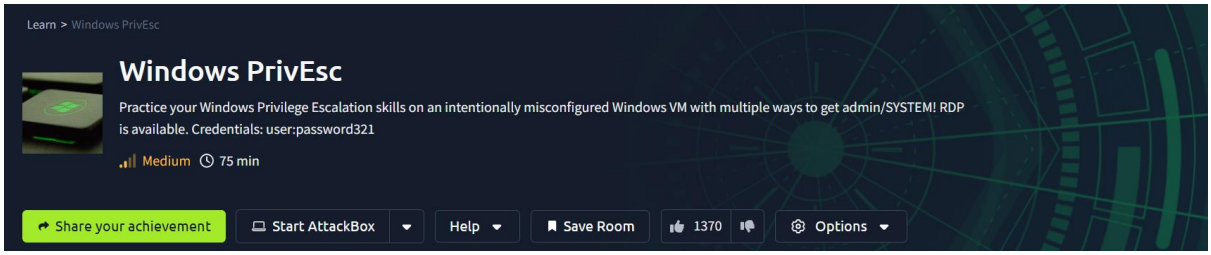

Task 1 Deploy the Vulnerable Windows VM

Task 2 Generate a Reverse Shell Executable

Task 3 Service Exploits - Insecure Service Permissions

What is the original BINARY_PATH_NAME of the daclsvc service?

C:\Program Files\DACL Service\daclservice.exe — ✓ Correct Answer

Task 4 Service Exploits - Unquoted Service Path

Answer the questions below

What is the BINARY_PATH_NAME of the unquotedsvc service?

C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe — ✓ Correct Answer

Task 5 Service Exploits - Weak Registry Permissions

Task 6 Service Exploits - Insecure Service Executables

Task 7 Registry - AutoRuns

Task 8 Registry - AlwaysInstallElevated

Task 9 Passwords - Registry

Answer the questions below

What was the admin password you found in the registry?

password123 — ✓ Correct Answer

Task 10 Passwords - Saved Creds

Task 11 Passwords - Security Account Manager (SAM)

Answer the questions below

What is the NTLM hash of the admin user?

a9fdfa038c4b75ebc76dc855dd74f0da — ✓ Correct Answer — Hint

Task 12 Passwords - Passing the Hash

Task 13 Scheduled Tasks

Task 14 Insecure GUI Apps

Task 15 Startup Apps

Task 16 Token Impersonation - Rogue Potato

Answer the questions below

Name one user privilege that allows this exploit to work.

SeImpersonatePrivilege ✓ Correct Answer Hint

Name the other user privilege that allows this exploit to work.

SeAssignPrimaryTokenPrivilege ✓ Correct Answer Hint

Task 17 Token Impersonation - PrintSpoofer

Task 18 Privilege Escalation Scripts