Host Compliance Tutorial Using Greenbone OpenVAS and SCAP Compliance Checker

Zuzanna Wieczorek and Trevor Devries

November 2025
Version 1.0

Executive Summary

This tutorial provides a step-by-step guide to performing host compliance scanning in an air-gapped network using two complementary tools: Greenbone OpenVAS and the DISA SCAP Compliance Checker. You will assess Windows systems (Windows 11, Windows 10, and Windows 8 Legacy) using a combination of Greenbone Windows Local Security Checks (LSC), Security Updates scanning, and SCAP-based STIG baselines. You will analyze vulnerabilities, correlate Greenbone findings with STIG rules, remediate issues, and validate compliance through rescanning.

Contents

1 Objectives >

- Understand how to perform host compliance scanning in an air-gapped network.
- Learn how to use Greenbone/OpenVAS to identify weak points in Windows hosts.
- Learn how to run SCAP-based STIG compliance scans with the SCAP Compliance Checker.
- Correlate Greenbone findings with STIG rule failures to prioritize remediation.
- Apply remediation steps and validate fixes through rescanning with both tools across multiple Windows versions.

2 Hardware and Software Requirements <>

The tutorial was executed using the following environment:

1. A computer capable of hosting at least **4** virtual machines.
2. A virtualization software platform such as VMWare, VirtualBox, or Proxmox.
3. Virtual Machines:
   - Kali Linux VM (running the Greenbone/OpenVAS scanner; web UI reachable at **`https://<kali-ip>:9392`**).
   - Windows 11 Target (with SCAP Compliance Checker and DISA STIG content installed).
   - Windows 10 Target (scanned by Greenbone and SCAP).
4. All VMs connected to the same internal (host-only/air-gapped) network.

3 Verifying Necessary Files <>

This tutorial will require:

1. Access to all three Windows VMs (Win11, Win10, Win8).
2. Access to the Kali Linux VM with Greenbone/OpenVAS already configured and running.
3. SCAP Compliance Checker installed on Win11 with appropriate DISA STIG/SCAP content (XCCDF benchmarks).
4. (Optional) A location to export Greenbone and SCAP reports (shared folder or removable media).

1. Confirm you can log into each Windows VM with administrative credentials.
2. Ask your instructor for the current **<kali-ip>** and the location of STIG/SCAP content bundles.

4 Greenbone/OpenVAS and SCAP Overview <>

1. Greenbone/OpenVAS performs network-based vulnerability and compliance scanning against remote hosts.
2. It supports Windows Local Security Checks (LSC) and Windows Security Updates checks, using authenticated scans where possible.
3. The DISA SCAP Compliance Checker runs locally on Windows and evaluates systems against STIG baselines (XCCDF/CPE).
4. In this lab, Greenbone gives you broad vulnerability/compliance visibility, while SCAP provides official STIG rule pass/fail status on Win11.

5 When to Use Compliance Scanning <>

1. Before placing hosts into sensitive or production networks.
2. After major configuration changes or patch cycles.
3. When comparing default security posture between OS versions or images.
4. During regular security audits or accreditation, using both Greenbone (vulnerability/compliance) and SCAP (STIG-based compliance).

6 Task 1: Accessing Greenbone and Validating Connectivity <>

Machine: Win11 VM (client) and Kali (scanner, via IP)

1. On Win11, determine your own IP address using **`ipconfig`**.
2. Using the **`<kali-ip>`** provided by your instructor, verify basic connectivity with **`ping <kali-ip>`**.
3. On the Kali machine, type in the command **`sudo gvm-start`** to start GreenBone on Kali. The password is "kali".
4. Open a web browser on Win11 and navigate to **`https://<kali-ip>:9392`**.
5. Examine the browser's certificate/security warning and proceed to the site (for lab use).
6. Log in to the Greenbone web interface using the credentials provided.

Baby Steps:

1. On Win11, open Command Prompt and run **`ipconfig`**. Note your IPv4 address and subnet.
2. Run **`ping <kali-ip>`** and ensure you receive replies with non-zero TTL and no 100% packet loss.
3. Open Edge (or another browser), type **`https://<kali-ip>:9392`** into the address bar, and press Enter.
4. When a certificate warning appears, review the details (issuer, CN, validity dates), then choose the option to continue.

5. Enter the Greenbone username and password provided by your instructor and verify the dashboard loads.

7 Challenge 1: Independent Access from a Different Client <>

1. From the **Win10** VM, independently determine whether you can reach the Greenbone web interface.
2. Without reusing browser history from Win11, derive the correct URL and confirm the login page appears.
3. Verify you can successfully log in and reach the same Scan Configs page as in Task 1.
4. Document any differences in connectivity behavior between Win11 and Win10 (initial failures, latency, or DNS attempts).

Hints:

1. Use **`ipconfig`** and **`ping <kali-ip>`** on Win10 to confirm that it is on the same subnet and can reach Kali.
2. If the page does not load, try **`https://<kali-ip>`** first to identify basic HTTPS connectivity issues.
3. You should be able to reach the same dashboard using the same credentials as on Win11.

8 Task 2: Creating Basic Targets for Each Windows VM <>

Machines: Win11, Win10, Greenbone UI

1. On each Windows VM (Win11, Win10), use **`ipconfig`** to identify its IPv4 address.
2. From Win11, in the Greenbone web UI, go to **`Configuration → Targets`**.
3. Create a target named **Win11 Target** with only the Win11 IP address.
4. Create a target named **Win10 Target** with only the Win10 IP address.
5. Confirm that each target uses the correct IP and that there are no overlapping or incorrect ranges.

Baby Steps:

1. On Win11, Win10, open Command Prompt and run **`ipconfig`**. Write down each IPv4 address.
2. On Win11, return to the Greenbone dashboard in your browser.
3. Click **`Configuration → Targets`** and then **`New Target`**.
4. Type **Win11 Target** as the Name and enter the Win11 IP in the Hosts field; save the target.
5. Repeat the process to create **Win10 Target** and **Win8 Legacy Target** with their corresponding IP addresses.
6. Verify the target list shows three entries with distinct names and expected IP addresses.

9 Task 3: Creating a Mixed Compliance Scan in Greenbone <>

Machine: Greenbone UI (from Win11)

1. In the Greenbone web UI, go to **`Scans → Tasks`**.
2. Click **`New Task`**.
3. Name the task **Win11 LSC Compliance Scan**.
4. Set the Scan Config to **Full and Fast**.
5. Assign the **Win11 Target** to this task.
6. Start the task.

Baby Steps:

1. On Win11, in your browser, make sure you are logged into Greenbone.
2. Click on **`Scans → Tasks`**, then click **`New Task`**.
3. Name the task **Win11 LSC Compliance Scan**, choose the **Full and Fast** Scan Config, and select **Win11 Target**.
4. Save the task, then create a second task named **Win11 Security Updates Scan** using the **Full and Fast** config with the same target.
5. Start each task using the play icon and monitor the status until both read *Done* or *Completed*.

10 Challenge 3: Win 10 Compliance Scan <>

1. Independently create a new task named **Win 10 Compliance Scan** using the **Full and Fast** target from Challenge 2.
2. Select an appropriate Windows Local Security Checks Scan Config that will use authentication.
3. Configure the task so that it runs against The win10 machine.
4. Start the task and estimate how scan duration and number of checks change compared to the single-host Win11 LSC scan from Task 3.

Hints:

1. You should now be able to complete the entire task with only the Task 3 experience; no explicit "New Task" walkthrough is given here.

11 Task 4: Reviewing Win11 Greenbone Scan Results <>

Machine: Win11 VM (Greenbone UI in browser)

1. In Greenbone, navigate to **`Scans → Reports`**.
2. Open the report for the **Win11 Scan**.
3. Filter findings by **High** and **Medium** severity.
4. Identify any missing critical or important patches and note their CVEs.

Hints:

1. On Win11, click **`Scans → Reports`** and select the latest **Win11 Compliance Scan** report.
2. Use the filtering options to display High and Medium severity results.
3. For each selected issue, click to open its details and read the description and impact.
4. Choose three issues that mention remote access, privilege escalation, or credential theft and write down their names.
5. Return to the Reports list and open the **Win11 Scan**.
6. Identify any missing updates marked as critical or high and note at least one associated CVE.

12 Challenge 4: Independent Analysis on Win10<>

1. Using only your experience from Task 4, analyze the LSC and Security Updates reports for **Win10**.
2. Compare overall risk level between Win11 and Win10 based on your findings.

Hints:

1. The workflow is the same as in Task 4, but now you apply it to Win10 without explicit step-by-step guidance.
2. Pay attention to older protocols and weaker defaults that may still be present on Win10.
3. Support your comparison with concrete numbers (e.g., count of High vs Medium findings).

13 Task 5: Fixing One Vulnerability on Win11 <>

Machine: Win11 VM

1. Choose one High or Medium severity misconfiguration from the Win11 LSC report.
2. Read the detailed description and remediation section in Greenbone.
3. Apply the recommended configuration change on the Win11 host using Group Policy, Registry Editor, or Windows Settings.
4. Validate the change locally (for example, viewing the effective Group Policy value).
5. Record the setting's original and new values in your lab notes.

Baby Steps:

1. In the Win11 LSC report, click on a specific finding to open its details, then scroll to the remediation section.
2. Identify which local policy, registry key, or Windows feature must be changed.
3. On Win11, open the appropriate tool (e.g., **`gpedit.msc`**, **`regedit`**, or **`Windows Security`**).
4. Navigate to the exact path noted in the remediation and verify the current setting.
5. Change the setting to match the recommended secure configuration and apply the change.
6. Re-open the policy or registry key to confirm the new value is still present.

14 Challenge 5: Hardening a Different Host Independently <>

1. On **Win10**, Choose High or Medium severity misconfigurations from the LSC report.
2. Without step-by-step guidance, use the appropriate Windows tools to apply the suggested remediations.
3. Validate each change locally, then document which policies or keys were modified.

Hints:

1. Reuse the general approach from Task 5, but apply it to Win10.
2. Prioritize misconfigurations that affect remote access, authentication, or encryption rather than cosmetic issues.
3. Verify that your changes did not unintentionally break normal operations.

15 Task 6: Rescanning Win11 with Greenbone to Validate Fixes <>

Machine: Greenbone UI (from Win11)

1. In Greenbone, navigate to **`Scans → Tasks`**.
2. Re-run the **Win11 LSC Compliance Scan**.
3. Wait for the new scan to complete.
4. Open the new report and search for the vulnerability you fixed in Task 5.
5. Verify that its status has changed (for example, it is no longer reported or its severity is reduced).

Baby Steps:

1. In the Tasks list, identify **Win11 LSC Compliance Scan** and click the start/play icon to launch a new run.
2. Wait until the status shows as *Done* or *Completed*.
3. Go to **`Scans → Reports`** and open the most recent report for that task.
4. Use the search/filter box to locate the vulnerability by name or plugin ID.
5. Confirm whether it still appears and compare the result to the original report.

16 Challenge 6: Independent Rescan and Delta Analysis on Win10 <>

1. Independently re-run the LSC scan for the **Win10 Target** after completing Challenge 5.
2. Compare the new Win10 report with the original Win10 report you analyzed in Challenge 4.
3. Identify which findings disappeared or changed severity as a result of your remediation.
4. Summarize how much you improved Win10's risk posture (for example, number of High findings reduced).

Hints:

1. Create or reuse a dedicated Win10 LSC Task if one does not already exist; apply what you learned from Task 3.
2. Export both the original and new reports if that helps you compare counts and severities.
3. Focus on the specific items you remediated to prove that your changes had an effect.

17 Task 7: Running SCAP Compliance Checker on Win11 <>

Machine: Win11 VM

1. Launch the SCAP Compliance Checker on Win11.
2. Load the appropriate DISA Windows 11 STIG/SCAP benchmark (XCCDF content) from the provided content library.
3. Configure a local scan of the Win11 host using the selected benchmark.
4. Run the scan and wait for it to complete.
5. View the SCAP results and identify at least three failing STIG rules (rule IDs and titles).
6. Note whether any of these failed rules conceptually match misconfigurations you saw in Greenbone for Win11.

Baby Steps:

1. On Win11, open the Start Menu and search for "SCAP Compliance Checker" and launch it.
2. In the SCAP interface, use the option to install STIG/SCAP content and browse to the Windows 11 STIG benchmark bundle (.xml/.xccdf).
3. Choose your local system as the scan target and start the assessment.
4. Wait until the scan shows as complete, then open the results view.
5. Filter the results to show only failing/non-compliant rules.

18 Challenge 7: Explore SCAP Reporting and Export <>

1. Using only the SCAP Compliance Checker interface (no step-by-step walkthrough), explore the different views of the Win11 STIG results (e.g., by group, severity, or system component).
2. Export the SCAP results to at least one available format (for example, HTML, CSV, or ARF/XML), saving the file in your lab workspace.
3. Identify which exported format would be most useful for creating a management summary versus a technical remediation checklist.
4. Note how SCAP represents rule status (pass/fail/not applicable) and how this could support compliance documentation.

Hints:

1. Look for options in SCAP to group by severity or by STIG section—these help you prioritize what to fix first.
2. HTML exports work well for human-readable management summaries; CSV or XML/ARF are better for scripting and automation.
3. Pay close attention to how exceptions and "not applicable" rules are displayed; they are important in real-world audits.

19 Task 8: Remediating Win11 Based on SCAP STIG Rules <>

Machine: Win11 VM

1. Choose one failing STIG rule from the Win11 SCAP results that describes a configuration you can change (for example, password policy, audit policy, or a registry-based hardening setting).
2. Open the detailed description of that SCAP rule and review its STIG discussion and fix text.
3. On Win11, use Group Policy Editor, Registry Editor, or the relevant management console to apply the required STIG-compliant configuration.
4. Verify locally that the configuration matches the STIG requirement (for example, correct password length or audit flag).
5. Re-run the SCAP Compliance Checker scan on Win11 using the same STIG benchmark.
6. Confirm that the selected STIG rule now passes and record the before/after status.

Baby Steps:

1. In the SCAP results, pick a failing rule with clear fix instructions.
2. Note the exact policy path or registry key mentioned in the STIG rule.
3. On Win11, open **`gpedit.msc`** or **`regedit`** and navigate to the path given by the STIG.
4. Change the configuration to match the STIG-specified value (for example, minimum password length of 14 characters).

5. Re-run the SCAP scan and use the report view to verify that the rule's status changed from fail to pass.

20 Challenge 8: Independent SCAP Remediation Cycle <>

1. Independently select a **different** failing STIG rule on Win11 than the one you fixed in Task 9.
2. Without step-by-step instructions, interpret the STIG rule's requirement and fix text.
3. Apply the necessary configuration change on Win11 to bring that rule into compliance.
4. Re-run the SCAP scan and verify that the rule status changes from fail to pass.

Hints:

1. Avoid rules that require installing new software or domain-level policy; focus on local changes you can make in the lab.
2. If the rule still fails after your change, re-read the STIG text carefully—some requirements are more specific than they first appear.
3. Consider whether Greenbone had a similar or related finding; if both tools complain about the same area, that setting is clearly important.

21 Maintaining Compliance <>

1. Compliance is not a one-time activity; systems drift over time as settings change and patches are applied or missed.
2. Air-gapped environments must still regularly import and apply patches and updated STIG/SCAP content from trusted media.
3. Scheduled Greenbone scans and periodic SCAP STIG assessments together help detect new issues introduced by configuration changes.
4. In real environments, results from both tools feed into a formal Plan of Action and Milestones (POA&M) process.

22 Challenges in Host Hardening <>

1. Rapid OS update cycles and changing baselines.
2. Legacy systems lacking support for modern security controls.
3. Limited bandwidth or logistics for patching and content updates in air-gapped networks.
4. Keeping Greenbone content, SCAP/STIG benchmarks, and organizational policies aligned with current security requirements.

23 Conclusion <>

1. Greenbone/OpenVAS can effectively assess host vulnerabilities and misconfigurations across multiple Windows versions in an air-gapped lab.
2. The SCAP Compliance Checker adds STIG-based, host-level compliance verification for Windows systems and supports formal audits.
3. Using both tools together, along with remediation and rescanning loops, supports a strong, measurable, and auditable host compliance program.

24 Bonus Challenge: Achieve Maximum Compliance <>

1. Using what you learned from all tasks and challenges, create a short hardening checklist for one OS of your choice (Win11, Win10, or Win8).
2. Apply at least three additional remediations beyond those already performed and rescan with Greenbone.
3. If you chose Win11, run a follow-up SCAP Compliance Checker scan and note any rules that changed from fail to pass.
4. Reflect on which remediations gave you the strongest "return on investment" in terms of reduced findings and improved STIG status.

Hints:

1. Combine your Greenbone and SCAP observations to decide which changes to prioritize.
2. Consider documenting your checklist in a way that could be reused by another administrator or for a future lab.
3. Think in terms of defense-in-depth—passwords, logging, patching, and protocol hardening all work together.

Change Log:

Ver.	Date	Authors	Changes
v1.0	March 2025	Cory Clairmont & Sam Grant	First draft of tutorial.
v2.0	December 2025	Zuzanna Wieczorek & Trevor Devries	Major content and structure changes.

References

Greenbone Networks. *Greenbone/OpenVAS Documentation*. Available: `https://docs.greenbone.net` [Accessed: Oct. 2025].

Greenbone Networks. "OpenVAS – Open Vulnerability Assessment System." Available: `https://www.openvas.org` [Accessed: Oct. 2025].

Greenbone Networks. *Greenbone Vulnerability Management (GVM) Architecture*. Available: `https://docs.greenbone.net/GSM-Manual/gos-21.04/en/gvm_architecture.html` [Accessed: Oct. 2025].

Defense Information Systems Agency (DISA). *SCAP Compliance Checker (SCC) User Guide*. Available: `https://public.cyber.mil/stigs/scap` [Accessed: Oct. 2025].

Defense Information Systems Agency (DISA). *Security Technical Implementation Guides (STIGs)*. Available: `https://public.cyber.mil/stigs` [Accessed: Oct. 2025].

Souppaya, M., Scarfone, K., Orebaugh, A. *NIST Special Publication 800-126 Revision 3: The Technical Specification for the Security Content Automation Protocol (SCAP)*. National Institute of Standards and Technology, 2023.

National Institute of Standards and Technology. *Extensible Configuration Checklist Description Format (XCCDF)*. Available: `https://csrc.nist.gov/projects/scap/xccdf` [Accessed: Oct. 2025].

MITRE. *Open Vulnerability and Assessment Language (OVAL)*. Available: `https://oval.mitre.org` [Accessed: Oct. 2025].

GovReady PBC. "Understanding SCAP, XCCDF, OVAL, and Automated Compliance." Available: `https://www.govready.com/scap-overview` [Accessed: Oct. 2025].

Greenbone Networks. "Windows Local Security Checks (LSC) Overview." Available: `https://community.greenbone.net` [Accessed: Oct. 2025].