

LAB (8): Reconnaissance and Scanning

Hamzah Al-Alami (32015334503)

Ayham Al-Hindi (31915179075)

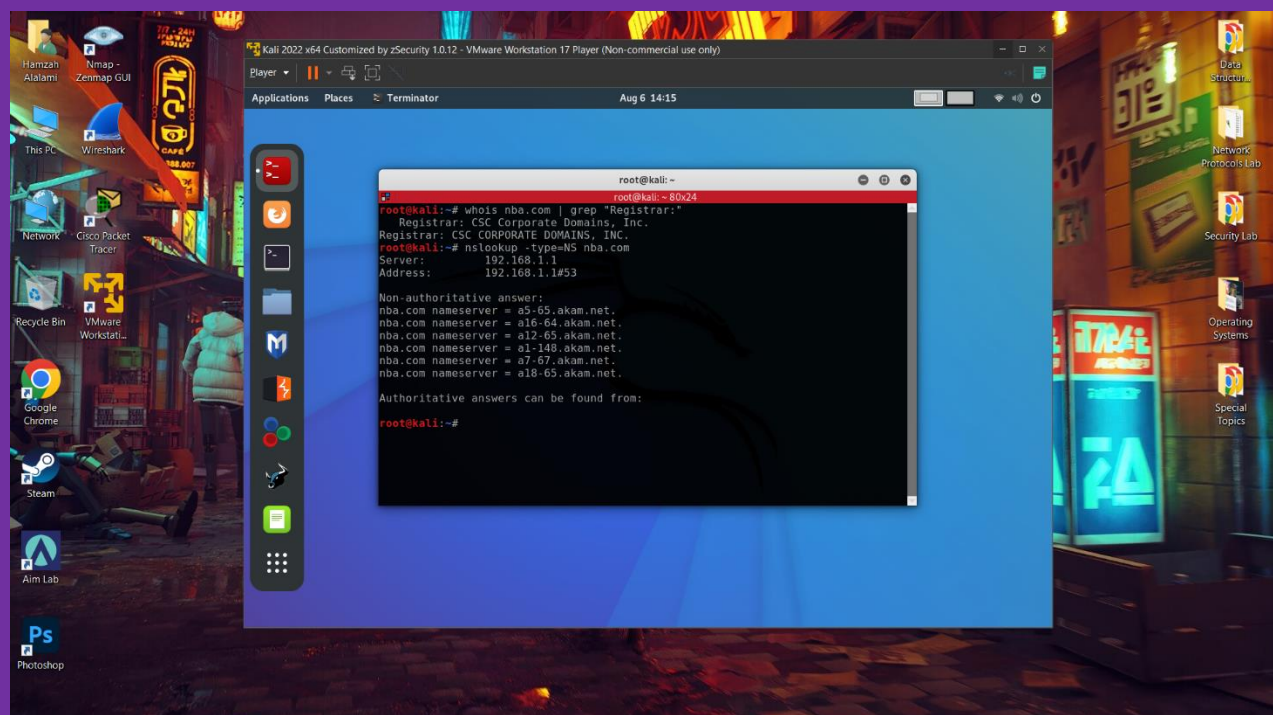
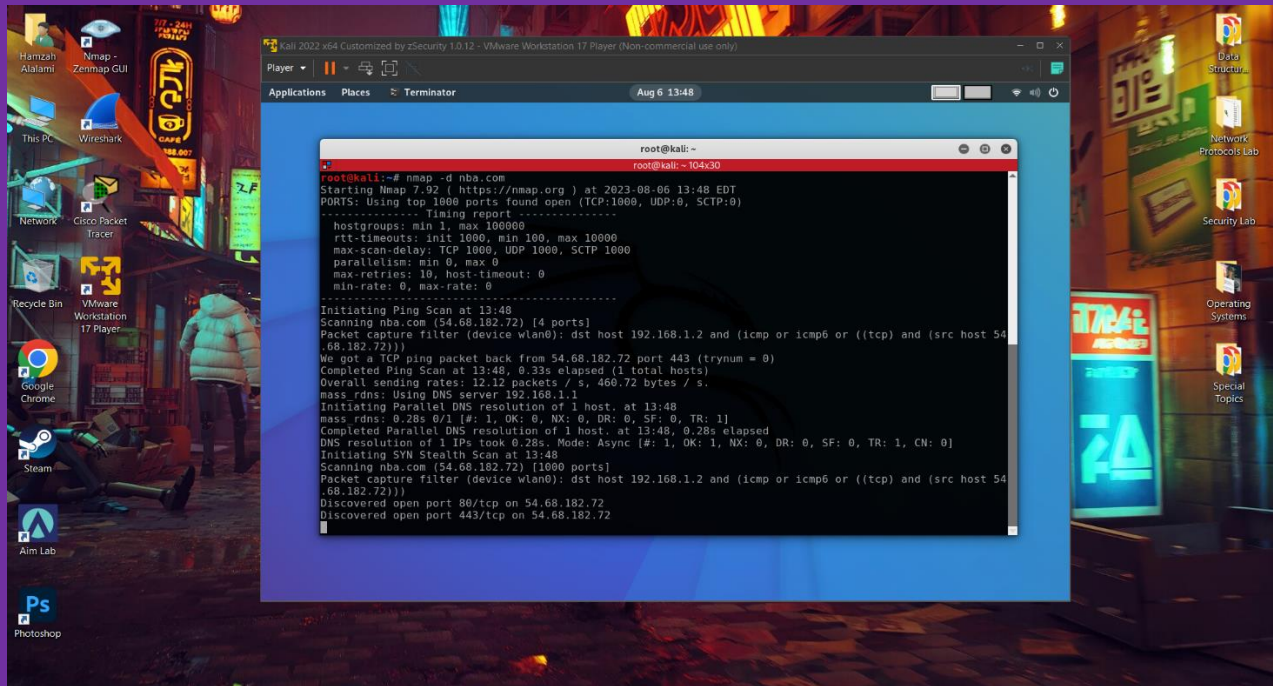
Taha Hadib (31915179032)

Date: 6/8/2023 (Summer Semester)

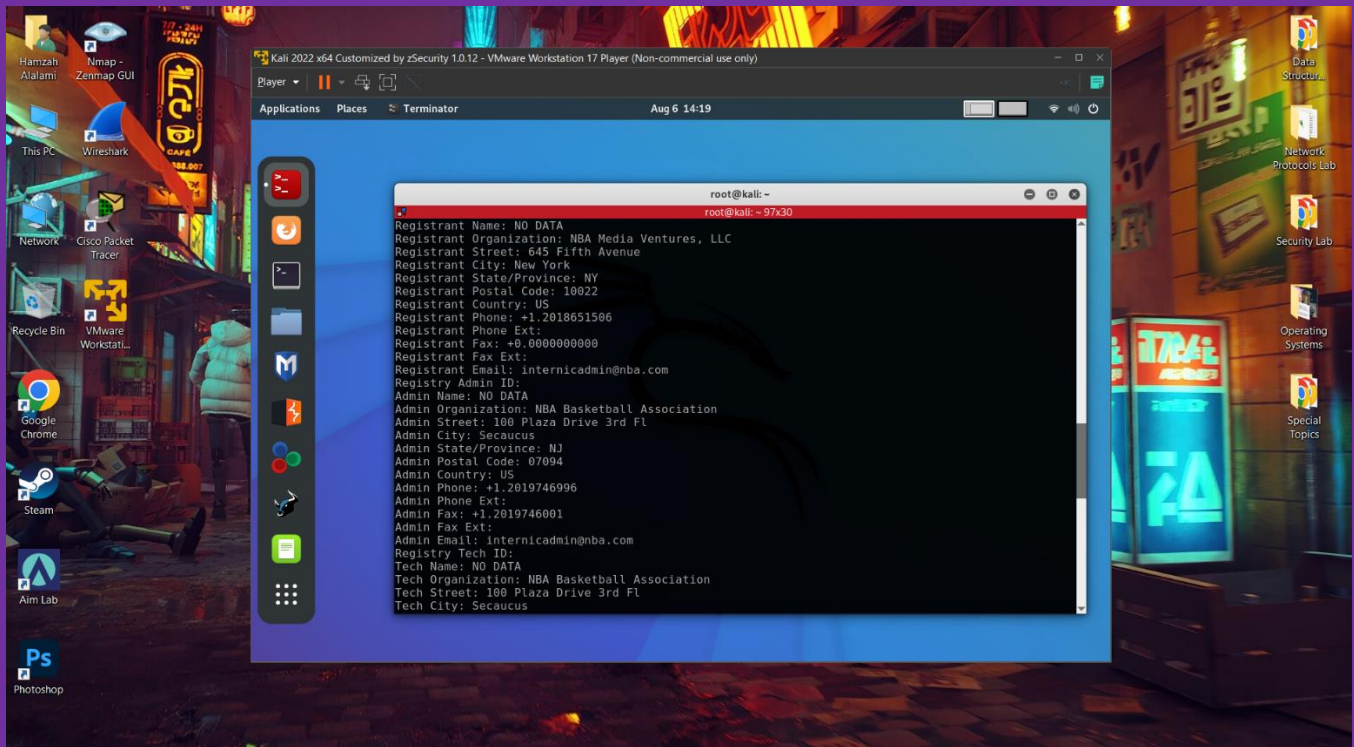
Objective: learn spying and scanning methods used to protect computer systems. exploring various ways to gather information and find weaknesses in computer systems.

Question (1) asked us to gather info about the domain's registrar name and provide the list of authoritative DNS name servers from nba.com

we used N-map in Linux to gather this info using these commands.



It also asked us to the domain's admin name and, address and phone number, we gathered them using WHOIS lookup, which is a protocol that provides information about domain registration, including administrative contact details.



Meanwhile in Q2, it asked us to use google hacking techniques to o do information gathering about the domain “ist.ucf.edu”, list of word files that contain keyword “phone” and Find the PDF files in IST that contains “security”.

Here are the search phrases that we used to do that:

The image displays two screenshots of Google search results, demonstrating Google Hacking techniques. The first screenshot shows a search for PDF files on ist.ucf.edu containing the keyword 'security'. The search query is 'ist.ucf.edu filetype:pdf intext:security'. The results show two PDF files from the University of Central Florida: 'Usable Security & Privacy - UCF Modeling and Simulation' and 'Course Syllabus IDC 6602 Usable Cybersecurity & Privacy'. The second screenshot shows a search for document files on ist.ucf.edu containing the keyword 'phone'. The search query is 'ist.ucf.edu filetype:doc intext:phone'. The results show a document from the Simulation Interoperability Standards Organization titled 'Call for Papers', which includes contact information for Pat Burgess.

Search 1: PDF files containing 'security' on ist.ucf.edu

Search query: `ist.ucf.edu filetype:pdf intext:security`

About 739 results (0.37 seconds)

University of Central Florida
<https://msgrad.ist.ucf.edu/LinkClick.aspx?LinkClickID=1&LinkClickName=Usable+Security+Privacy+UCF+Modeling+and+Simulation> PDF

Usable Security & Privacy - UCF Modeling and Simulation
The course introduces usability problems in security and privacy methods, tools, and software and overviews prominent examples of both failures and successes in ...

University of Central Florida
<https://msgrad.ist.ucf.edu/Portals/Files/Syllabus/IDC%206602%20Usable%20Cybersecurity%20and%20Privacy.pdf> PDF

Course Syllabus IDC 6602 Usable Cybersecurity & Privacy
The course introduces usability problems in security and privacy methods, tools, and software and overviews prominent examples of both failures and ...

Search 2: Document files containing 'phone' on ist.ucf.edu

Search query: `ist.ucf.edu filetype:doc intext:phone`

About 4 results (0.22 seconds)

Simulation Interoperability Standards Organization
<https://www.sisostds.org/DigitalLibrary/Call%20for%20Papers.pdf> DOC

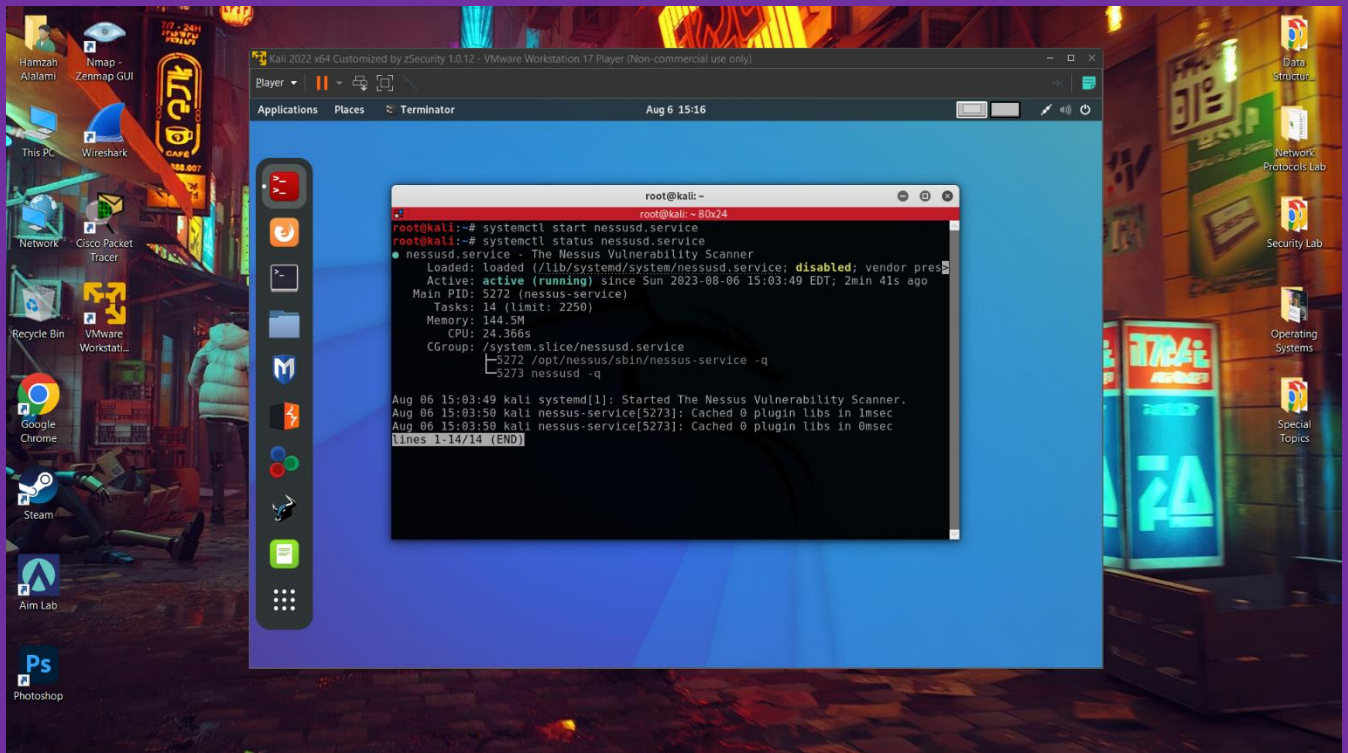
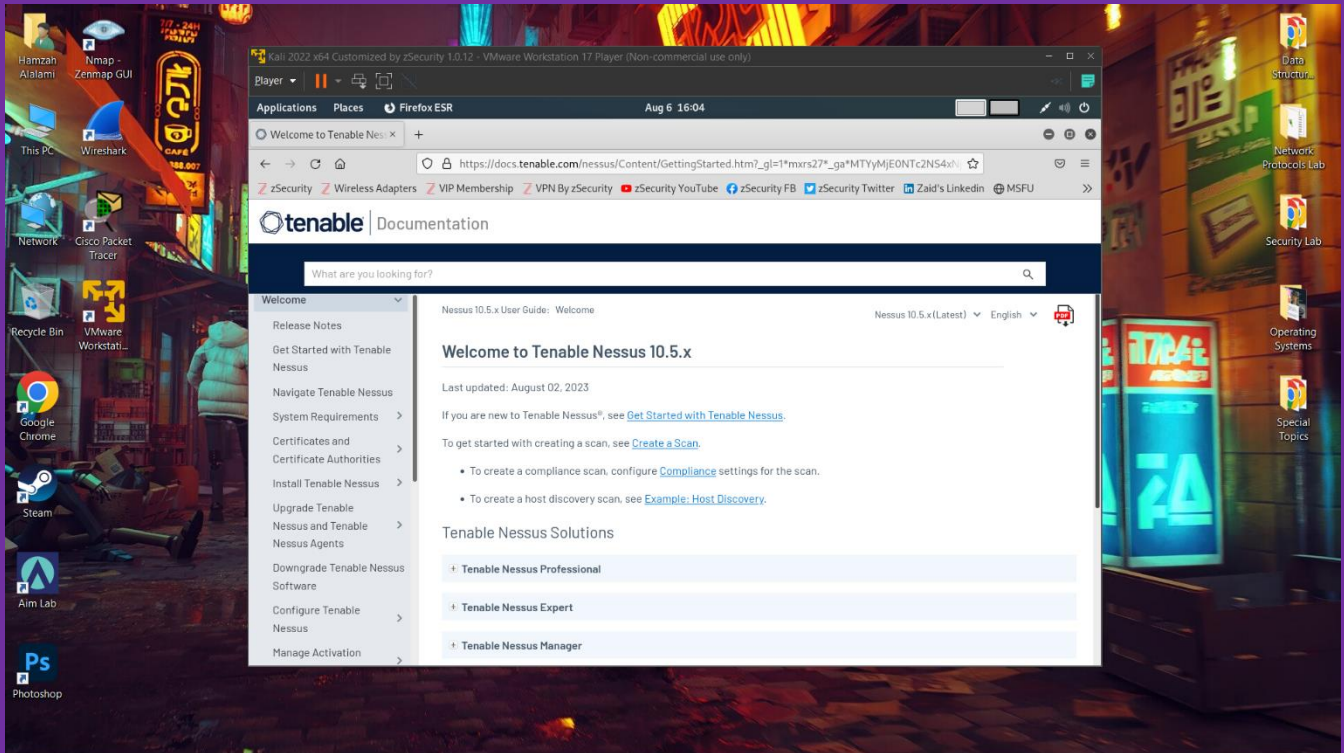
Call for Papers
If you have any problems or are unable to submit to the web site, please contact Pat Burgess
<pburgess@ist.ucf.edu>, phone: 407-882-1372, fax: 407-658-5059.

<https://www.sisostds.org/DigitalLibrary/ANNOUNCEMENT%20AND%20PRELIMINARY%20CALL%20FOR%20PAPERS.pdf> DOC

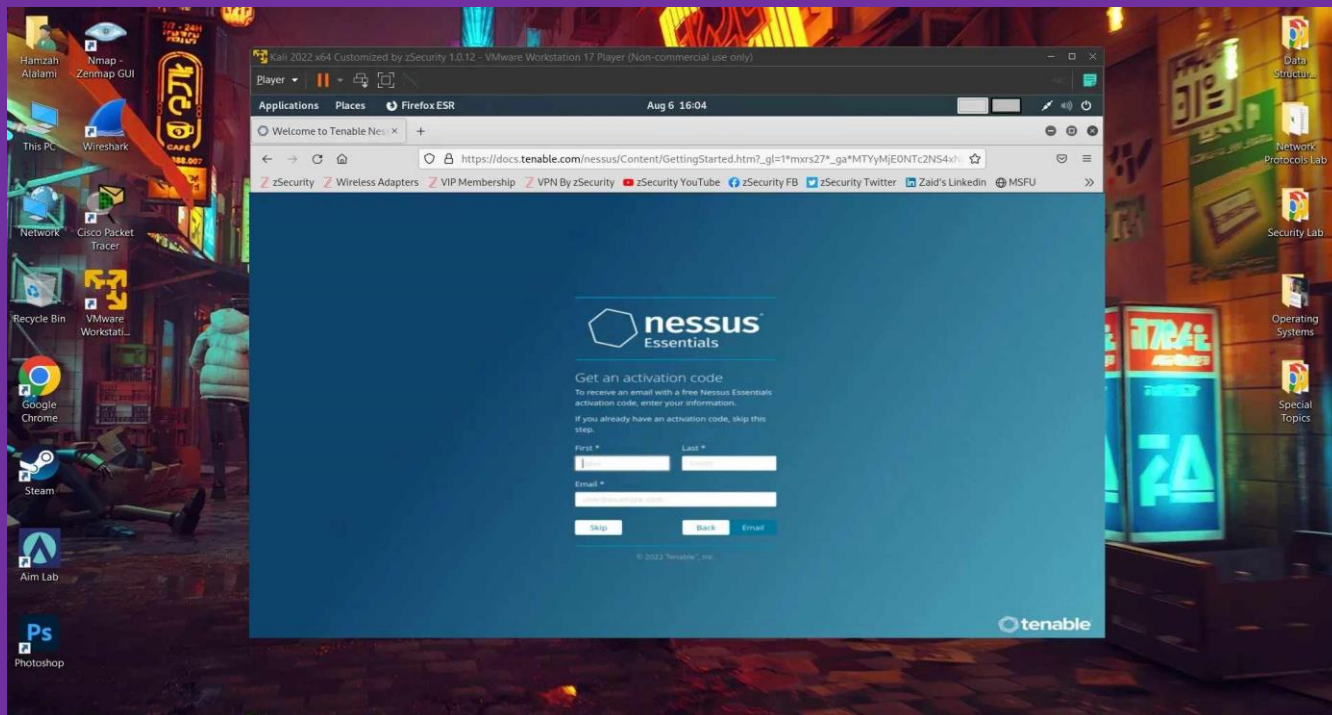
ANNOUNCEMENT AND PRELIMINARY CALL FOR PAPERS
If you have any problems or are unable to submit to the web site, please contact Pat Burgess
<pburgess@ist.ucf.edu>, phone: 407-882-1372,.

Command and Control Research Portal

Q3 was about downloading and installing Nessus on our system and to show the Nessus login interface, then to run network scan to scan our Metasploitable Linux VM.



According to the report, it would be OK if we found less than 10 critical vulnerabilities, which we did.



Aggressive Scan / 10.0.2.4

[Back to Hosts](#)

[Configure](#)

[Audit Trail](#)

[Launch](#)

[Report](#)

[Export](#)

Vulnerabilities 57

Filter

Search Vulnerabilities

57 Vulnerabilities

<input type="checkbox"/>	Sev	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	Bind Shell Backdoor Detection	Backdoors	1		
<input type="checkbox"/>	CRITICAL	NFS Exported Share Informatio...	RPC	1		
<input type="checkbox"/>	CRITICAL	rexecd Service Detection	Service detection	1		
<input type="checkbox"/>	CRITICAL	Unix Operating System Unsupp...	General	1		
<input type="checkbox"/>	CRITICAL	UnrealIRCd Backdoor Detection	Backdoors	1		
<input type="checkbox"/>	MIXED	4 Web Server (Multiple Issues)	Web Servers	5		
<input type="checkbox"/>	MIXED	4 ISC Bind (Multiple Issues)	DNS	4		
<input type="checkbox"/>	HIGH	rlogin Service Detection	Service detection	1		
<input type="checkbox"/>	MIXED	4 HTTP (Multiple Issues)	Web Servers	7		
<input type="checkbox"/>	MIXED	4 DNS (Multiple Issues)	DNS	5		
<input type="checkbox"/>	MIXED	2 Apache Tomcat (Multiple I...	Web Servers	2		
<input type="checkbox"/>	MEDIUM	NFS Shares World Readable	RPC	1		

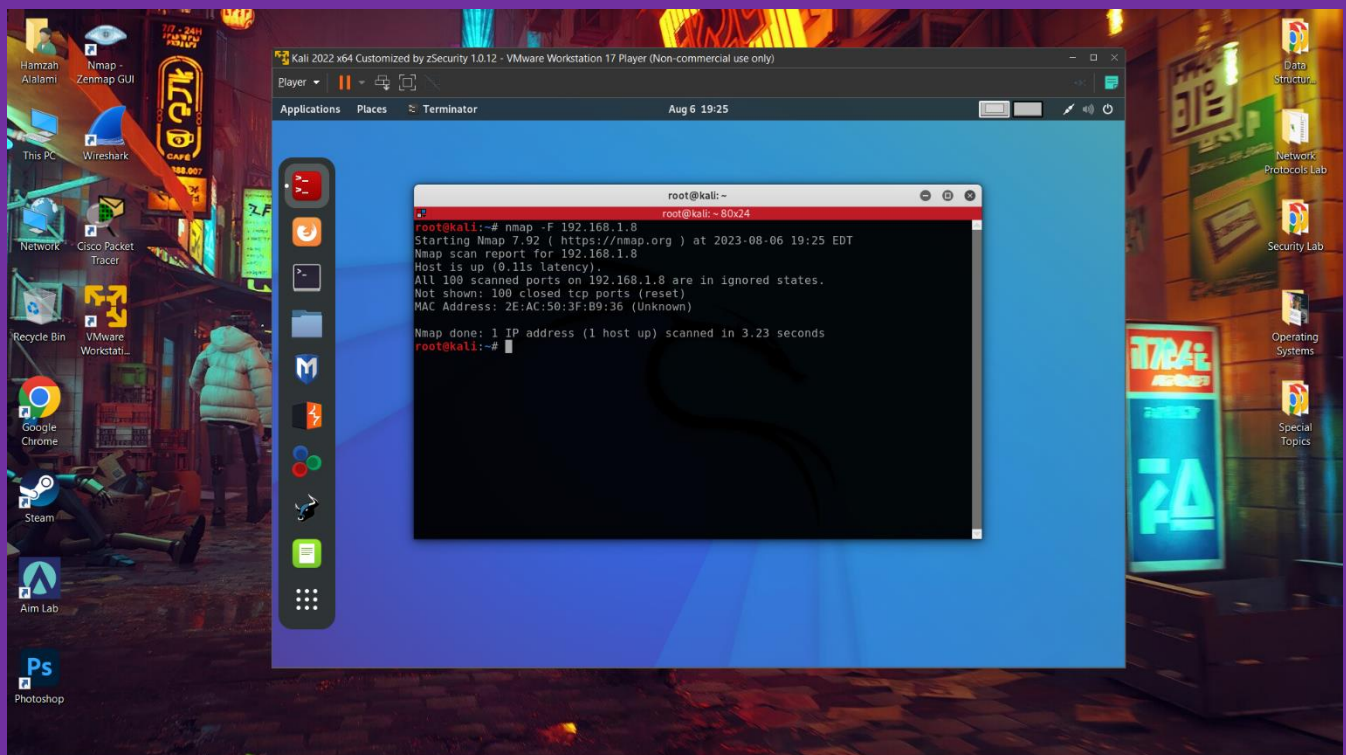
Host Details

IP: 10.0.2.4
MAC: 08:00:27:A7:4E:80
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Start: Today at 9:35 PM
End: Today at 9:49 PM
Elapsed: 14 minutes
KB: [Download](#)

Vulnerabilities



Finally, in Q4, we were asked to conduct standard fast scan to scan our Metasploitable Linux VM. In order to discover standard service opened on the Metasploitable Linux VM.



Abstract

we explored various cybersecurity techniques such as internet information gathering, Google hacking, Nessus vulnerability scanning, and Nmap scanning. The practical exercises helped us to discover domain registrar details, find files with specific keywords, perform network scans, and identify open services.