Eccles Vulnerability Scanning Lab

(Difficulty: MODERATE)

> The intent of this lab is for you to work with common software used by the majority of companies in industry. There will NOT be step-by-step instructions, as you are responsible to figure this out like you would in the real-world. Google is your friend that can help you on this assignment.

📖

Prereading

It is recommended that you read the following articles before beginning. Additional research may be necessary if you run into problems.

- https://en.wikipedia.org/wiki/Nessus_(software)
- https://docs.tenable.com/nessus/Content/Scans.htm (link is to a newer version, but the concepts are the same)

📜 Supplemental Reading

This reading is not required but may give you a deeper understanding of the material (link below is to a newer version, but the concepts are the same).

- https://docs.tenable.com/nessus/10_7/Content/PDF/Nessus_10_7.pdf

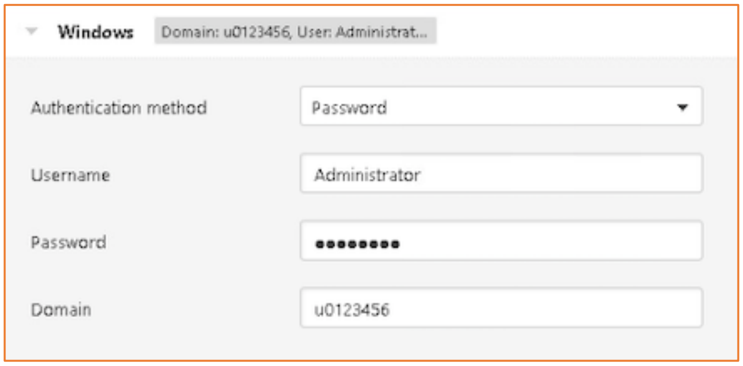
📖 Lab Objective

Configure a vulnerability scanner and scan Windows computers on a domain for missing updates, misconfigurations and malware.

📃 Outline

1. Make a reservation for **4 hours**. It likely will not take this time, but if you do not get the correct scan results you will have to troubleshoot and/or rebuild and rescan, which can take more time than you would expect.
2. Review the **Setup** instructions at the bottom of this document.
3. Logon **CLIENT-01** (click the "Desktop Client" button in the NETLAB UI) using the local administrator account ("Desktop-User")
4. **Rename CLIENT-01** to CLIENT-UNID (i.e., CLIENT-your University ID) (e.g., CLIENT-u0123456). If you don't do this, you will get a zero for the assignment! *HINT: Do this from the Control Panel on CLIENT-01.*

5. Disable the **Windows Defender Firewall with Advanced Security** for the Domain and Private Profiles on *all three computers.*
    1. Do this by modifying the Default Domain Policy on DC1 using the Group Policy Management Editor. Be sure to run “gpupdate” manually on all three computers, otherwise you will have to wait a longtime.
    2. **Reflection Question:** Why did you disable the Windows Defender Firewall on all three computers?
    3. **Reflection Question:** What other (more complex) configuration change could you have made in lieu of disabling the Windows Defender Firewall on all three computers?
6. Logon SERVER-01 (click the “Member Server” button in the NETLAB UI) using the Domain Administrator account (“U0123456\Administrator”)
7. Login to Nessus (using the Bookmark in FireFox) using the credentials below. Give it a few minutes to load and ignore any errors about being out of date (it is out of date, as the lab is not connected to the Internet, but that is OK for what you are doing).
8. Configure Nessus Essentials to scan as follows:
    1. Create and run a scan called **Host Discovery scan** that includes *DNS name resolution* AND *fingerprints the operating system* (will run for 5-15 minutes).
        1. Scan 192.168.42.1 and 192.168.42.50-192.168.42.55
        2. **Reflection Question:** Why did you NOT scan the entire subnet of 192.168.42.0/24?
        3. **Reflection Question:** If ICMP responses (ping responses) had been disabled on all three computers would the scan have still found the computers?
    2. Create and run a scan called **Host Advanced Scan** (using the Advanced Scan template) that includes *DNS name resolution* (will run for 15-30 minutes).
        1. Scan 192.168.42.1 and 192.168.42.50-192.168.42.55
        2. Use the **Domain Admin** account as Windows credentials for the scan and enable ALL “global Credential Settings”
            1. Here is the **proper format** (do NOT use "u0123456.corp\Administrator" or "u0123456\Administrator" for the username….it won’t work):



Windows Domain: u0123456, User: Administrat...

Authentication method	Password ▾
Username	Administrator
Password	••••••••
Domain	u0123456

            2. **Reflection Question:** Why did you have to enter Domain Administrator credentials to run this advanced scan?

        3. **Reflection Question:** How would the scan results have changed if you had used only the CLIENT-u0123456 local administrator account credentials (specifically, the **Desktop-User** account)?

    3. Enable **Malware Detection**

9. Gather screenshots for the assignment submission as outlined in the Assignment in Canvas.
10. The lab is complete, click “End Reservation Now” to free up resources for others.

🛠️ Setup

🧪 Virtual Machines

- DC1 (NETLAB label: “DC Server”)
- SERVER-01 (NETLAB label: “Member Server”)
- CLIENT-01 (NETLAB label: “Desktop Client”)

🔗 Active Directory Domain

- u0123456.corp

🔑 Active Directory Accounts

- **Domain Admin**
    - Username: u0123456.corp\Administrator
    - Password: dcAdmin01
- **Secondary Domain Admin**
    - Username: SysAdmin
    - Password: Lockdown$Admin1
- **Domain User (if needed)**
    - Username: u0123456.corp\bgates
    - Password: Changeme! (the first time you use this account you will be prompted to change your password! Write it down!)

🖥️ CLIENT-10 Local Admin Account

- Username: .\Desktop-User
- Password: desktop01

🔑 Nessus Accounts (open FireFox and it will load the login page)

- Username: admin

- Password: admin