


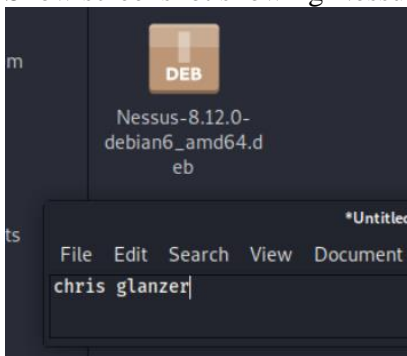
# Lab 6 – Nessus

---

## Part I. Nessus Scan

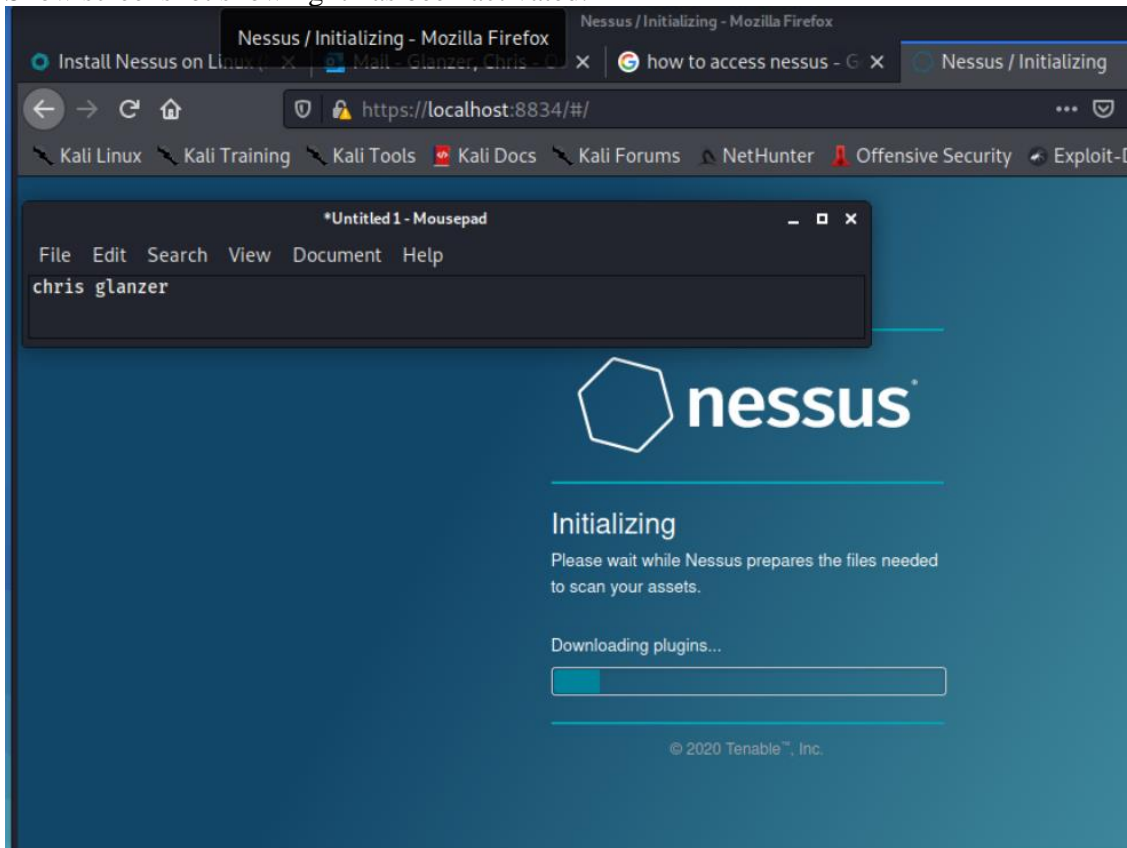
*Make sure you are watching the lectures, as they provide information you may need to complete this task. Please Provide the screenshots indicated. **Your name** must be seen somewhere in the background for each. A small terminal screen open is fine. Please be sure to crop screenshots appropriately and produce readable screenshots that can be read without zooming in; other screenshots that do not meet this requirement **will not receive points**.*

- Install Nessus scan in Linux.
- Show screenshot showing Nessus is installed in Kali. 

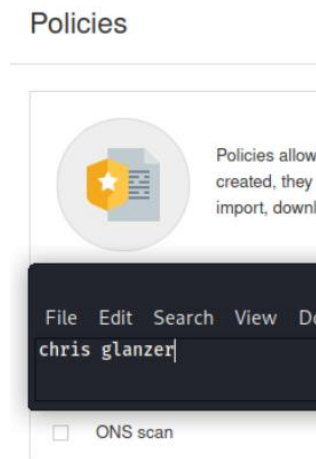



- Obtain community key to register Nessus as home user.  
The only readily apparent programs were the pro free trial and the essentials for educators and students... so I went with the essentials key. Didn't see anything about home users – hopefully that's all good

- Show screenshot showing it has been activated. 



Creating policy 



- The Report, showing the number of vulnerabilities found. 

ONS scan

[Back to My Scans](#)

Hosts 1

Vulnerabilities 76

History 2

Filter

Search Vulnerabilities

76 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	3
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	NFS Exported Share Information Disclos...	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
MIXED	5 DNS (Multiple Issues)	DNS	6
MIXED	5 ISC Bind (Multiple Issues)	DNS	5

Scan Details

Policy:

ONS scan

Status:

Running

Scanner:

Local Scanner

Start:

Today at 6:02 PM

Vulnerabilities

\*Untitled1 - Mousepad

File Edit Search View Document Help

chris glanzers

## Part II. Understanding Vulnerabilities

Answer the following questions:

1. Select one of the critical severity vulnerabilities reported by Nessus and enter all of the items in the list above. For item 4, other vulnerability identifiers, only list CVE identifiers if available; otherwise, list only the first other identifier reported.
2. Select one that is not critical severity that you think could be promising. Enter all of the items in the list above. For item 4, other vulnerability identifiers, only list CVE identifiers if available; otherwise, list only the first other identifier reported.

Click on the first vulnerability of critical severity to see the details Nessus reported about the vulnerability. Each vulnerability has multiple attributes, the most important of which are the following:

1. Nessus plugin ID number: 32321
2. Nessus plugin name: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check).
3. CVE-2008-0166
4. CVSS base score: 10
5. Exploit available: True
6. Exploitable with: Core Impact
7. Nessus plugin ID number: 10205
8. Nessus plugin name: rlogin Service Detection
9. CVE-1999-0651
10. CVSS base score: 7.5
11. Exploit available: true
12. Exploitable with: metasploite (rlogin authentication scanner)

## Deliverables

These MUST be contained all in one PDF or DOC/DOCX.

You may select **two questions** to skip if you so desire.