

Cyber Security and Digital
Forensics Internship

ASSIGNMENT 15

WINDOWS
PRIVILEGE
ESCALATION

SWASTIK GONDHI

DOON UNIVERSITY

Drive Link -

<https://drive.google.com/drive/folders/1WCK00ki1F3lFPT07y5tdSmeKcrDeWjvs?usp=sharing>

TRYHACKME ROOM 1

The screenshot shows the completion page for the 'Windows PrivEsc' room on TryHackMe. At the top, a browser tab shows the URL 'tryhackme.com/room/windows10privesc'. The main content area features a large green circular icon with a white checkmark. Below it, the text 'Congratulations on completing Windows PrivEsc!!!' is displayed. A row of five statistics boxes shows: 'Points earned 48', 'Completed tasks 18', 'Room type Walkthrough', 'Difficulty Medium', and 'Streak 1'. At the bottom, there are two buttons: 'Leave Feedback' and 'Continue'.

tryhackme.com/room/windows10privesc

Congratulations on completing Windows PrivEsc!!!

Points earned 48

Completed tasks 18

Room type Walkthrough

Difficulty Medium

Streak 1

Leave Feedback

Continue

The screenshot shows the details page for the 'Windows PrivEsc' room. The header includes the TryHackMe logo and navigation links: 'Dashboard', 'Learn', 'Compete', and 'Other'. A 'Go Premium' button is visible. The main content area has a dark background with a green circular icon and the text 'Windows PrivEsc'. Below this, it says 'Practice your Windows Privilege Escalation skills on an intentionally misconfigured Windows VM with multiple ways to get admin/SYSTEM! RDP is available. Credentials: user:password321'. The difficulty is 'Medium' and the estimated time is '75 min'. A row of buttons includes 'Share your achievement', 'Start AttackBox', 'Help', 'Save Room', '1391', and 'Options'. At the bottom, a green bar indicates 'Room completed (100%)'. Below this, a list of five tasks is shown, each with a green checkmark and a dropdown arrow.

TryHackMe

Dashboard Learn Compete Other

Access Machines

Go Premium

Learn » Windows PrivEsc

Windows PrivEsc

Practice your Windows Privilege Escalation skills on an intentionally misconfigured Windows VM with multiple ways to get admin/SYSTEM! RDP is available. Credentials: user:password321

Medium 75 min

Share your achievement

Start AttackBox

Help

Save Room

1391

Options

Room completed (100%)

Task 1 Deploy the Vulnerable Windows VM

Task 2 Generate a Reverse Shell Executable

Task 3 Service Exploits - Insecure Service Permissions

Task 4 Service Exploits - Unquoted Service Path

Task 5 Service Exploits - Weak Registry Permissions



