

Exercise Nessus Vulnerability Scanner

1. Task description

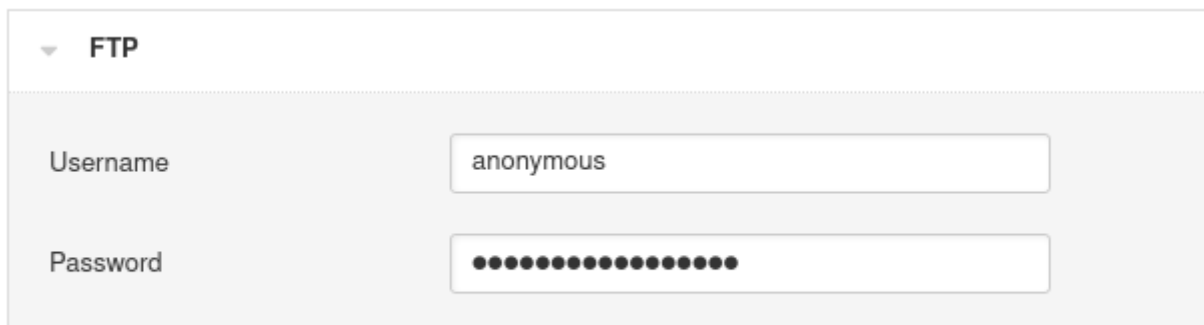
Nessus is a powerful network & vulnerability scanner developed by Tenable, Inc.. In this challenge, you will get access to an instance of Nessus running in the Hacking Lab environment.

After learning howto import a previous scan in nessus, you did learn howto perform your own scan against a target. Please answer the following questions:

1. Describe how you would configure a username and password when testing an ftp service?
2. Describe how you would configure a domain when testing an Active Directory
3. Describe how you would configure the portscan prior the vulnerability scan
4. Is is possible to run a brute-force attack against an ssh service?

2. Answers

1. I would test if anonymous login is allowed. When you perform a new scan with nessus, you'll find a template for that under credentials.



The image shows a screenshot of the Nessus interface for configuring an FTP service. At the top, there is a dropdown menu labeled 'FTP'. Below it, there are two input fields: 'Username' and 'Password'. The 'Username' field contains the text 'anonymous'. The 'Password' field is filled with a series of black dots, indicating that the password is hidden.

2. Under credentials there is also a template for windows. Here you can enter your active directory credentials.

▼ **Windows**

Authentication method	<input type="text" value="Password"/>
Username	<input type="text" value="administrator"/> <small>REQUIRED</small>
Password	<input type="password"/> <small>REQUIRED</small>
Domain	<input type="text"/>

3. I'd use the default SYN Scan with soft detection enabled.

SYN

Override automatic firewall detection

Use soft detection

Use aggressive detection

Disable detection

4. I didn't find any option for that. By default setting it's not possible, but it works if hydra is installed on the same system.

New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings [Credentials](#) [Compliance](#) [Plugins](#)

BASIC >

DISCOVERY >

ASSESSMENT ▾

- [General](#)
- [Brute Force](#)
- [Web Applications](#)
- [Windows](#)
- [Malware](#)

REPORT >

ADVANCED >

General Settings

Only use credentials provided by the user
Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.

Oracle Database

Test default accounts (slow)

Brute Force Options

The Brute Force tab specifies how the scanner tests for information against SCADA systems.

Additionally, if Hydra is installed on the same host as a Nessus server linked to SecurityCenter, the Hydra section will be enabled. Hydra extends brute force login testing for the following services: Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, S7-300, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.