

07 - Nessus Vulnerability Scanner

Security Questions

1. describe how you would configure a username and password when testing an ftp service? There is a option in the credentials section of the scan settings.

The screenshot shows the 'Credentials' tab in the Nessus interface. On the left, there is a 'CATEGORIES' dropdown set to 'All' and a search bar labeled 'Filter Credentials'. Below this is a list of categories: Database, MongoDB (1), SSH, Windows, ADSI (5), and Palo Alto Networks PAN-OS (1). On the right, the 'FTP' service is selected. It shows fields for 'Username' (set to 'anonymous') and 'Password' (masked with dots).

2. describe how you would configure a domain when testing an Active Directory There is a option in the credentials section of the scan settings.

The screenshot shows the 'Credentials' tab in the Nessus interface. On the left, the 'CATEGORIES' dropdown is set to 'All', and the search bar contains 'window'. Below this is a list of categories: Windows. On the right, the 'Windows' service is selected. It shows fields for 'Authentication method' (set to 'Password'), 'Username' (set to 'administrator'), 'Password' (masked with dots), and 'Domain' (empty). Below these fields is a section titled 'Global Credential Settings' with four checkboxes: 'Never send credentials in the clear' (checked), 'Do not use NTLMv1 authentication' (checked), 'Start the Remote Registry service during the scan' (unchecked), and 'Enable administrative shares during the scan' (unchecked).

3. describe how you would configure the portscan prior the vulnerability scan
I would scan the from 0 to 49151 for a single host, enable UDP Scan, Scan Network Printers and Novell Netware Hosts.
4. is is possible to run a brute-force attack against an ssh service? Yes, there is a Plugin Hydra that provide provides more option for the scans.
https://docs.tenable.com/tenable/c/5_8/Content/CustomScanPolicyOptions.htm?Highlight=hash#Brute

