**Industrial Control Systems**

**Cybersecurity (300) Training**

Learning Objectives

At the completion of this course, participants will be able to:

LO1: Describe basic industrial control systems

LO2: Discuss cyber risks to industrial control systems

LO3: Discuss a process control exploit

LO4: Employ passive discovery

LO5: Employ active discovery

LO6: Develop the requirements to manage cybersecurity risk

LO7: Develop safeguards to ensure delivery of critical infrastructure services

LO8: Identify a cybersecurity event

LO9: Execute activities taken during and after a cybersecurity event

LO10: Recognize current trends

LO11: Discuss the three main stages of an attack

LO12: Describe Metasploit

LO13: Use Metasploit Framework

LO14: Discuss basic web hacking techniques

LO15: Describe password security

LO16: Discuss basic wireless hacking techniques

LO17: Define Zero Trust

LO18: Discuss the Zero Trust Material Model

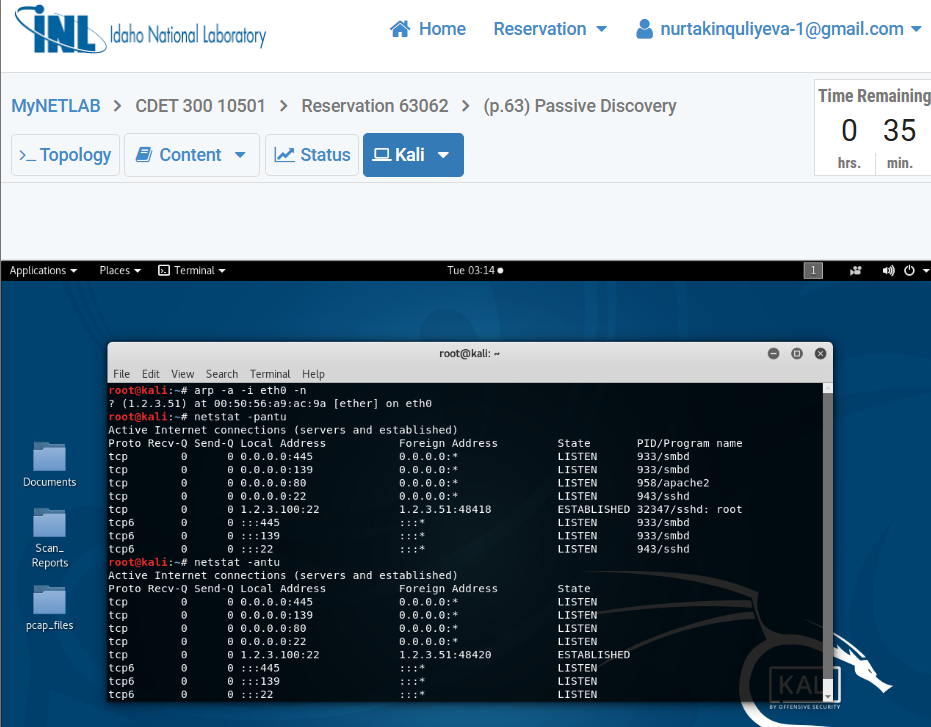
LO19: Describe how Zero Trust principles can be applied to an ICS/OT Network

1)· arp → ARP cədvəlini göstərir və ya idarə edir.

· -a → Bütün ARP qeydlərini siyahıya alır.

· -i eth0 → Yalnız **eth0** şəbəkə interfeysinə aid olan qeydləri göstərir.

· -n → IP ünvanlarını adlara çevirmədən (DNS sorğusu etmədən) rəqəmsal formada göstərir.



2)netstat -pantu əmri Linux sistemlərində **aktiv şəbəkə bağlantılarını və açıq portları** göstərmək üçün istifadə olunur.

-p → Həmin bağlantını istifadə edən proqramın **PID (Process ID)** və adını göstərir

-a → Bütün socket-ləri göstərir (həm aktiv, həm də listening olanlar)

-n → IP və portları adlara çevirmədən (DNS etmədən) rəqəmsal göstərir

-t → TCP bağlantıları göstərir

-u → UDP bağlantıları göstərir

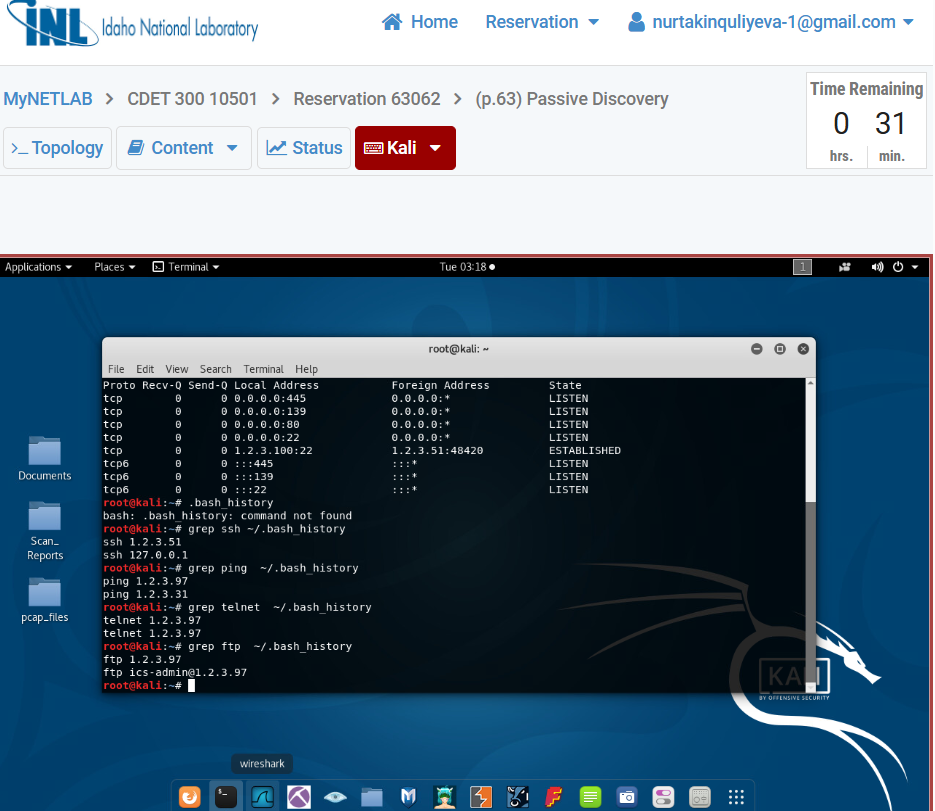
1. grep əmri vasitəsilə bash\_history də ssh,ping telnet əmrilərinin axtarışı

4). FTP connections are another example of past activity that we could look for.

grep ftp ~/.bash\_history

Commands can also contain interesting information such as usernames. Did you find any? If so, list them below as part of your passive collection of information!

Ftp axtardığımız zaman iki nəticə alırıq. ftp 1.2.3.97 / ftp ics.admin@1.2.3.97

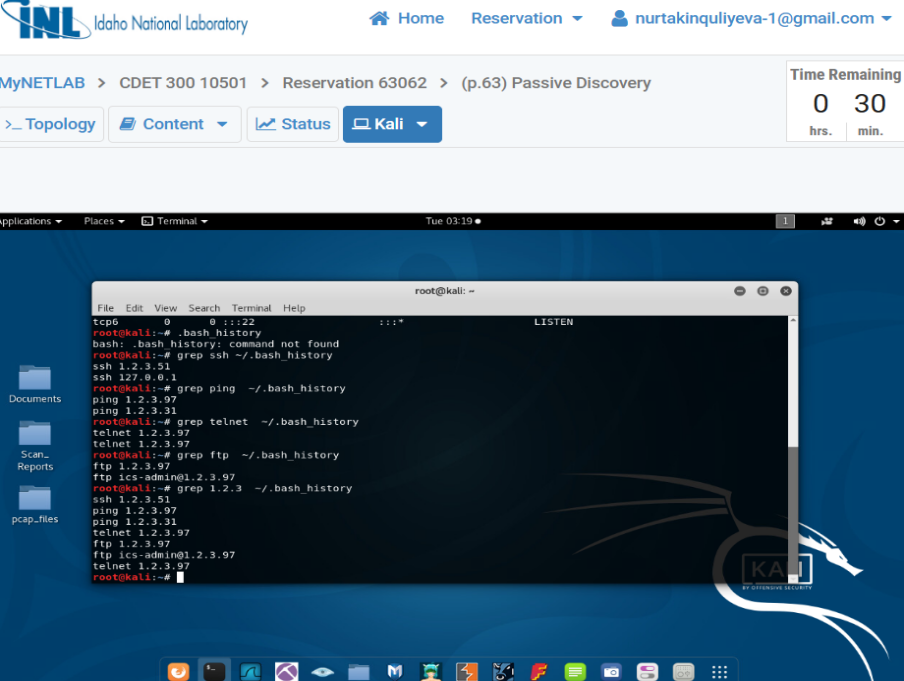


5)At this point, you may have taken an interest in the 1.2.3.0/24 IP network. Perhaps you would

like to see all commands that included the text “1.2.3.” to attempt searching for related IP

addresses. These are the first 3 octets matching that IP network. Find any command that may

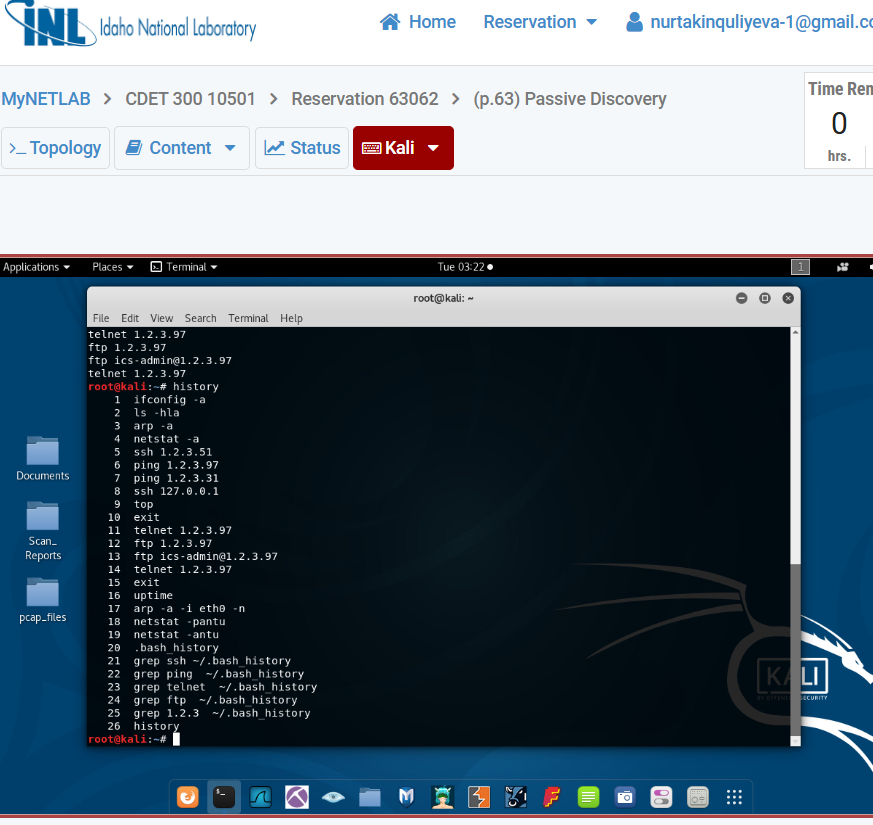
have used them and list them below.



Nəticə olaraq görə bilərik ki, ssh,ping,telnet,ftp əmrləri istifadə olunmuşdur.

7. Then start a new command shell and use the history command. You will now see all the

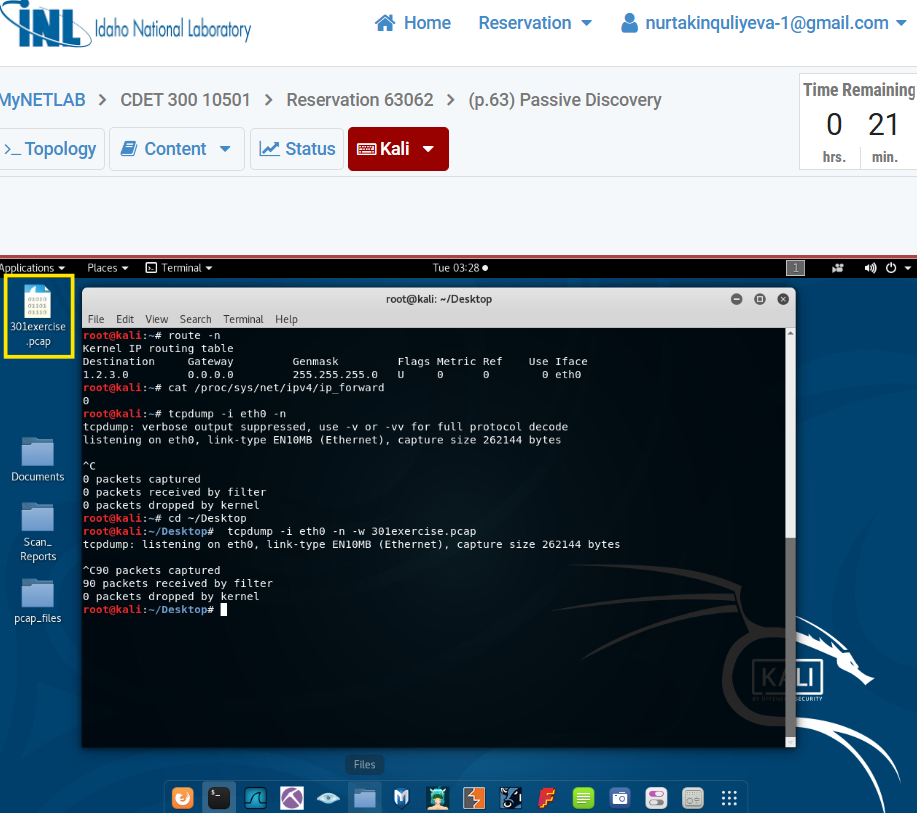
commands you entered in the command shell before you exited.

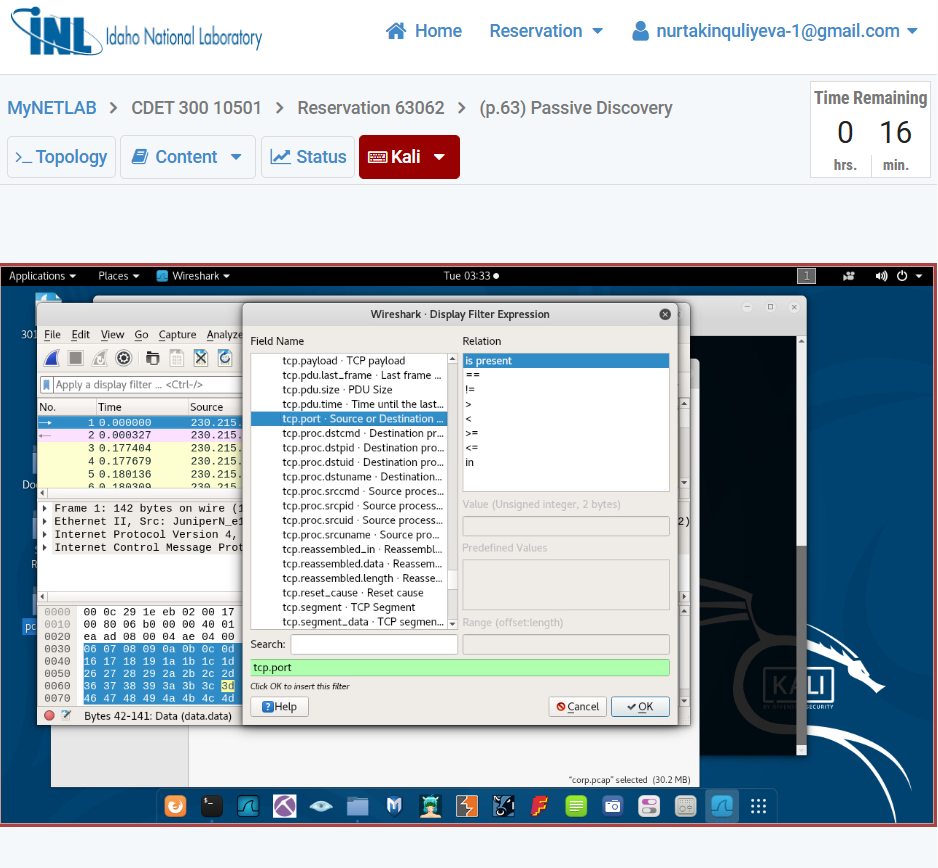


## 8)tcpdump -i eth0 -n -w 301exercise.pcap

-w 301exercise.pcap → tutulmuş paketləri .pcap faylına yazır

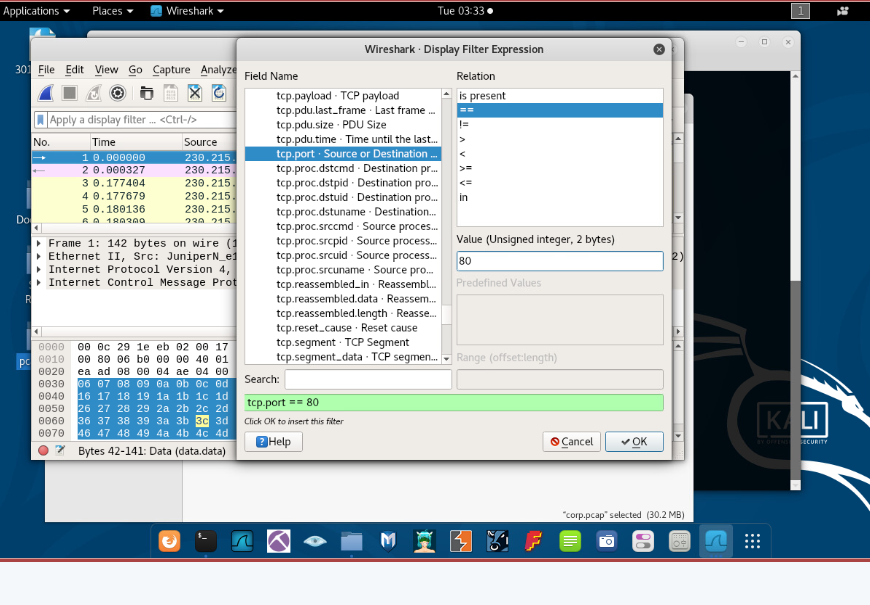
.pcap → Wireshark kimi proqramlarla açılan şəbəkə capture formatıdır

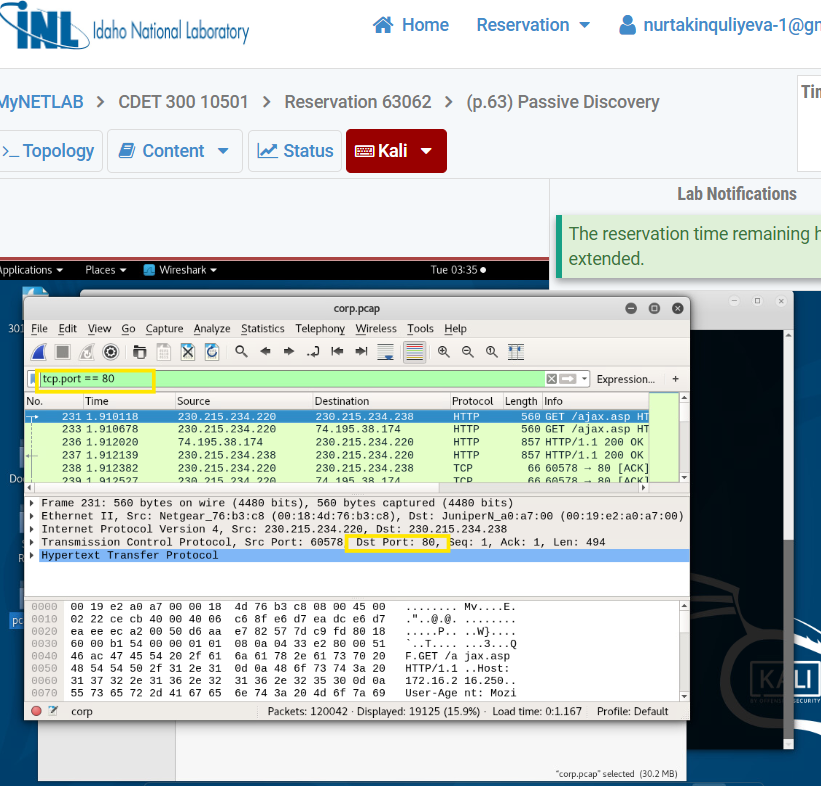


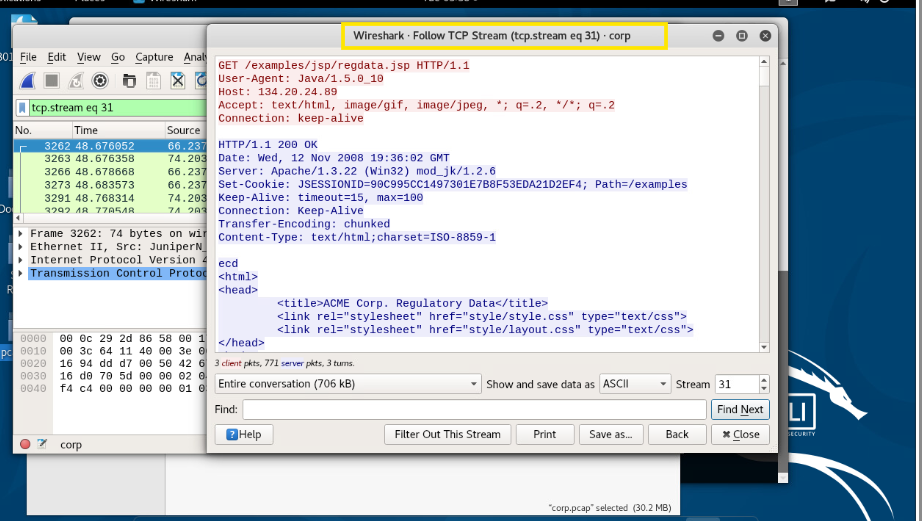


Bu filteri yaratmağımızın məqsədi şəbəkə trafiki içində bizə lazım olan məlumatı tez və rahat tapmaqdır. Şəbəkədə eyni anda minlərlə paket hərəkət edir və onların hamısını analiz etmək həm çətin, həm də vaxt aparandır. Ona görə filter istifadə edərək yalnız maraqlandığımız trafiki görürük.

Məsələn, **TCP port 80** HTTP (veb) trafikinə aiddir. Əgər biz istifadəçinin hansı saytlara qoşulduğunu, serverin cavab verib-vermədiyini və ya veb əlaqəsində problem olub-olmadığını yoxlamaq istəyiriksə, yalnız port 80 ilə bağlı paketləri filtrdən keçiririk. Bu, analiz prosesini sadələşdirir və diqqətimizi konkret problemə yönəldir.



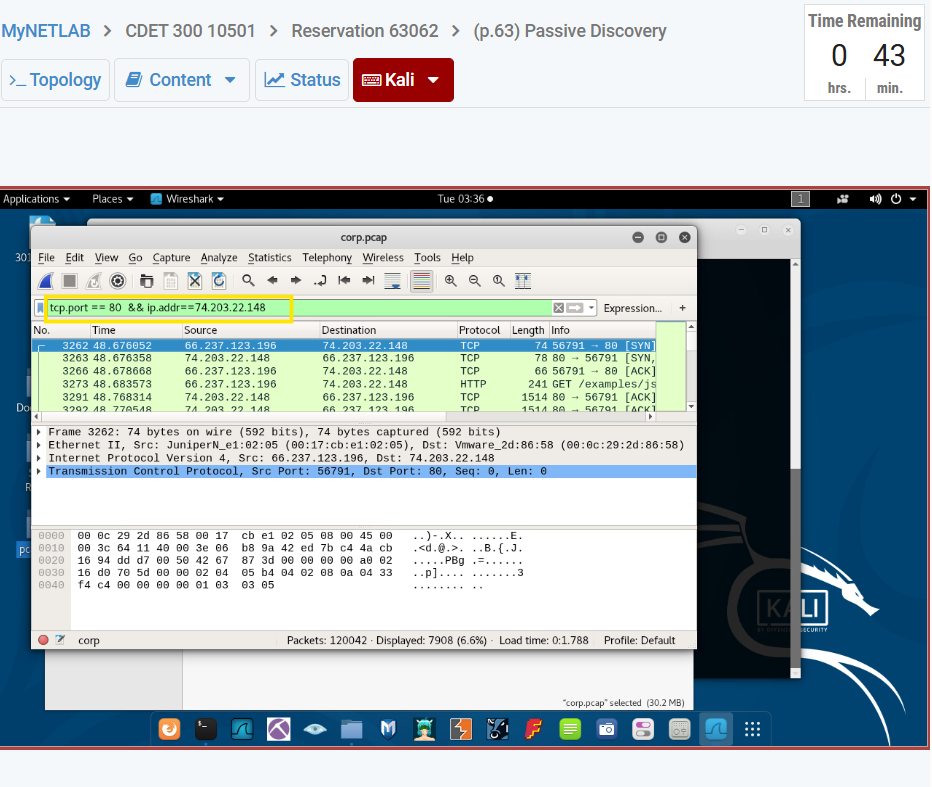




**Wireshark-da “Follow TCP Stream” funksiyası bizə eyni TCP bağlantısına aid bütün paketləri birləşdirilmiş şəkildə göstərmək üçün lazımdır.**

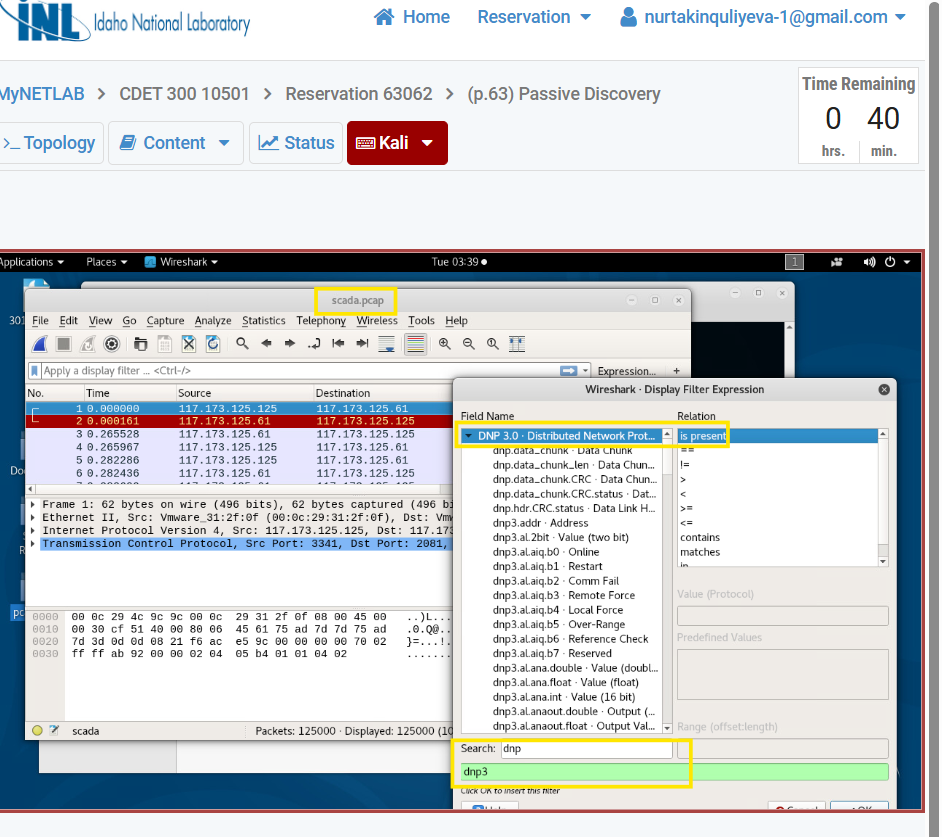
Şəbəkədə məlumatlar paket-paket göndərilir və normal görünüşdə qarışıq ola bilər. Bu funksiya həmin paketləri düzgün ardıcıllıqla birləşdirir və oxunaqlı mətn formasında təqdim edir. Beləliklə, əlaqə zamanı müştəri və server arasında gedən bütün məlumatları birdəfəlik görmək mümkündür.

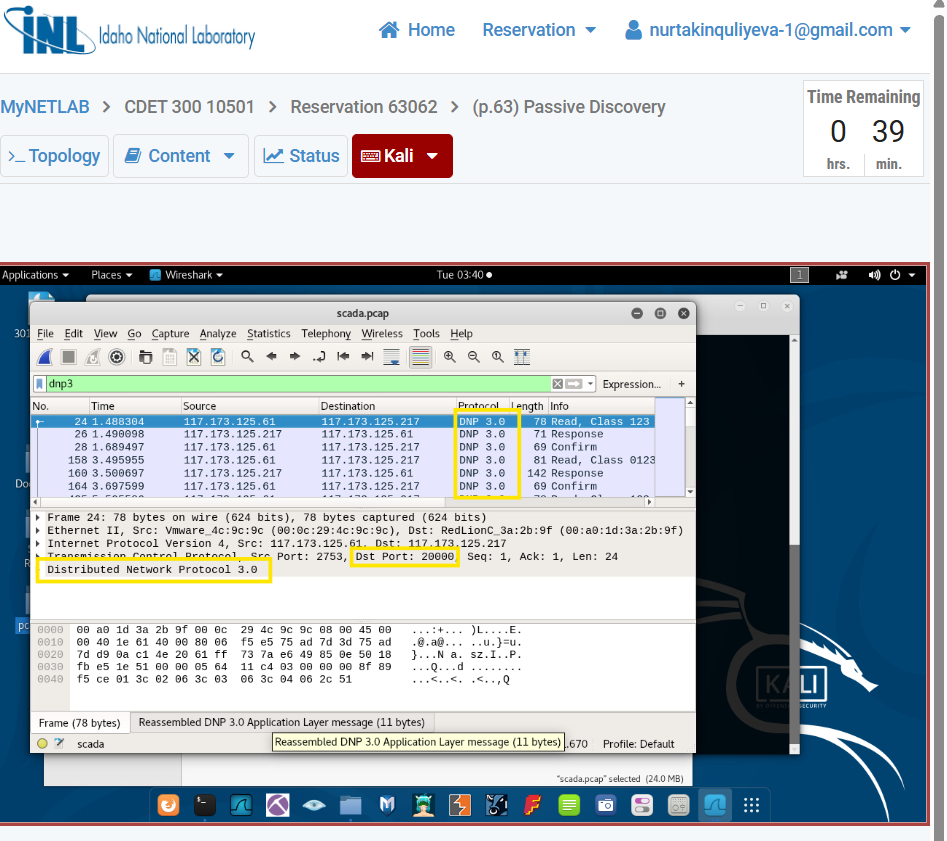
İçində HTTP sorğuları və cavabları, göndərilən və qəbul edilən məlumatlar, cookie və header məlumatları, hətta şifrələnməmiş login məlumatları ola bilər. Bu funksiyadan istifadə edərək veb problemlərini araşdırmaq, server-müştəri trafikini izləmək və təhlükəsizlik yoxlamaları aparmaq asanlaşır.





Wiresharda istifadə oluna biləcək əmrlər.

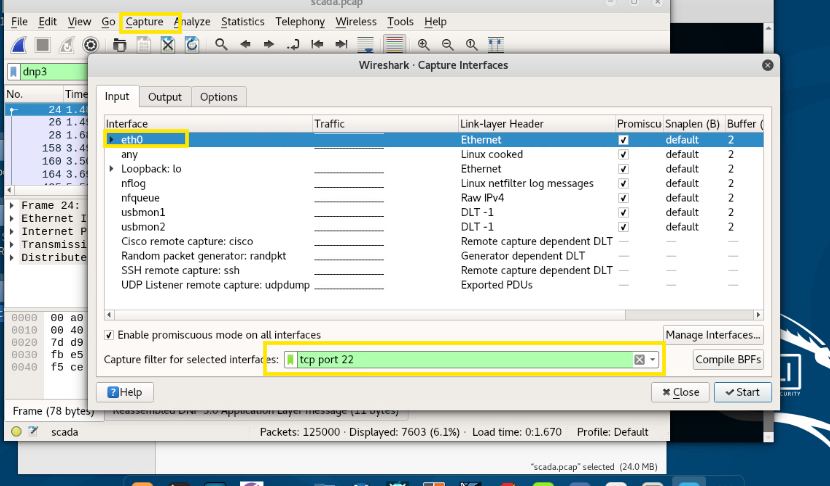


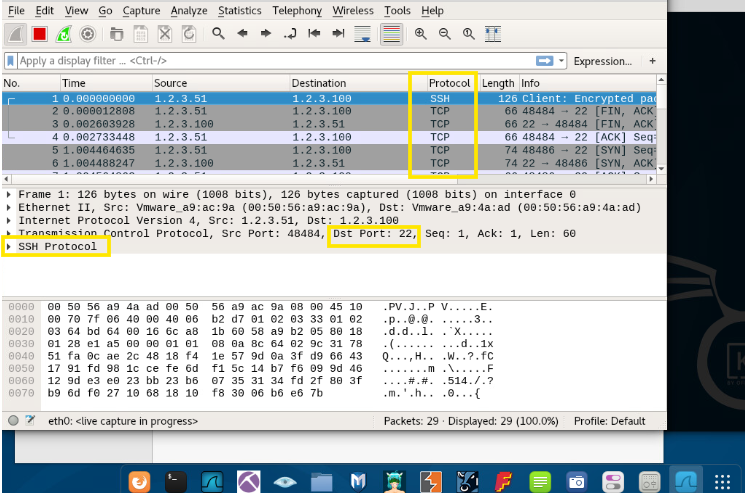


**DNP3.0 (Distributed Network Protocol 3.0)** sənaye və enerji sistemlərində, xüsusilə SCADA və elektrik stansiyalarında istifadə olunur. Bu protokol cihazlar arasında **ölçü məlumatları, hadisələr, idarəetmə əmrləri və vaxt stempləri** kimi məlumatları ötürür.

Wireshark-da DNP3 trafiki izlənə və analiz edilə bilər. Protokol TCP və UDP üçün **20000 port**dan istifadə edir.

Qısacası, DNP3.0 sistemlərin avtomatlaşdırılması və uzaqdan monitorinqi üçün cihazlar arasında məlumat mübadiləsini təmin edən protokoldur.



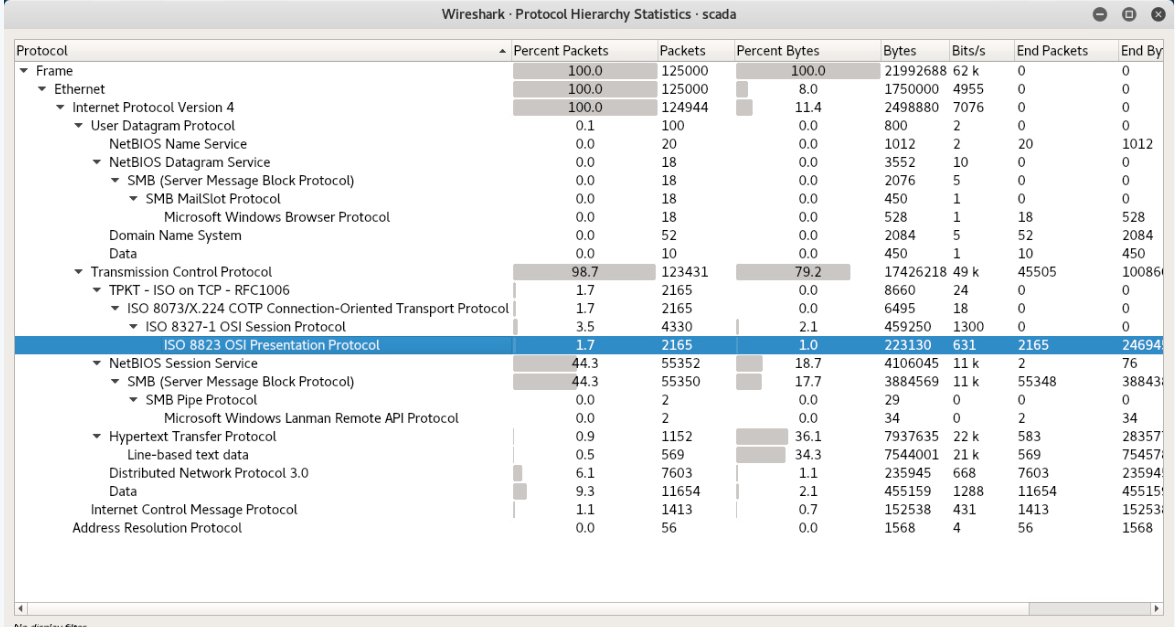


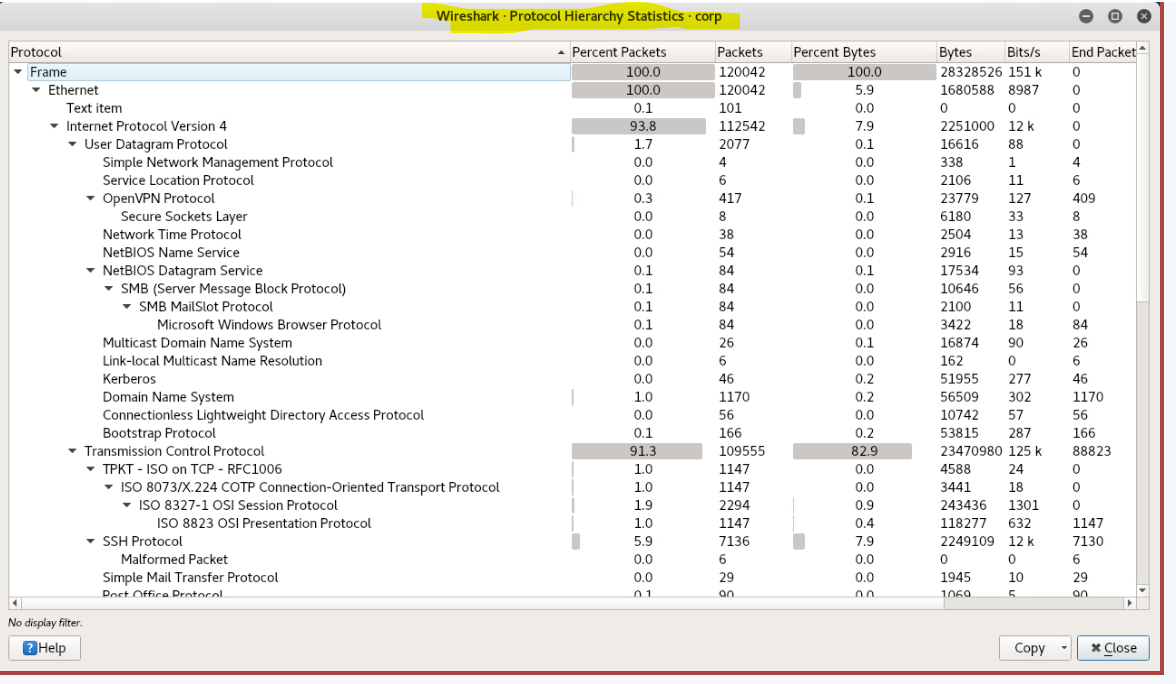
**Wireshark-da capture filter** şəbəkə trafiki tutularkən hansı paketlərin qeyd olunacağını seçmək üçün istifadə olunur.

Yəni, şəbəkədə minlərlə paket hərəkət edir, amma hər birini saxlamaq lazım deyil. Capture filter sayəsində yalnız **maraqlandığımız trafiki** tuturuq, məsələn: müəyyən **IP ünvanı, port, protokol** və ya **şəbəkə interfeysi** üzrə.

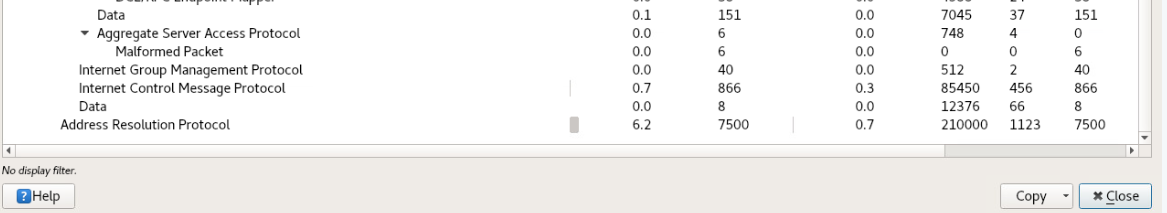
Bu həm **disk yaddaşını qoruyur**, həm də **analizi sadələşdirir**, çünki fayla yalnız lazım olan paketlər yazılır.

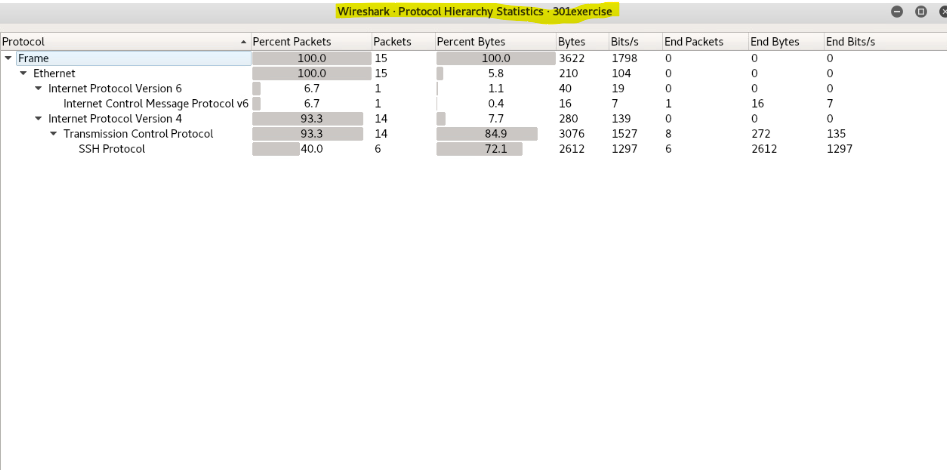
Post-exercise analysis

• What network protocols did you find? 





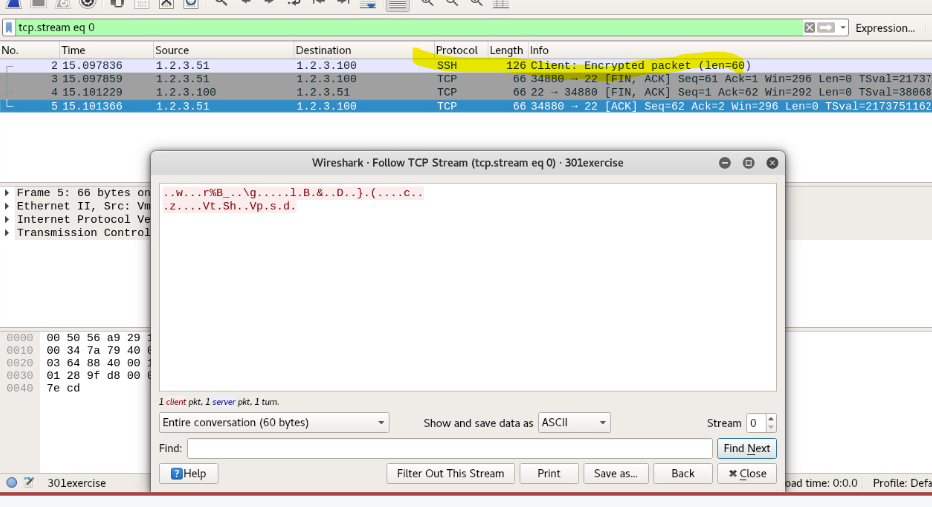




• What ICS-specific protocols did you find?

DNP3, Ethernet

• Were there plain text protocols?



Lab2

Active Discovery Exercises

1)arp-scan -g 1.2.3.0/24 əmri lokal şəbəkədə aktiv cihazları tapmaq üçün istifadə olunur.

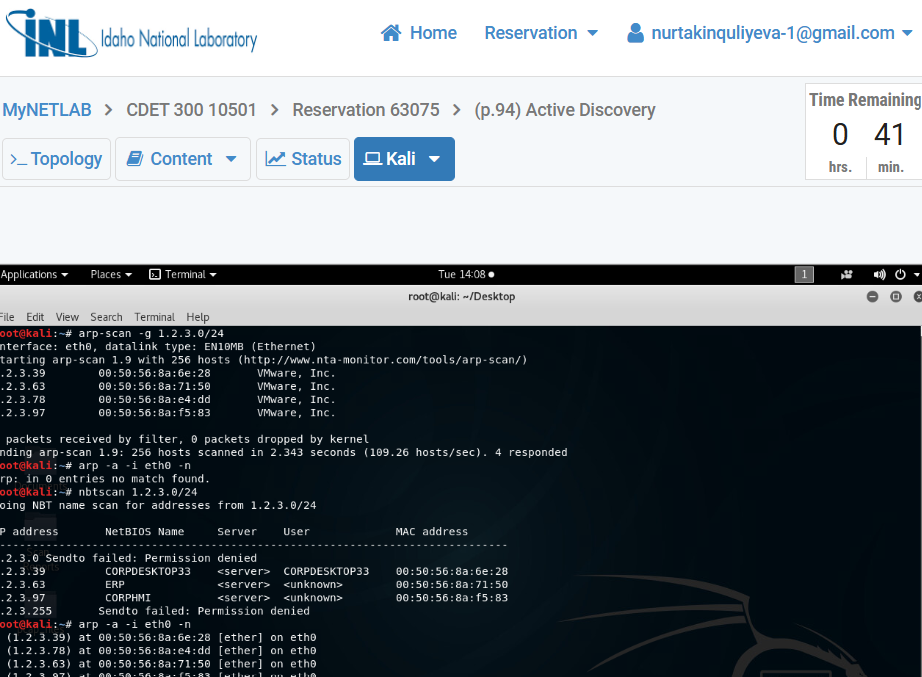
Bu əmr göstərilən şəbəkə aralığında (burada **1.2.3.0/24**) ARP sorğuları göndərir və cavab verən cihazların IP və MAC ünvanlarını siyahıya alır.

-g parametri “gratuitous ARP” üsulu ilə skan etməyə imkan verir. /24 isə həmin şəbəkədə 256 IP ünvanın (1.2.3.0 – 1.2.3.255 aralığı) yoxlanacağını göstərir.

arp -a -i eth0 -n əmri sistemdə **ARP cədvəlini** göstərmək üçün istifadə olunur.

Bu əmr eth0 şəbəkə interfeysi üzrə kompüterin artıq tanıdığı IP və MAC ünvan uyğunluqlarını siyahıya alır. Yəni sistem daha əvvəl əlaqə qurduğu cihazların məlumatını göstərir.

-a bütün ARP qeydlərini göstərir, -i eth0 yalnız həmin interfeysə aid olanları seçir, -n isə IP ünvanlarını adlara çevirmədən rəqəmsal formada göstərir



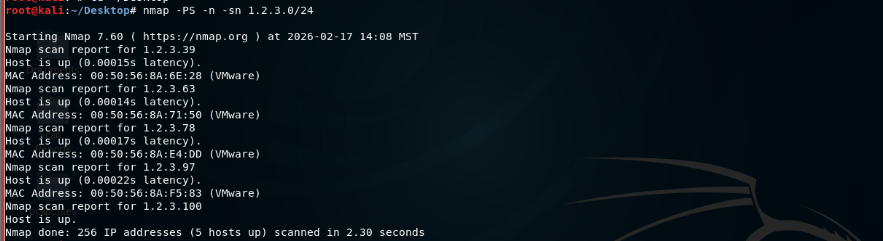
nbtscan 1.2.3.0/24 göstərilən /24 şəbəkə aralığında NetBIOS sorğuları göndərərək Windows sistemlərini tapır. Bu əmr aktiv cihazların IP ünvanını və NetBIOS adını (kompüter adını) göstərir. Yəni bu, şəbəkə skan etmə alətidir və əsasən Windows maşınlarını müəyyən etmək üçün istifadə olunur.

Qeyd olaraq, Windows-da olan nbtstat -c əmri skan etmir, sadəcə NetBIOS keşini göstərir.

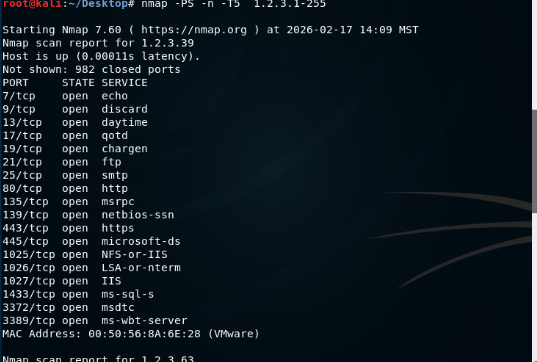
Daha sonra arp -a -i eth0 -n əmri icra ediləndə sistemin ARP cədvəli göstərilir. nbtscan zamanı şəbəkəyə sorğular göndərildiyi üçün aktiv cihazlar cavab verir və onların IP–MAC uyğunluğu ARP cədvəlinə düşür. Bu əmr həmin IP və MAC ünvanlarını görməyə imkan verir.

Əmrlər Nmap vasitəsilə şəbəkədə aktiv hostları tapmaq və analiz etmək üçün istifadə olunur.

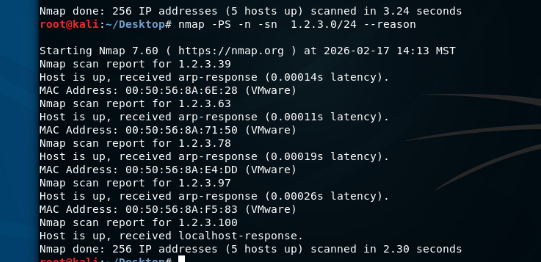
nmap -PS -n -sn 1.2.3.0/24 əmri göstərilən /24 şəbəkədə aktiv cihazları tapmaq üçündür. Burada TCP SYN ping göndərilir, DNS həlli edilmir və port skanı aparılmadan yalnız hansı hostların “up” olduğu müəyyən edilir.



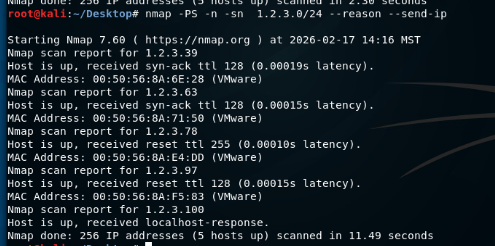
nmap -PS -n -T5 1.2.3.1-255 əmri eyni məqsədlə istifadə olunur, lakin IP aralığı əl ilə göstərilib və -T5 parametri ilə çox sürətli (aqressiv) rejimdə skan edilir.



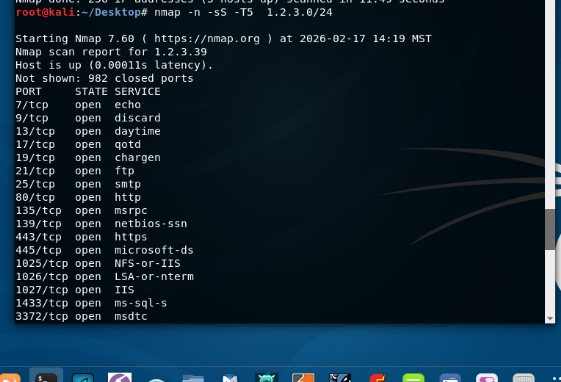
nmap -PS -n -sn 1.2.3.0/24 --reason əmri hostun niyə aktiv (up) kimi göründüyünü göstərir, məsələn hansı cavaba əsasən nəticə çıxarıldığını bildirir.



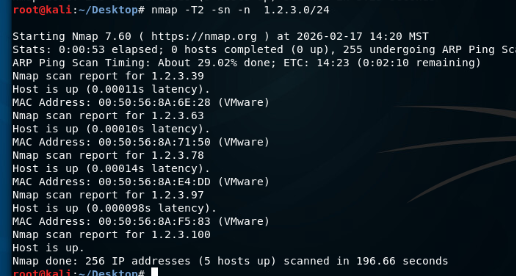
nmap -PS -n -sn 1.2.3.0/24 --reason --send-ip əmri isə ARP əvəzinə birbaşa IP paketləri göndərərək skan edir və səbəbi ilə birlikdə nəticə göstərir.



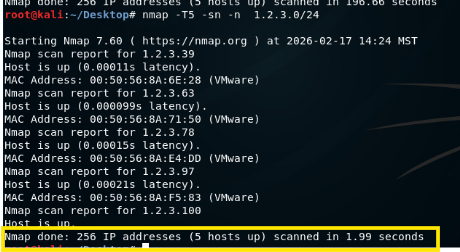
nmap -n -sS -T5 1.2.3.0/24 əmri artıq port skanı aparır. SYN (yarım açıq) üsulla açıq portları müəyyən edir və bunu sürətli rejimdə edir.

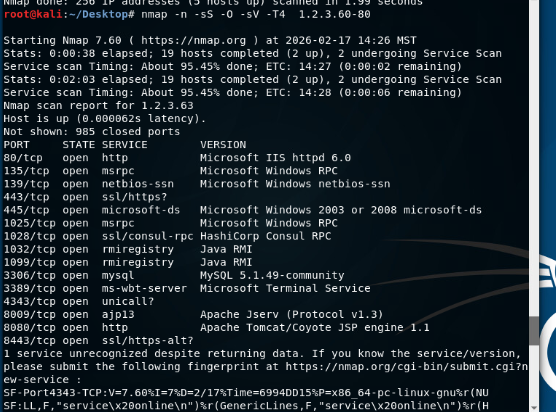


nmap -T2 -sn -n 1.2.3.0/24 əmri daha yavaş və səssiz skandır. Bu üsul daha az diqqət çəkir

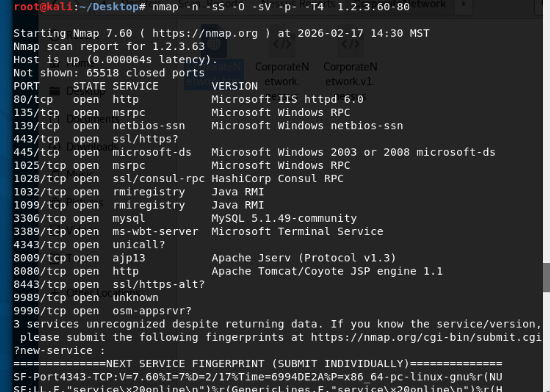


nmap -T5 -sn -n 1.2.3.0/24 isə çox sürətli və aqressiv host aşkarlama skanıdır.





nmap -n -sS -O -sV -T4 1.2.3.60-80 əmri 1.2.3.60-dan 1.2.3.80-ə qədər olan IP ünvanlarını SYN (yarım açıq) üsulla skan edir. Burada həm əməliyyat sistemi aşkarlanır (-O), həm də servis versiyaları tapılır (-sV). -T4 isə balanslı və daha stabil sürətli rejimdir.



nmap -n -sS -O -sV -p- -T4 1.2.3.60-80 əmri isə əvvəlki əmrdən fərqli olaraq bütün 65535 portu (-p-) yoxlayır. Yəni yalnız standart portlar deyil, gizli və qeyri-standart portlar da aşkar edilə bilər. Bu daha dərin və ətraflı port analizidir.

Nessus

1. Review “Scan Reports” located in the directory /root/Desktop/Scan\_Reports for output from

Nessus

2. Identify specific vulnerabilities for network hosts

3. Complete your network map.

**Post-exercise review**

• What information does Nessus provide that you didn’t find with Nmap?

Nessus yalnız açıq portları ve servisləri deyil, hemin servislerin konkret zəifliklerini (CVE nömrəlǝri, risk sǝviyyǝsi, exploit mövcudluğu vǝ s.) göstǝrdi.

Nmap port scanning va service detection etdi, lakin Nessus əlave olaraq:

· CVE ID-lerini göstərdi

· Risk səviyyasini (Low, Medium, High, Critical) tǝyin etdi

· Patch olub-olmadığını bildirdi

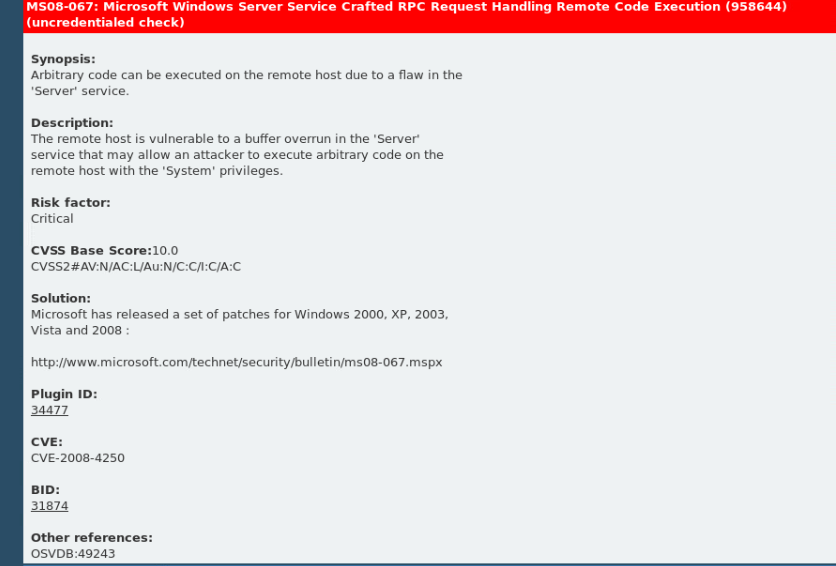
· Konfiqurasiya səhvlerini aşkar etdi

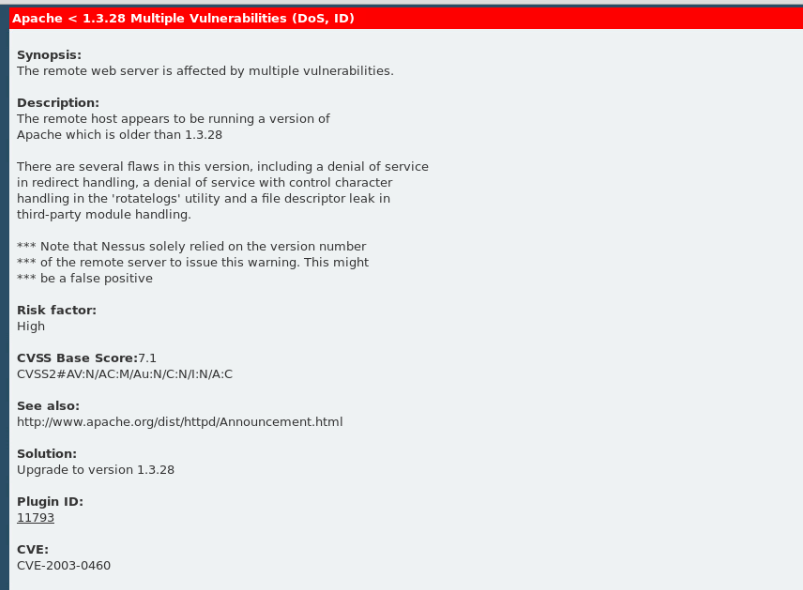
· Zeif SSL/TLS versiyalarını göstǝrdi

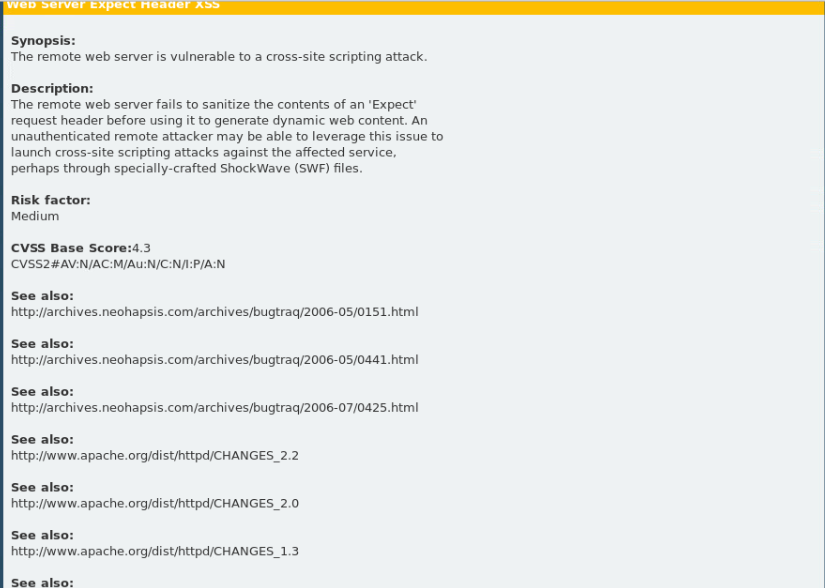
· Default credential problemlerini aşkar etdi

Yəni, Nmap "nə açıqdır?" sualına cavab verdi, Nessus isǝ "ne qeder təhlükəlidir" sualını cavablandırdı.

• What different types of security problems did you discover?







• Were there any false-positives and how did you identify them?

· Host Windows XP-dirsə (sənin halda) → vulnerability teorik olaraq mövcuddur

· · Əgər host artıq patch-lanıb → exploit mümkün deyil → Nessus false positive