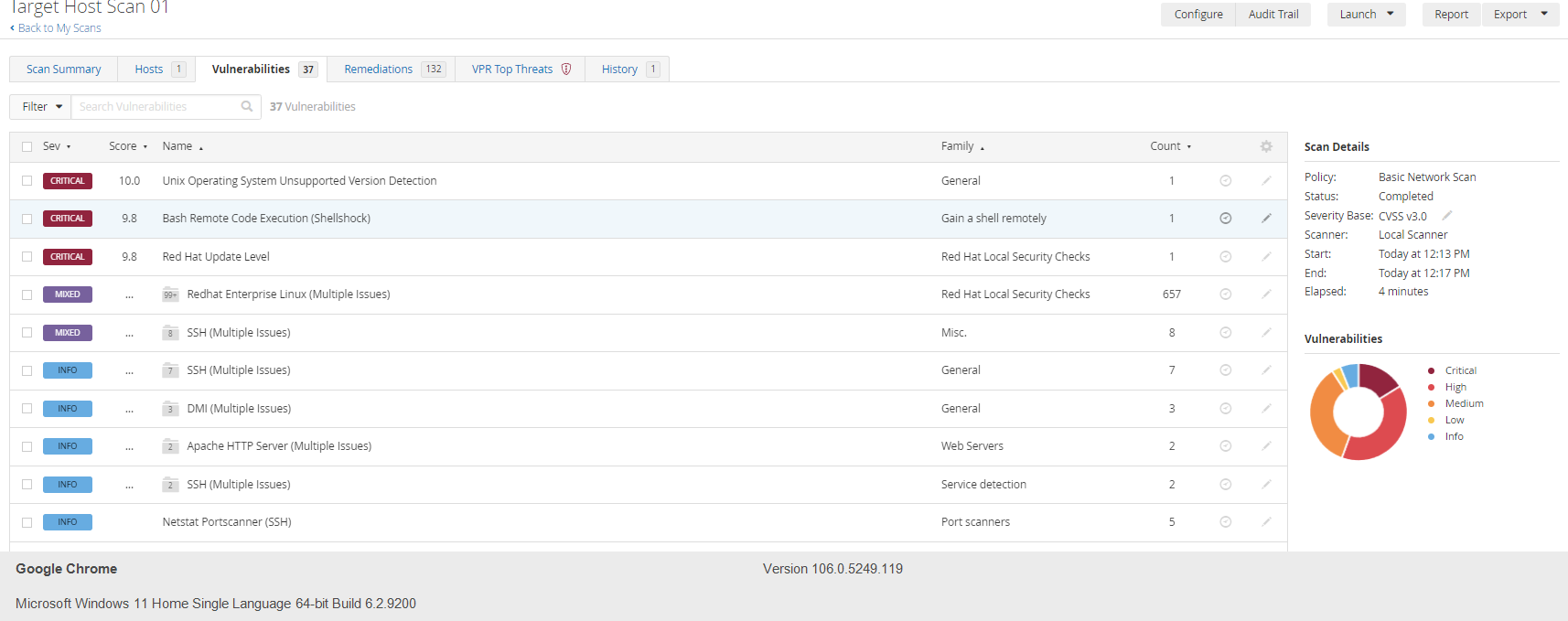
Using an elevated account, the scan is repeated using a credentialed ssh login. This would reveal the depths of the actual Vulnerabilities.

The elevated account is disabled or password changed after the scan is completed.

The Summary of the scans are:

* Number of CRITICAL severity Vulnerabilities: 116
* Number of HIGH severity Vulnerabilities: 272
* Number of MEDIUM severity Vulnerabilities: 252
* Number of LOW severity Vulnerabilities: 24



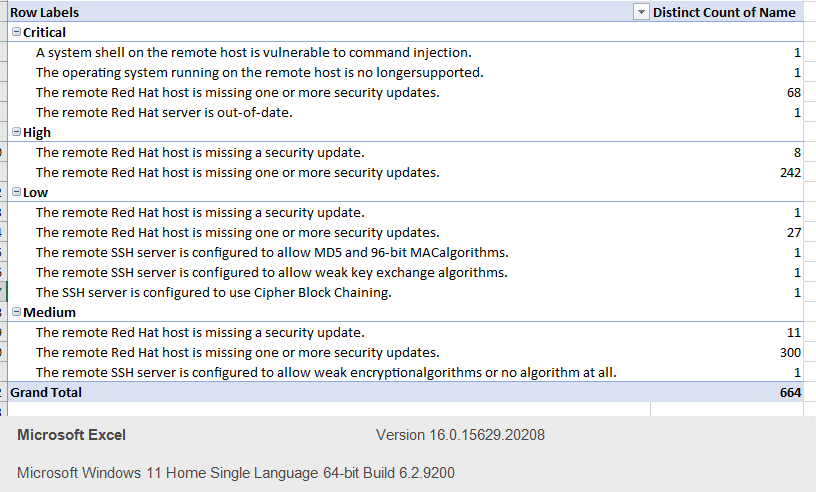


It is clear that this server contains too many CRITICAL and HIGH severity Vulnerabilities and these needs to be remediated prior to being a live production system.

## Detailed Scanned Results and Priority

The detailed report is attached in the Appendix.

However, for an action plan, the Security Analyst performs some analysis of the Vulnerabilities and creates the following summary.



The security Analyst recommends that All of the CRITICAL and HIGH severity can be remediated with an OS and package date to the latest stable release.

## REMEDIATION PLAN

The CISO and Business jointly agrees on the following:

1. The risk needs to be remediated and agrees that all CRITICAL and HIGH Vulnerabilities MUST be remediated prior to launch
2. A rescan is perform to verify the results.
3. All MEDIUM Severity Vulnerabilities are agreed to be remediated within 30 days.
4. Weekly Scans are to be performed and discovered Vulnerabilities are to be remediated within the following SLA:
   1. CRITICAL: 24 hours
   2. HIGH: 7 days
   3. MEDIUM: 30 days
5. Further to that any Vulnerabilities that are not able to be remediated due to compatibility or operational risk are tracked in a Risk register and the risk accepted by the management.
   1. The risk register is to be reviewed Quarterly to re-access the risk

# APPENDIX

