

# Auditing Windows Systems for Security Compliance (3e)

Security Strategies in Windows Platforms and Applications, Third Edition - Lab 06

Student:

Jacob Jeffers

Email:

jjeffers6151@ucumberlands.edu

Time on Task:

5 hours, 20 minutes

Progress:

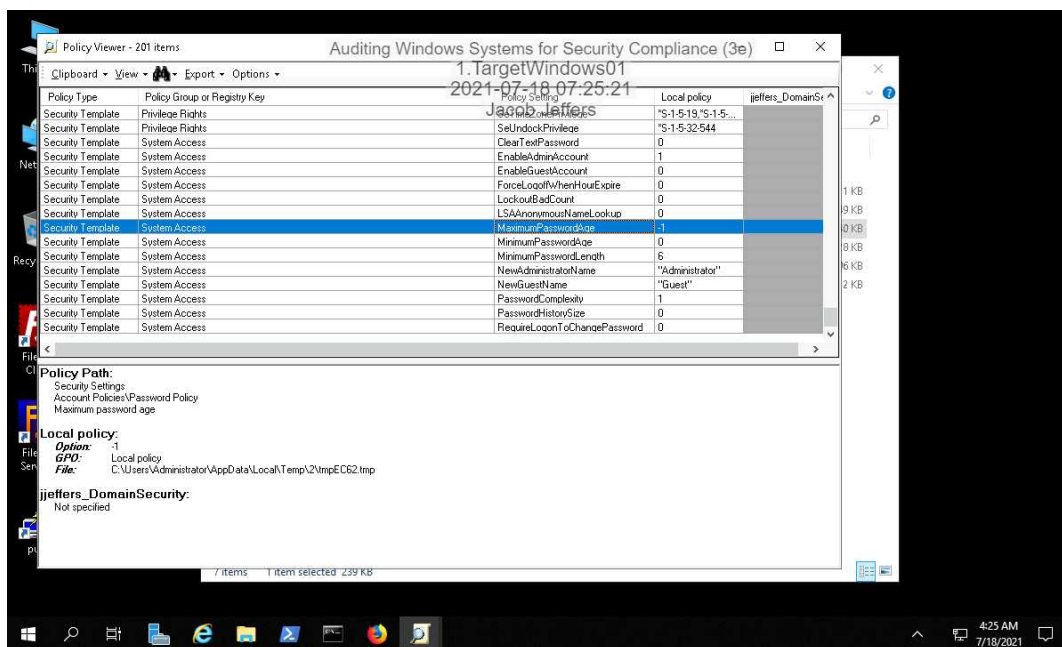
100%

Report Generated: Sunday, July 18, 2021 at 8:29 AM

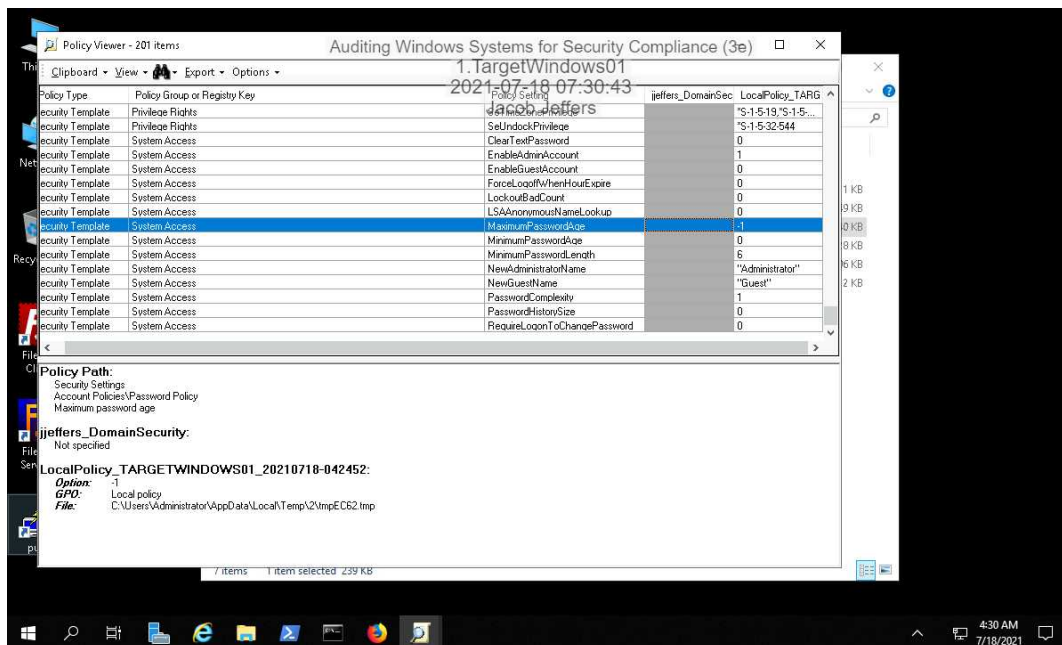
## Section 1: Hands-On Demonstration

### Part 1: Audit a Windows System using Policy Analyzer

16. Make a screen capture showing the **current MaximumPasswordAge** setting in the **Policy Viewer**.

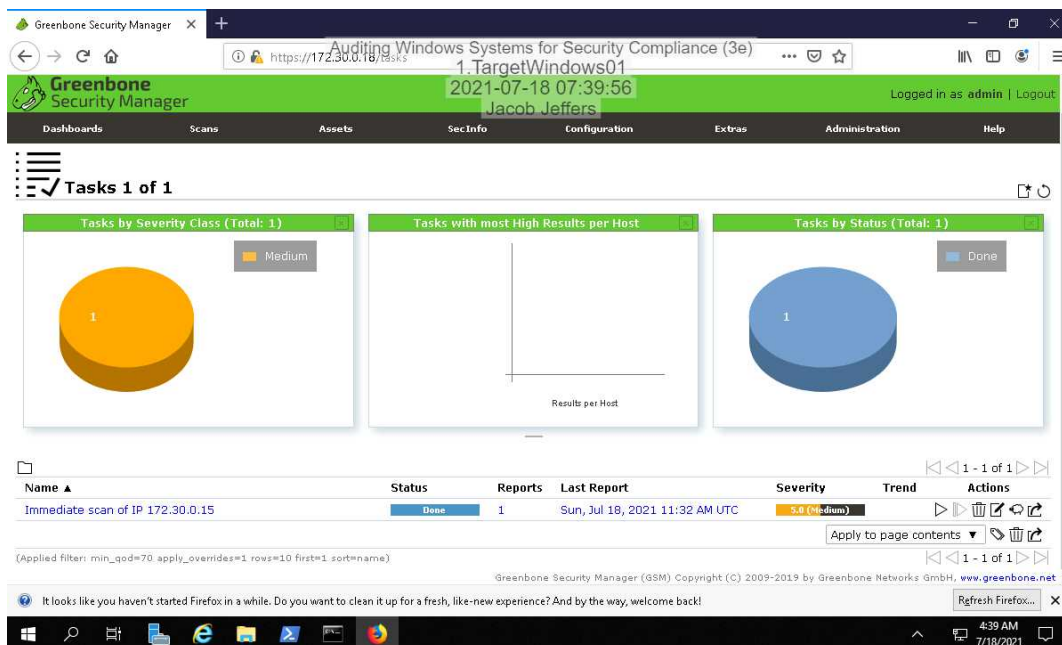


35. Make a screen capture showing the **updated MaximumPasswordAge** setting in the **Policy Viewer**.

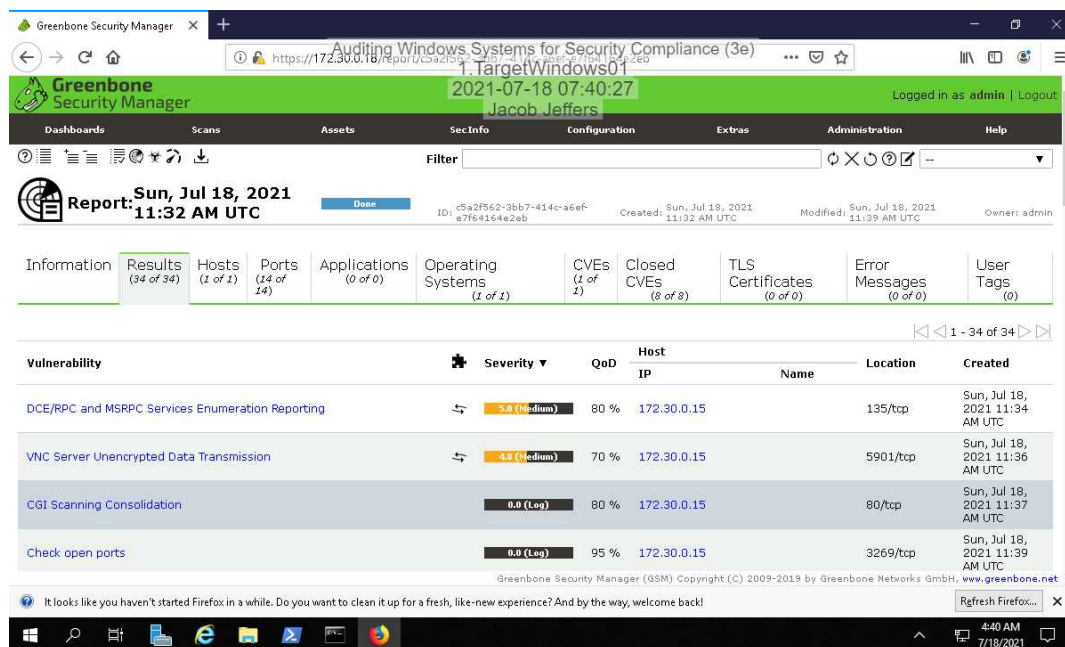


## Part 2: Audit a Windows System using OpenVAS

8. Make a screen capture showing the **completed scan of TargetWindows01**.



11. **Make a screen capture** showing the **vulnerabilities** from the completed scan of **TargetWindows01**.



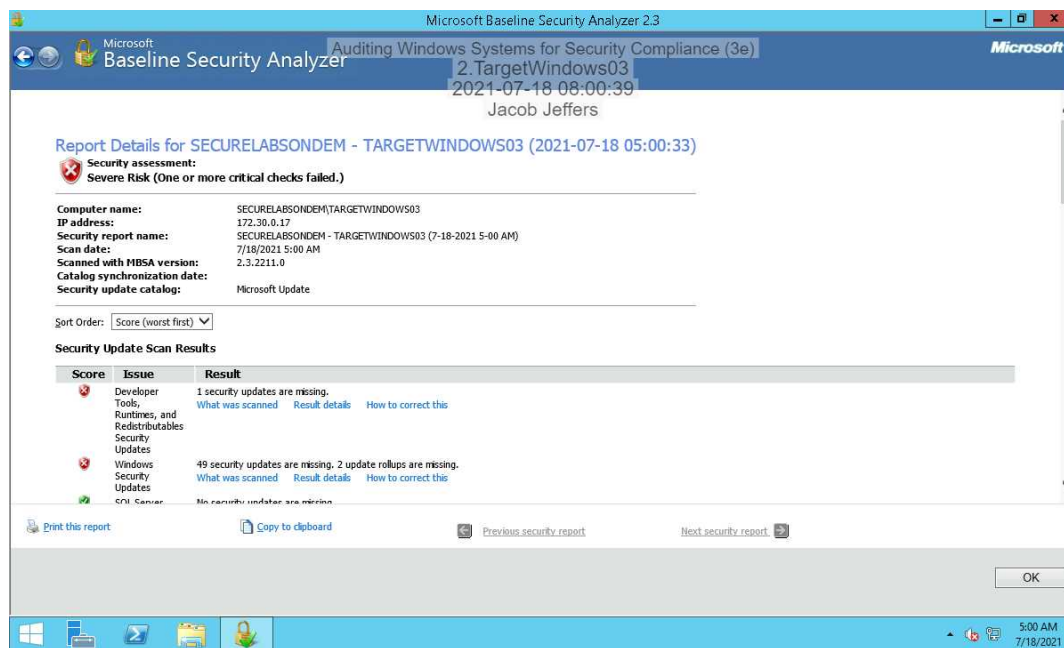
13. **Describe** remediation steps for the vulnerability you selected.

The vulnerability allows the attackers to gain more knowledge about the remote host. The best mitigation strategy is to filter incoming traffic to the affected ports.

## Section 2: Applied Learning

### Part 1: Audit a Windows System using MBSA

11. Make a screen capture showing the **MBSA scan results**.

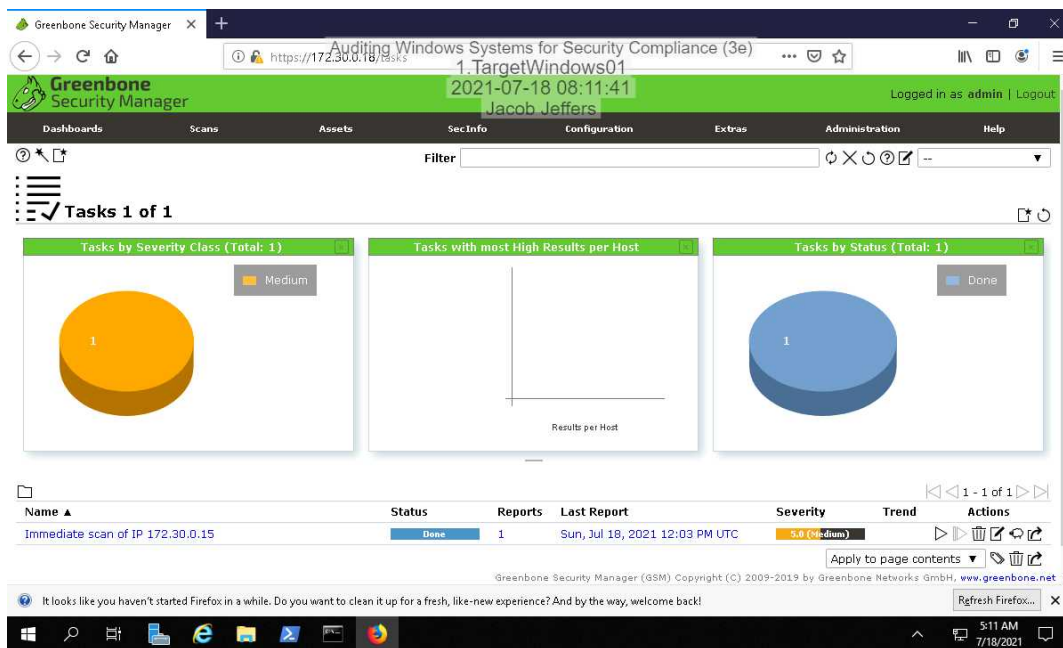


16. **Describe** the security issue for this missing update.

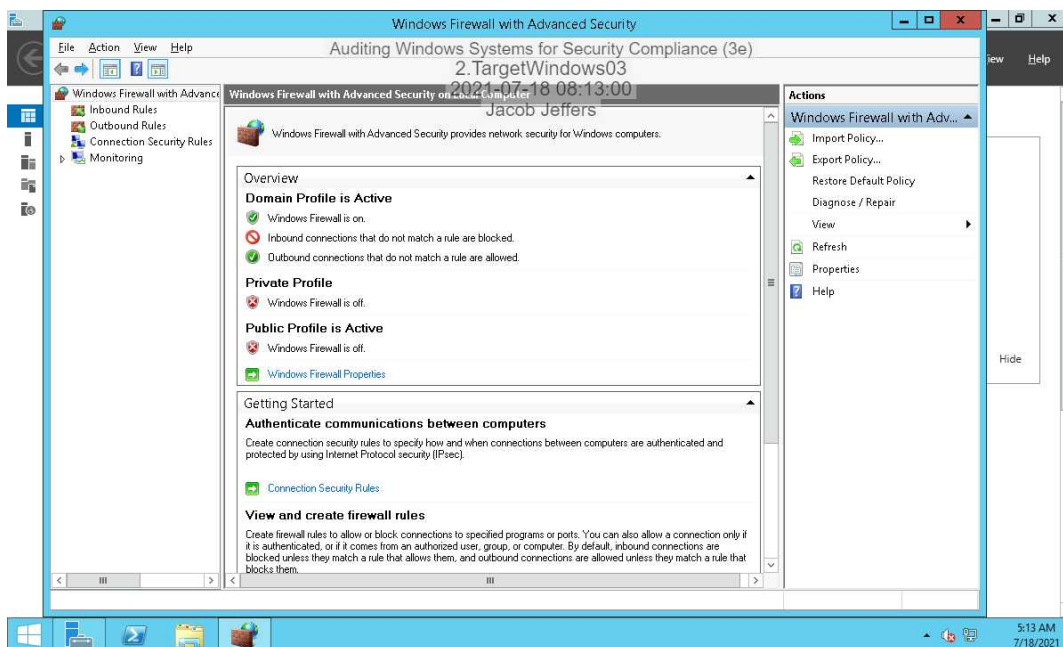
On the Windows Update security update, the security with this issue is that the server does not have all required updates.

### Part 2: Audit a Windows System using OpenVAS

7. Make a screen capture showing the vulnerabilities from the completed scan of TargetWindows03.



17. Make a screen capture showing the active Windows Firewall.



# Auditing Windows Systems for Security Compliance (3e)

Security Strategies in Windows Platforms and Applications, Third Edition - Lab 06

21. Make a screen capture showing the vulnerabilities from the latest completed scan of TargetWindows03 (without the DCE/RPC vulnerability listed).

Greenbone Security Manager

Report: Sun, Jul 18, 2021 12:13 PM UTC

Hosts: 1 of 1

Ports: 14 of 14

Applications: 0 of 0

Operating Systems: 1 of 1

CVEs: 1 of 1

Closed CVEs: 8 of 8

TLS Certificates: 0 of 0

Error Messages: 0 of 0

User Tags: 0

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
CGI Scanning Consolidation	0.0 (Log)	80 %	172.30.0.15		80/tcp	Sun, Jul 18, 2021 12:18 PM UTC
CPE Inventory	0.0 (Log)	80 %	172.30.0.15		general/CPE-T	Sun, Jul 18, 2021 12:20 PM UTC
DCE/RPC and MSRPC Services Enumeration	0.0 (Log)	80 %	172.30.0.15		135/tcp	Sun, Jul 18, 2021 12:15 PM UTC
DNS Server Detection (TCP)	0.0 (Log)	80 %	172.30.0.15		53/tcp	Sun, Jul 18, 2021 12:15 PM UTC

Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net

### Section 3: Challenge and Analysis

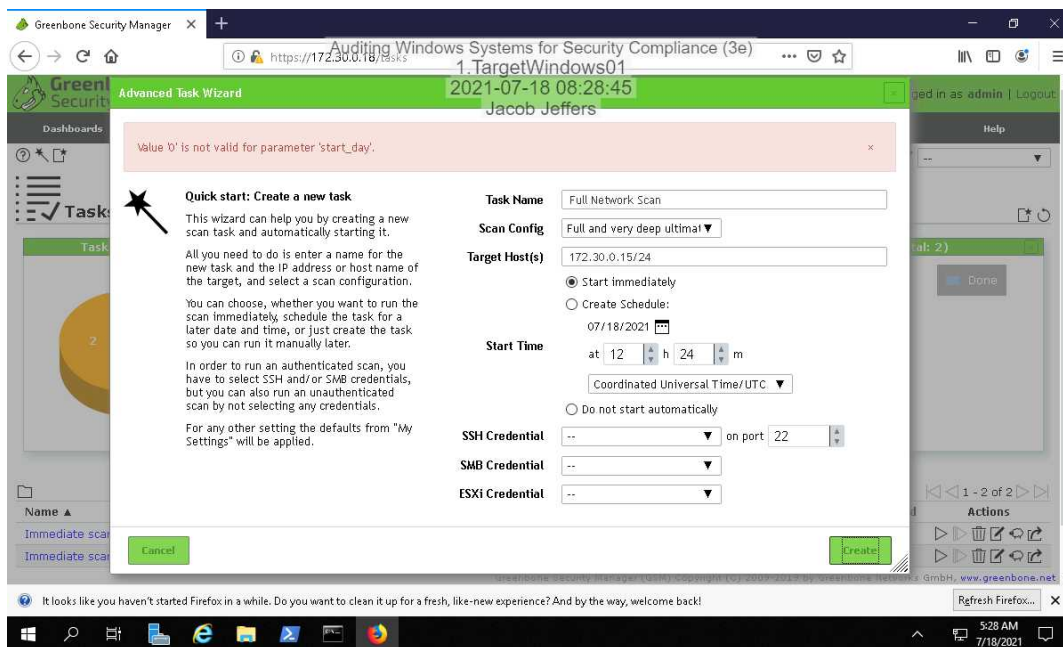
#### Part 1: Analysis and Discussion

In what context would you consider using the Microsoft Baseline Security Analyzer to conduct a security audit? Is it worth using MBSA at all, or are there similar, more effective tools that could be used in the same context? Use the Internet to research MBSA and alternative tools.

MBSA is a Microsoft-developed tool that performs a security audit of a Windows target and makes recommendations based on Microsoft's definitions. MBSA is a good tool to use in a tool box. An organization should never rely on a single product to audit their security. Utilizing many software would be the best option for performing a security audit.

#### Part 2: Tools and Commands

Make a screen capture showing the subnet scan results in the GSM.



#### Part 3: Challenge Exercise



**Make a screen capture** showing the **update confirmation** on **TargetWindows03**.

