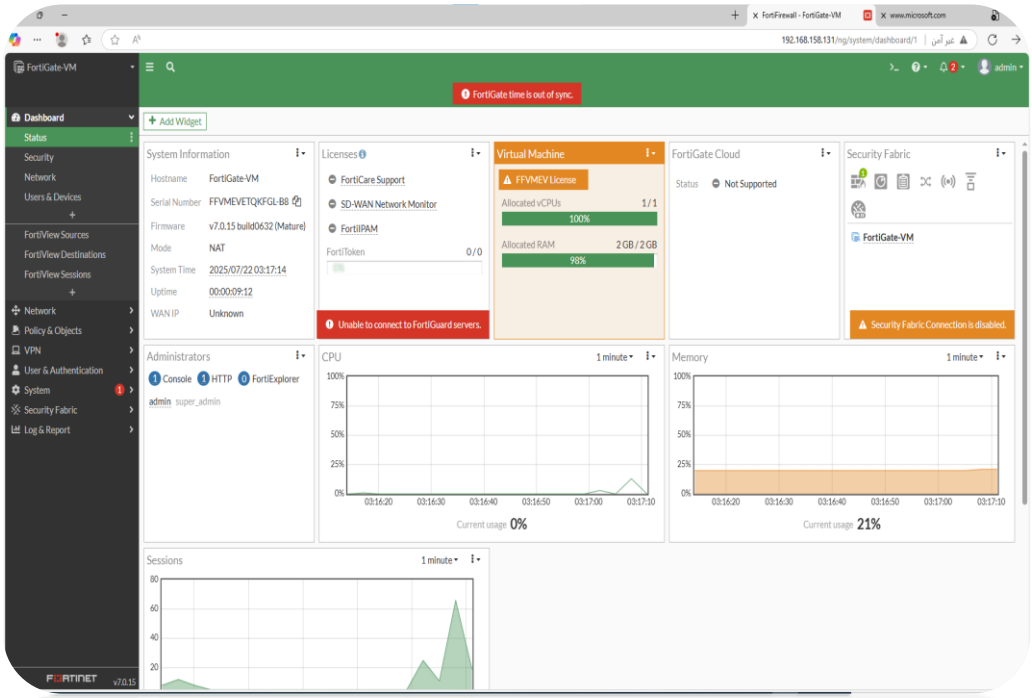
TRAINING-PROJECT

تحت اشراف الدكتور : نشوان الذبحاني



اعداد الطالب:

نورالدين عبد الكريم سالم اسماعيل

محمد نعمان

محمد عبد الواحد

انس الخامري

بسم الله الرحمن الرحيم

الحمد لله رب العالمين، والصلاة والسلام على أشرف المرسلين، سيدنا محمد وعلى آله وصحبه أجمعين اما بعد :-

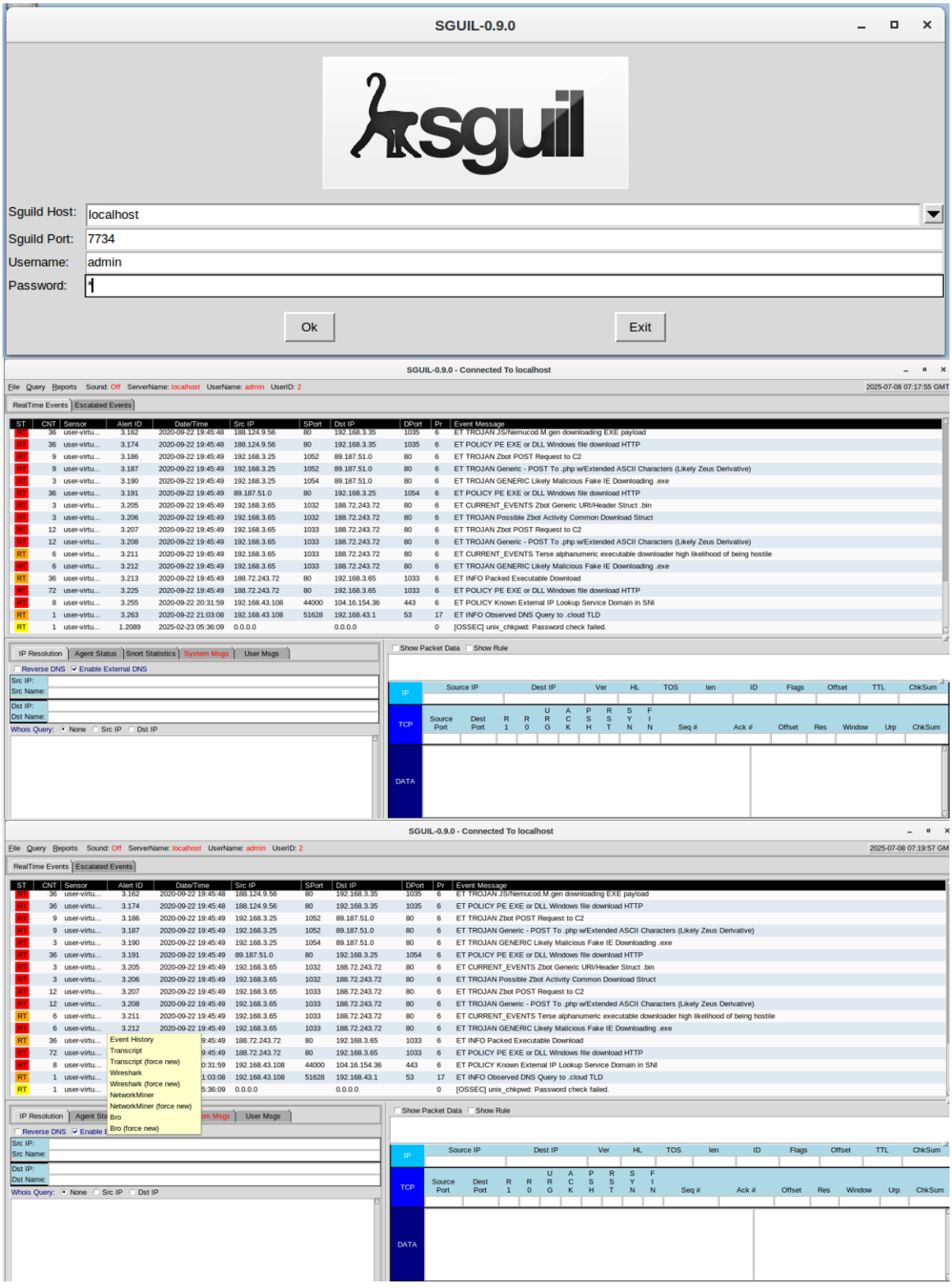
Firstly working with kibana:-

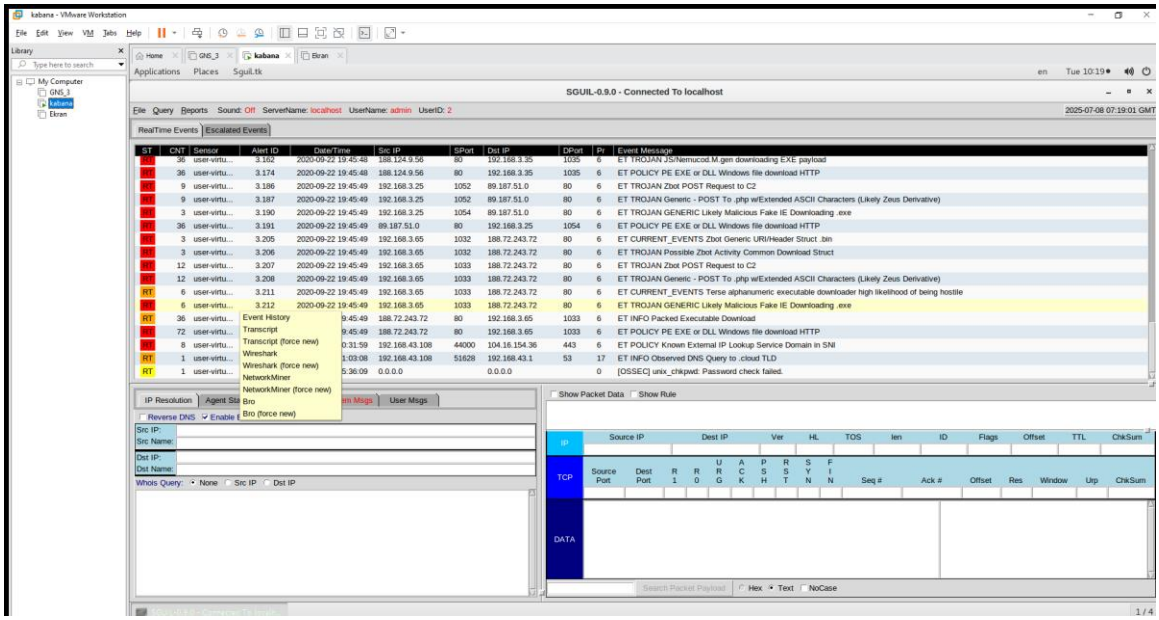
I add security onion in vmware in our lab the user name is user and password is a

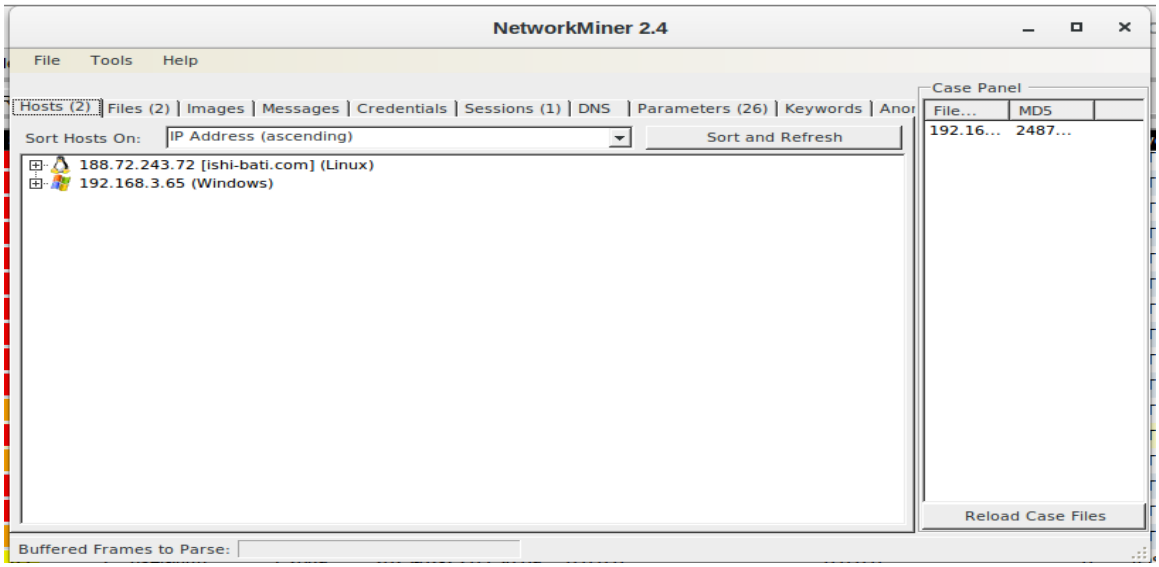

home
Setup
CyberChef
Kibana
README
Squert
Squil
command
Trash
SecurityOnion


home
Setup
CyberChef
Kibana
README
Squert
Open
Cut
Copy
Move To…
Copy To…
Make Link
Rename…
Move to Trash
Resize Icon…
Restore Icon's Original Size
Compress…
Properties
SecurityOnion

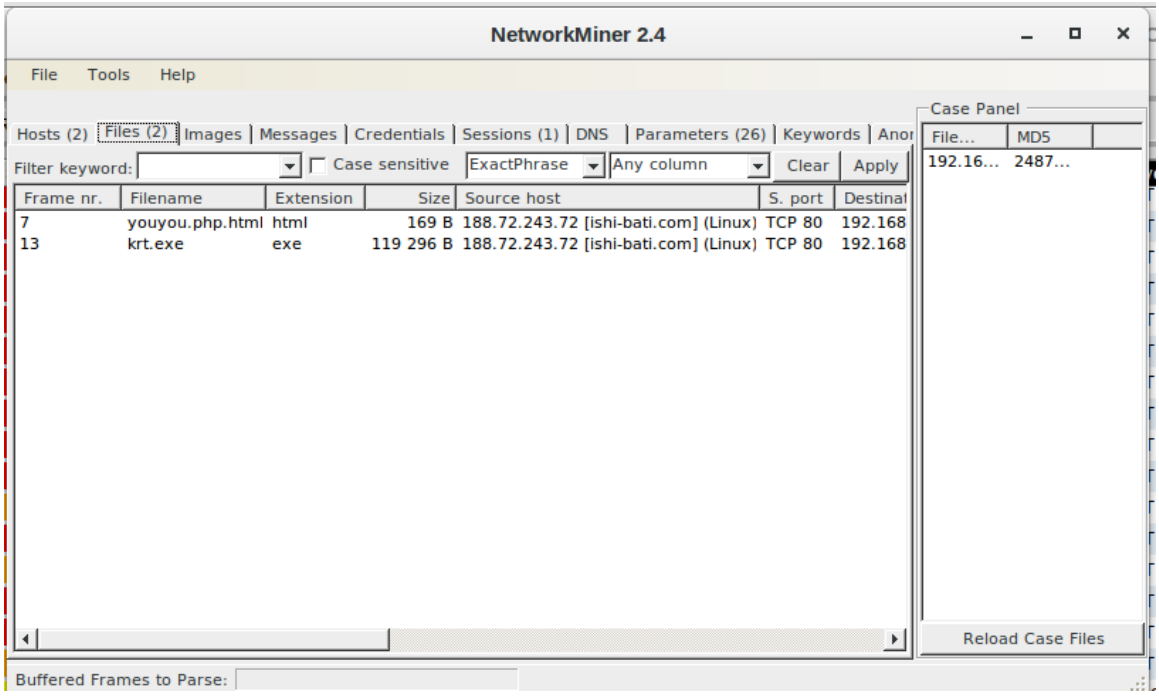
This is how to use squli to analysis files



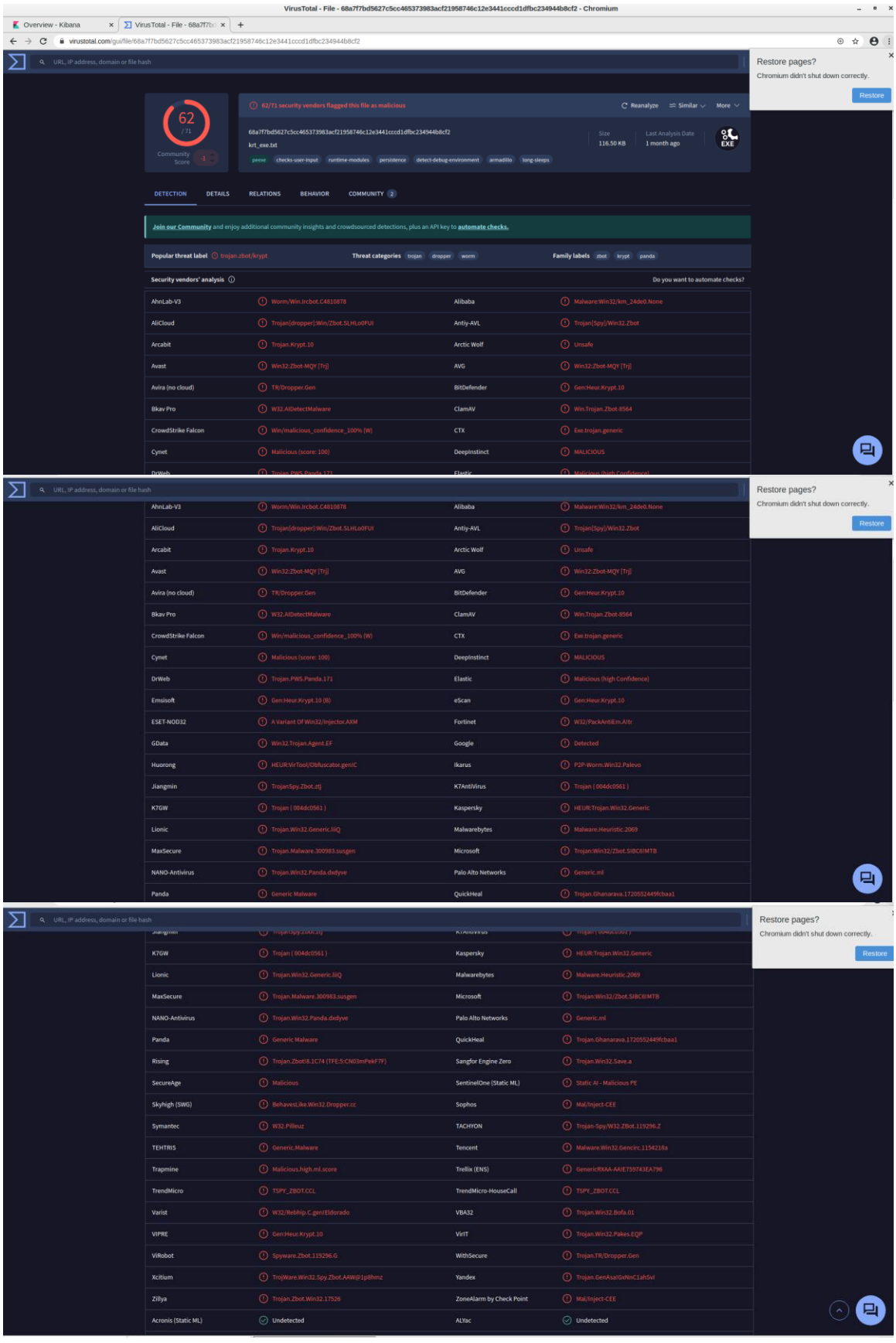

kabana - VMware Workstation
SGUIL-0.9.0 - Connected To localhost


NetworkMiner 2.4
File
Tools
Help
Hosts (2)
Files (2)
Images
Messages
Credentials
Sessions (1)
DNS
Parameters (26)
Keywords
Case Panel
Sort Hosts On:
IP Address (ascending)
Sort and Refresh
188.72.243.72 [ishi-bati.com] (Linux)
192.168.3.65 (Windows)
Reload Case Files
Buffered Frames to Parse:

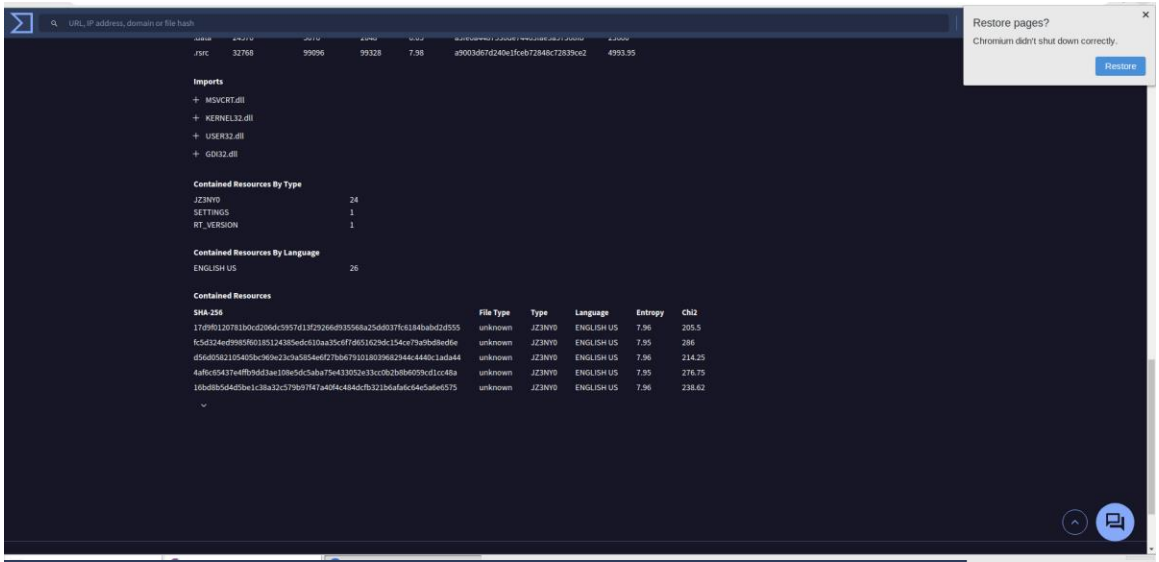
As we see that is files is exe

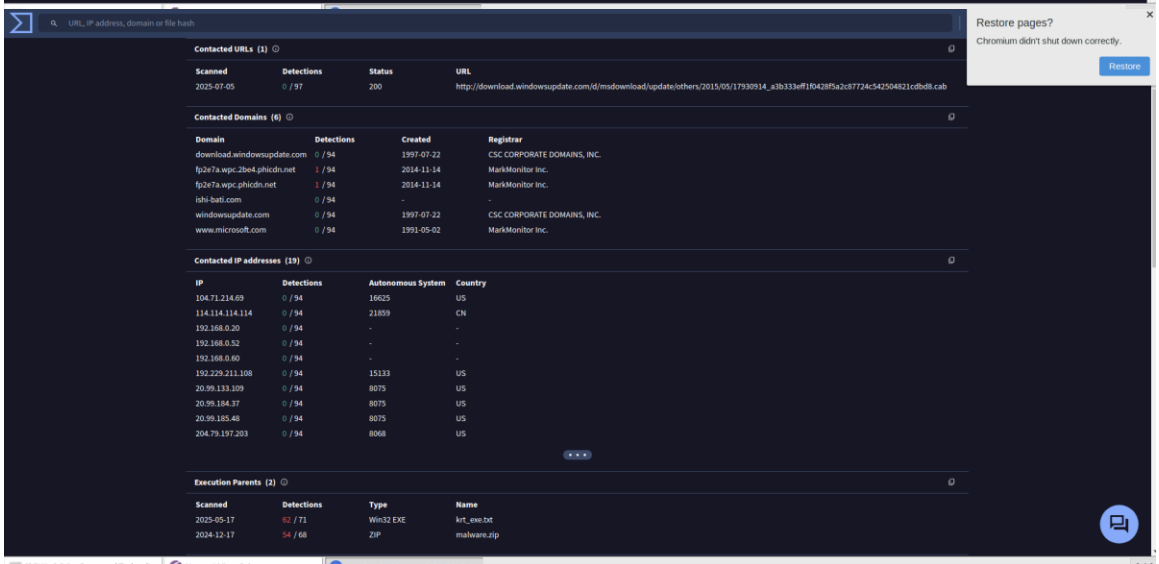


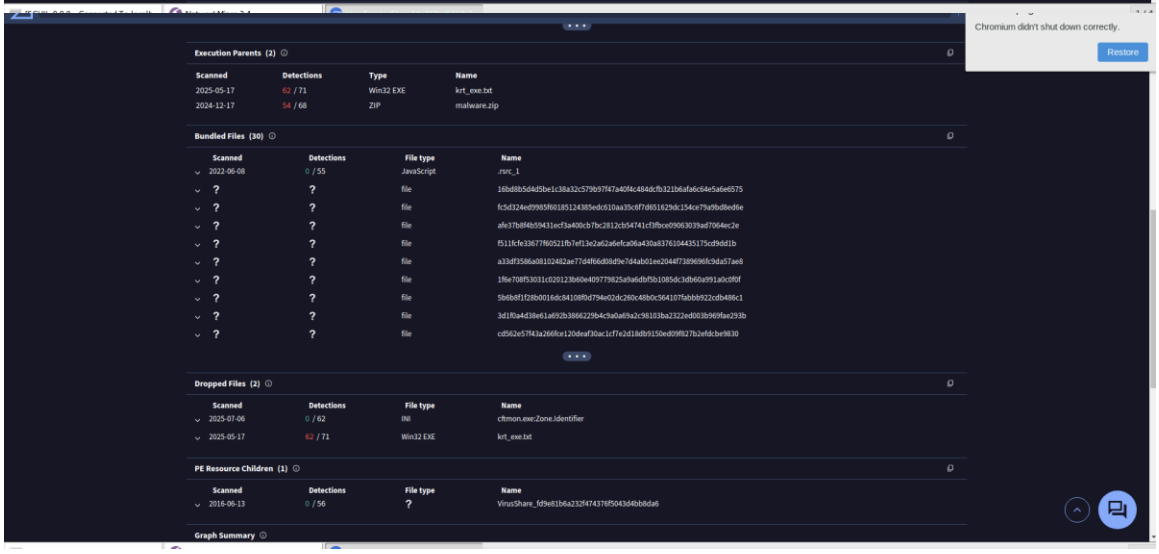
We will capy it to virus total side to see if there is any signatures about it

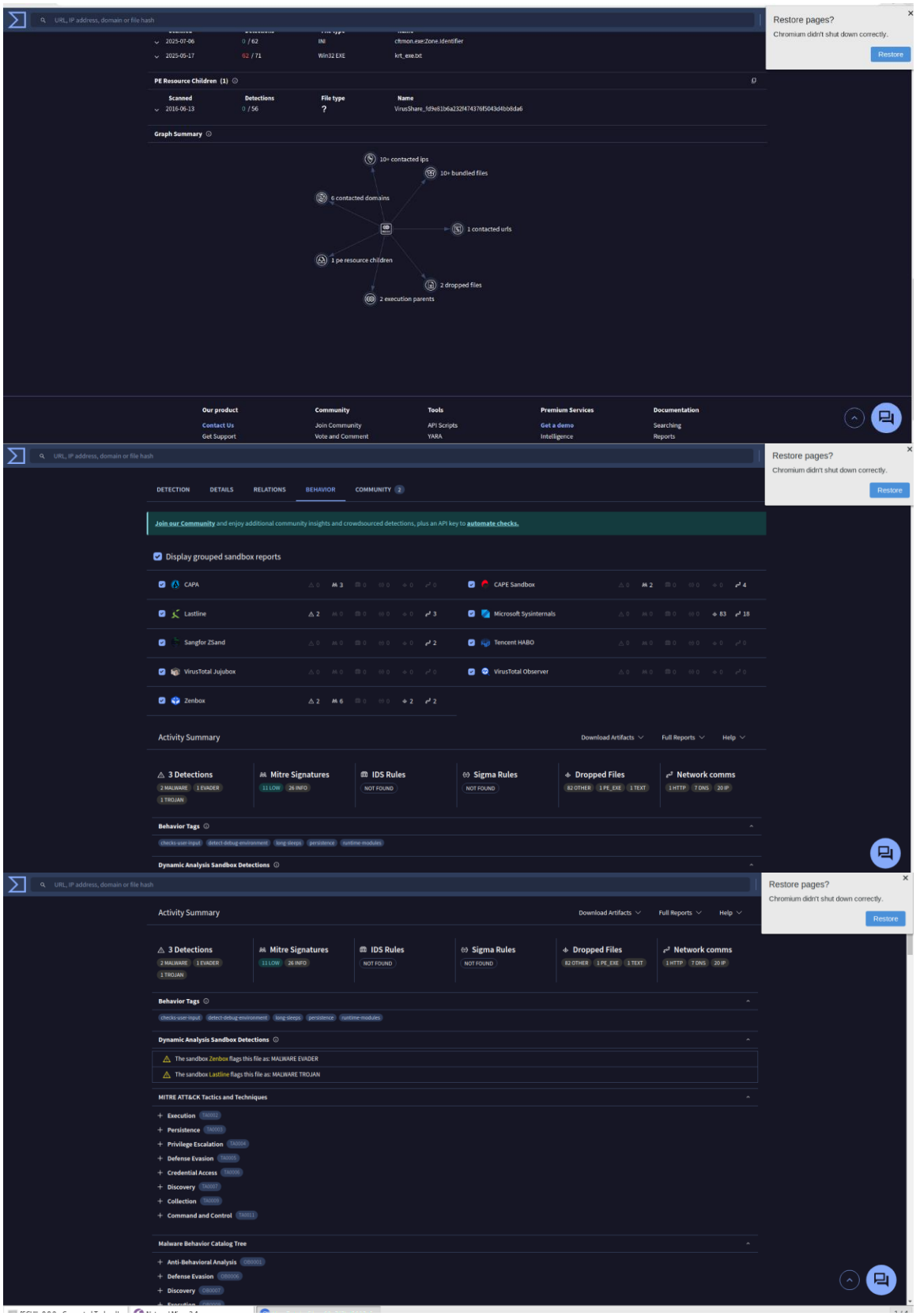

VirusTotal - File - 68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2 - Chromium
Overview - Kibana
VirusTotal - File - 68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2
virustotal.com/gui/file/68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2
URL, IP address, domain or file hash
Restore pages?
Chromium didn't shut down correctly.
Restore
62 / 71
Community Score
62/71 security vendors flagged this file as malicious
Reanalyze
Similar
More
68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2
krt_exe.txt
Size
116.50 KB
Last Analysis Date
1 month ago
peexe
checks-user-input
runtime-modules
persistence
detect-debug-environment
armadillo
long-sleeps
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 2
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.zbot/krypt
Threat categories trojan dropper worm
Family labels zbot krypt panda
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Worm/Win.Ircbot.C4810878
Alibaba Malware:Win32/km_24de0.None
AliCloud Trojan[dropper]:Win/Zbot.SLHLo0FUI
Antiy-AVL Trojan[Spy]/Win32.Zbot
Arcabit Trojan.Krypt.10
Arctic Wolf Unsafe
Avast Win32:Zbot-MQY [Trj]
AVG Win32:Zbot-MQY [Trj]
Avira (no cloud) TR/Dropper.Gen
BitDefender Gen:Heur.Krypt.10
Bkav Pro W32.AIDetectMalware
ClamAV Win.Trojan.Zbot-8564
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.generic
Cynet Malicious (score: 100)
DeepInstinct MALICIOUS
DrWeb Trojan.PWS.Panda.171
Elastic Malicious (high Confidence)
Emsisoft Gen:Heur.Krypt.10 (B)
eScan Gen:Heur.Krypt.10
ESET-NOD32 A Variant Of Win32/Injector.AXM
Fortinet W32/PackAntiEm.A!tr
GData Win32.Trojan.Agent.EF
Google Detected
Huorong HEUR:VirTool/Obfuscator.gen!C
Ikarus P2P-Worm.Win32.Palevo
Jiangmin TrojanSpy.Zbot.ztj
K7AntiVirus Trojan (004dc0561)
K7GW Trojan (004dc0561)
Kaspersky HEUR:Trojan.Win32.Generic
Lionic Trojan.Win32.Generic.liiQ
Malwarebytes Malware.Heuristic.2069
MaxSecure Trojan.Malware.300983.susgen
Microsoft Trojan:Win32/Zbot.SIBC6!MTB
NANO-Antivirus Trojan.Win32.Panda.dxdyve
Palo Alto Networks Generic.ml
Panda Generic Malware
QuickHeal Trojan.Ghanarava.1720552449fcbaa1
Rising Trojan.Zbot!8.1C74 (TFE:5:CN63mPekF7F)
Sangfor Engine Zero Trojan.Win32.Save.a
SecureAge Malicious
SentinelOne (Static ML) Static AI - Malicious PE
Skyhigh (SWG) BehavesLike.Win32.Dropper.cc
Sophos Mal/Inject-CEE
Symantec W32.Pilleuz
TACHYON Trojan-Spy/W32.Zbot.119296.Z
TEHTRIS Generic.Malware
Tencent Malware.Win32.Gencirc.1154218a
Trapmine Malicious.high.ml.score
Trellix (ENS) GenericRXAA-AA!E759743EA796
TrendMicro TSPY_ZBOT.CCL
TrendMicro-HouseCall TSPY_ZBOT.CCL
Varist W32/Rebhip.C.gen!Eldorado
VBA32 Trojan.Win32.Bofa.01
VIPRE Gen:Heur.Krypt.10
VirIT Trojan.Win32.Pakes.EQP
ViRobot Spyware.Zbot.119296.G
WithSecure Trojan.TR/Dropper.Gen
Xcitium TrojWare.Win32.Spy.Zbot.AAW@1p8hmz
Yandex Trojan.GenAsaIGxNnC1ahSvI
Zillya Trojan.Zbot.Win32.17526
ZoneAlarm by Check Point Mal/Inject-CEE
Acronis (Static ML) Undetected
ALYac Undetected


URL, IP address, domain or file hash
68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2
krt_exe.txt
Size 116.50 KB
Last Analysis Date 1 month ago
peexe checks-user-input runtime-modules persistence detect-debug-environment armadillo long-sleeps
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Basic properties
MD5 e759743ea7967ccccee0d27b9bfcbaa1
SHA-1 73603c37609d862509a777cb5d2c25e6a9582036
SHA-256 68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2
Vhash 015046551d6577z2001a19fz9fz
Authentihash a1bd7786e3a1cc11ae4bf29b64bddc850bee0ae59ab31dac3e8eaf9d11c00eac
Imphash b36ac1fa243e945f73d26ba487f8e2a5
Rich PE header hash 1cbe8a9b25adc758348d559505c85ff6
SSDEEP 3072:lL9rDE6ZJRyiNZNfKyj/4A01XCxFmLgm8ouzUcCy9kOZ:K/EE6fRyuZ/u1+msLuGy9g
TLSH T1A7C3D005A6C64A2AE0E681F20231C3F3D47FBAF23F017757E7D049A6A63521DAD2525F
File type Win32 EXE executable windows win32 pe peexe
Magic PE32 executable (GUI) Intel 80386, for MS Windows
TrID Win32 Executable MS Visual C++ (generic) (43.3%) | Microsoft Visual C++ compiled executable (generic) (22.9%) | Win32 Dynamic Link Library (generic) (9.1%) | Win16 N...
DetectItEasy PE32 | Compiler: EP:Microsoft Visual C/C++ (6.0 [1720-9782]) [EXE32] | Compiler: Microsoft Visual C/C++ (12.00.8168) [C++] | Linker: Microsoft Linker (6.00.8168) | Tool: ...
Magika PEBIN
File size 116.50 KB (119296 bytes)
PEiD packer Microsoft Visual C++
History
Creation Time 2010-02-17 23:30:17 UTC
First Submission 2010-02-24 16:34:55 UTC
Last Submission 2025-06-17 07:26:52 UTC
Last Analysis 2025-05-17 11:19:46 UTC
Names
krt_exe.txt
krt_exe
krt.exe
krt[2].exe
krt[6].exe
krt[1].exe
krt[5].exe
krt[14].exe
krt[11].exe
malware.exe
Signature info
Signature Verification
File is not signed
File Version Information
Copyright Copyright © 2009
File Version 2, 0, 0, 0
Portable Executable Info
Compiler Products
[C] VS98 (6.0) build 8168 count=11
[LNK] VS98 (6.0) imp/exp build 8168 count=3
[---] Unmarked objects count=64
[C++] VS98 (6.0) build 8168 count=1
[RES] VS98 (6.0) cvtres build 1720 count=1
id: 0x5d, version: 2179 count=6
id: 0xe, version: 7299 count=1
Header
Target Machine Intel 386 or later processors and compatible processors
Compilation Timestamp 2010-02-17 23:30:17 UTC
Entry Point 18406
Contained Sections 4
Sections
Name Virtual Address Virtual Size Raw Size Entropy MD5 Chi2
.text 4096 14700 14848 5.7 3be9e381ce995c01c6bf5b659b652a59 191834.23
.rdata 20480 1680 2048 4.41 5d1fde34aa0ad4a7e14cabb2d073b29d 99669.75
.data 24576 5076 2048 6.05 a3fe0a4487530de74463fae3a57568fb 23660
.rsrc 32768 99096 99328 7.98 a9003d67d240e1fceb72848c72839ce2 4993.95
Imports
MSVCRT.dll
Restore pages?
Chromium didn't shut down correctly.
Restore


URL, IP address, domain or file hash
.rsrc 32768 99096 99328 7.98 a9003d67d240e1fceb72848c72839ce2 4993.95
Imports
MSVCRT.dll
KERNEL32.dll
USER32.dll
GDI32.dll
Contained Resources By Type
JZ3NY0 24
SETTINGS 1
RT_VERSION 1
Contained Resources By Language
ENGLISH US 26
Contained Resources
SHA-256 File Type Type Language Entropy Chi2
17d9f0120781b0cd206dc5957d13f29266d93556a25dd037fc6184babd2d555 unknown JZ3NY0 ENGLISH US 7.96 205.5
fc5d324ed9985f60185124385edc610aa35c6f7d651629dc154ce79a9bd8ed6e unknown JZ3NY0 ENGLISH US 7.95 286
d56d0582105405bc969e23c9a5854e6f27bb67910180396294 4c4440c1ada44 unknown JZ3NY0 ENGLISH US 7.96 214.25
4af6c65437e4ffb9dd3ae108e5dc5aba75e433052e33cc0b2b8b6059cd1cc48a unknown JZ3NY0 ENGLISH US 7.95 276.75
16bd8b5d4d5be1c38a32c579b97f47a40f4c484dcfb321b6afa6c64e5a6e6575 unknown JZ3NY0 ENGLISH US 7.96 238.62
Restore pages?
Chromium didn't shut down correctly.
Restore

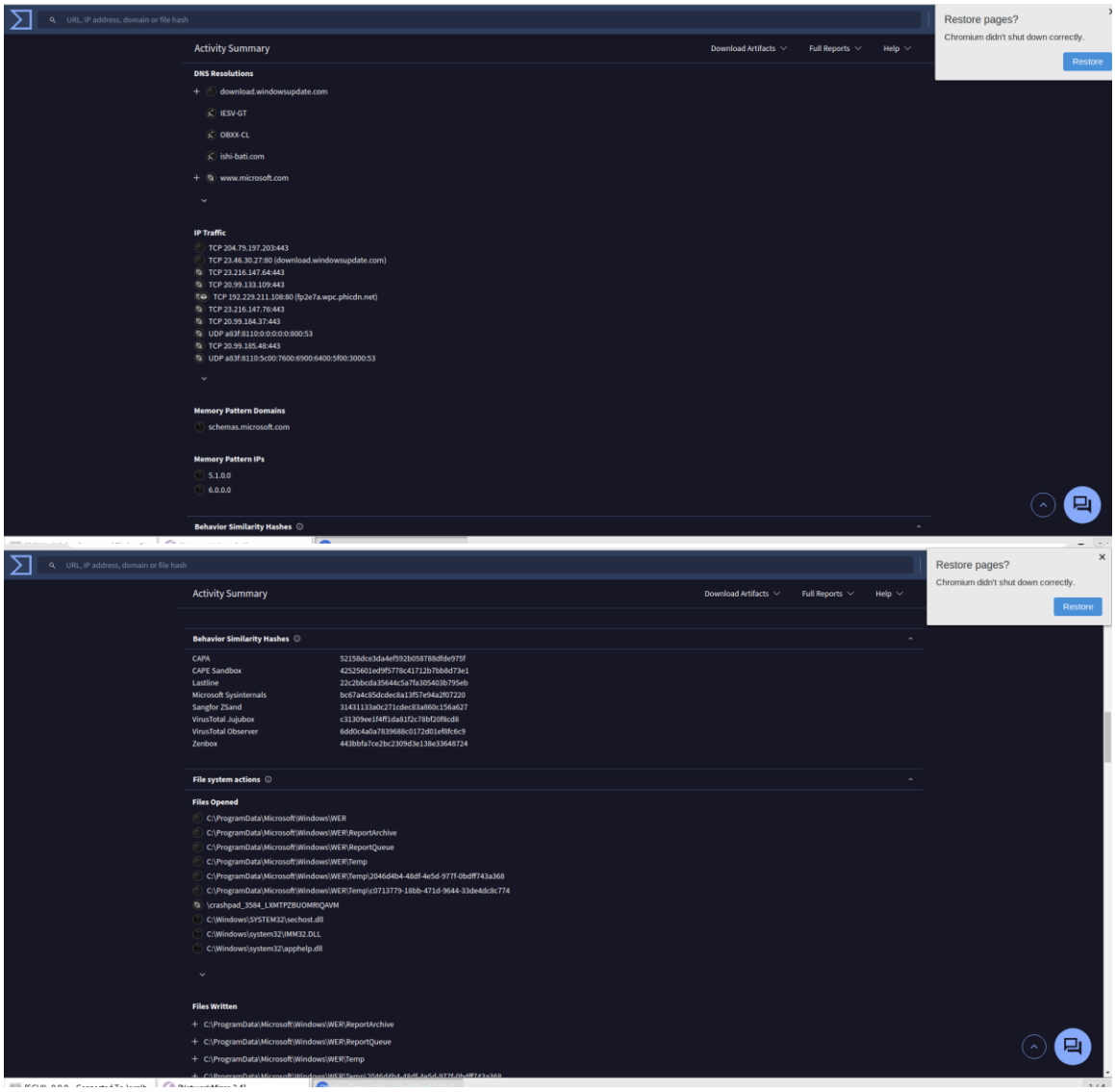

URL, IP address, domain or file hash
Contacted URLs (1)
Scanned Detections Status URL
2025-07-05 0 / 97 200 http://download.windowsupdate.com/d/msdownload/update/others/2015/05/17930914_a3b333eff1f0428f5a2c87724c542504821cdbd8.cab
Contacted Domains (6)
Domain Detections Created Registrar
download.windowsupdate.com 0 / 94 1997-07-22 CSC CORPORATE DOMAINS, INC.
fp2e7a.wpc.2be4.phicdn.net 1 / 94 2014-11-14 MarkMonitor Inc.
fp2e7a.wpc.phicdn.net 1 / 94 2014-11-14 MarkMonitor Inc.
ishi-bati.com 0 / 94 - -
windowsupdate.com 0 / 94 1997-07-22 CSC CORPORATE DOMAINS, INC.
www.microsoft.com 0 / 94 1991-05-02 MarkMonitor Inc.
Contacted IP addresses (19)
IP Detections Autonomous System Country
104.71.214.69 0 / 94 16625 US
114.114.114.114 0 / 94 21859 CN
192.168.0.20 0 / 94 - -
192.168.0.52 0 / 94 - -
192.168.0.60 0 / 94 - -
192.229.211.108 0 / 94 15133 US
20.99.133.109 0 / 94 8075 US
20.99.184.37 0 / 94 8075 US
20.99.185.48 0 / 94 8075 US
204.79.197.203 0 / 94 8068 US
Execution Parents (2)
Scanned Detections Type Name
2025-05-17 62 / 71 Win32 EXE krt_exe.txt
2024-12-17 54 / 68 ZIP malware.zip
Restore pages?
Chromium didn't shut down correctly.
Restore


Execution Parents (2)
Scanned Detections Type Name
2025-05-17 62 / 71 Win32 EXE krt_exe.txt
2024-12-17 54 / 68 ZIP malware.zip
Bundled Files (30)
Scanned Detections File type Name
2022-06-08 0 / 55 JavaScript .rsrc_1
? ? file 16bd8b5d4d5be1c38a32c579b97f47a40f4c484dcfb321b6afa6c64e5a6e6575
? ? file fc5d324ed9985f60185124385edc610aa35c6f7d651629dc154ce79a9bd8ed6e
? ? file afe37b8f4fb59431ecf3a400cb7bc2812cb54741cf1fbce09063039ad7064ec2e
? ? file f511fcfe33677f60521fb7ef13e2a62a6efca06a430a837610443517 5cd9dd1b
? ? file a33df3586a08102482ae77d4f66d08d9e7d4ab01ee2044f7389696fc9da57ae8
? ? file 1f6e708ff53031c020123b60e409779825a9a6dbf5b1085dc3db60a991a0c0f0f
? ? file 5b6b8f1f28b0016dc84108f0d794e02dc260c48b0c564107fabbb922cdb486c1
? ? file 3d1f0a4d38e61a692b3866229b4c9a0a69a2c58103ba2322ed003b969fae293b
? ? file cd562e57f43a266fce120deaf30ac1cf7e2d18db9150ed09f827b2efdcbe9830
Dropped Files (2)
Scanned Detections File type Name
2025-07-06 0 / 62 INI cftmon.exe:Zone.Identifier
2025-05-17 62 / 71 Win32 EXE krt_exe.txt
PE Resource Children (1)
Scanned Detections File type Name
2016-06-13 0 / 56 ? VirusShare_fd9e81b6a232f47376f5043d4bb8da6
Graph Summary
Chromium didn't shut down correctly.
Restore

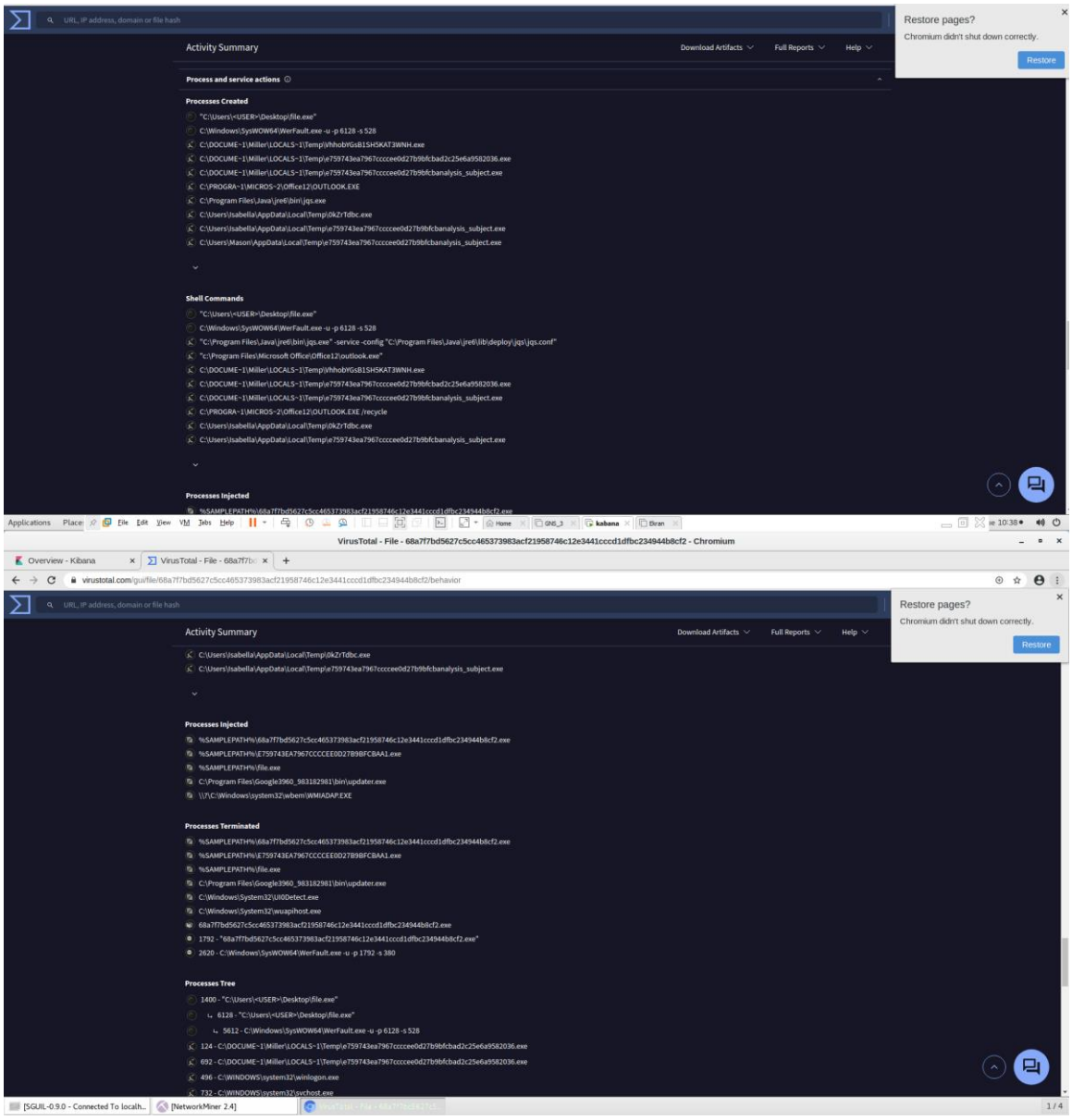

URL, IP address, domain or file hash
2025-07-06 0 / 62 INI cftmon.exe:Zone.Identifier
2025-05-17 62 / 71 Win32 EXE krt_exe.txt
PE Resource Children (1)
Scanned Detections File type Name
2016-06-13 0 / 56 ? VirusShare_fd9e81b6a232f74376f5043d4bb8da6
Graph Summary
10+ contacted ips
10+ bundled files
6 contacted domains
1 contacted urls
1 pe resource children
2 dropped files
2 execution parents
Restore pages?
Chromium didn't shut down correctly.
Restore
Our product
Contact Us
Get Support
Community
Join Community
Vote and Comment
Tools
API Scripts
YARA
Premium Services
Get a demo
Intelligence
Documentation
Searching
Reports
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Display grouped sandbox reports
CAPA
CAPE Sandbox
Lastline
Microsoft Sysinternals
Sangfor ZSand
Tencent HABO
VirusTotal Jujubox
VirusTotal Observer
Zenbox
Activity Summary
Download Artifacts
Full Reports
Help
3 Detections
2 MALWARE 1 EVADER 1 TROJAN
Mitre Signatures
11 LOW 26 INFO
IDS Rules
NOT FOUND
Sigma Rules
NOT FOUND
Dropped Files
82 OTHER 1 PE_EXE 1 TEXT
Network comms
1 HTTP 7 DNS 20 IP
Behavior Tags
checks-user-input detect-debug-environment long-sleeps persistence runtime-modules
Dynamic Analysis Sandbox Detections
The sandbox Zenbox flags this file as: MALWARE EVADER
The sandbox Lastline flags this file as: MALWARE TROJAN
MITRE ATT&CK Tactics and Techniques
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Collection
Command and Control
Malware Behavior Catalog Tree
Anti-Behavioral Analysis
Defense Evasion
Discovery

as we see that is a malwre and a lot of sides

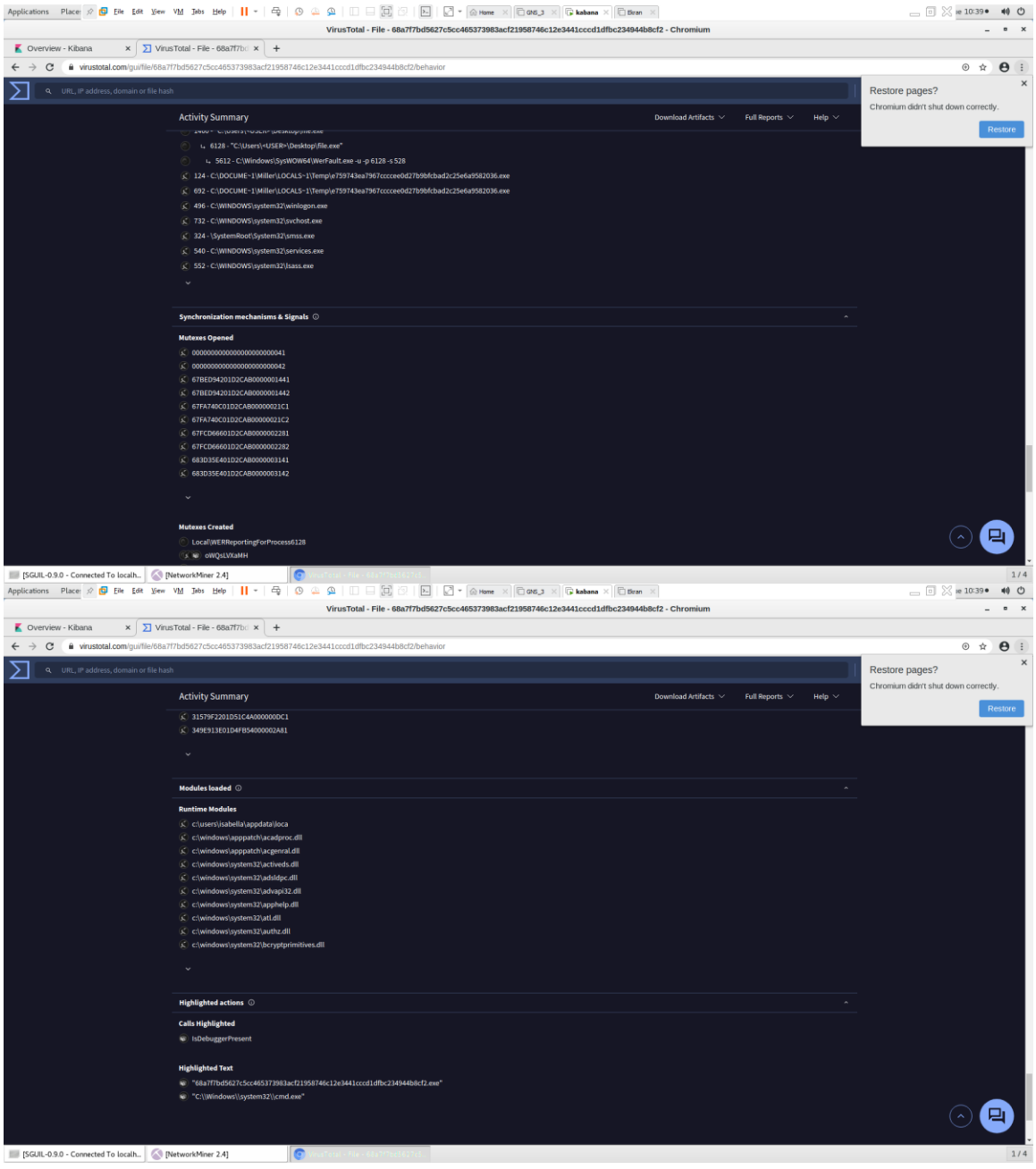
it says it worm



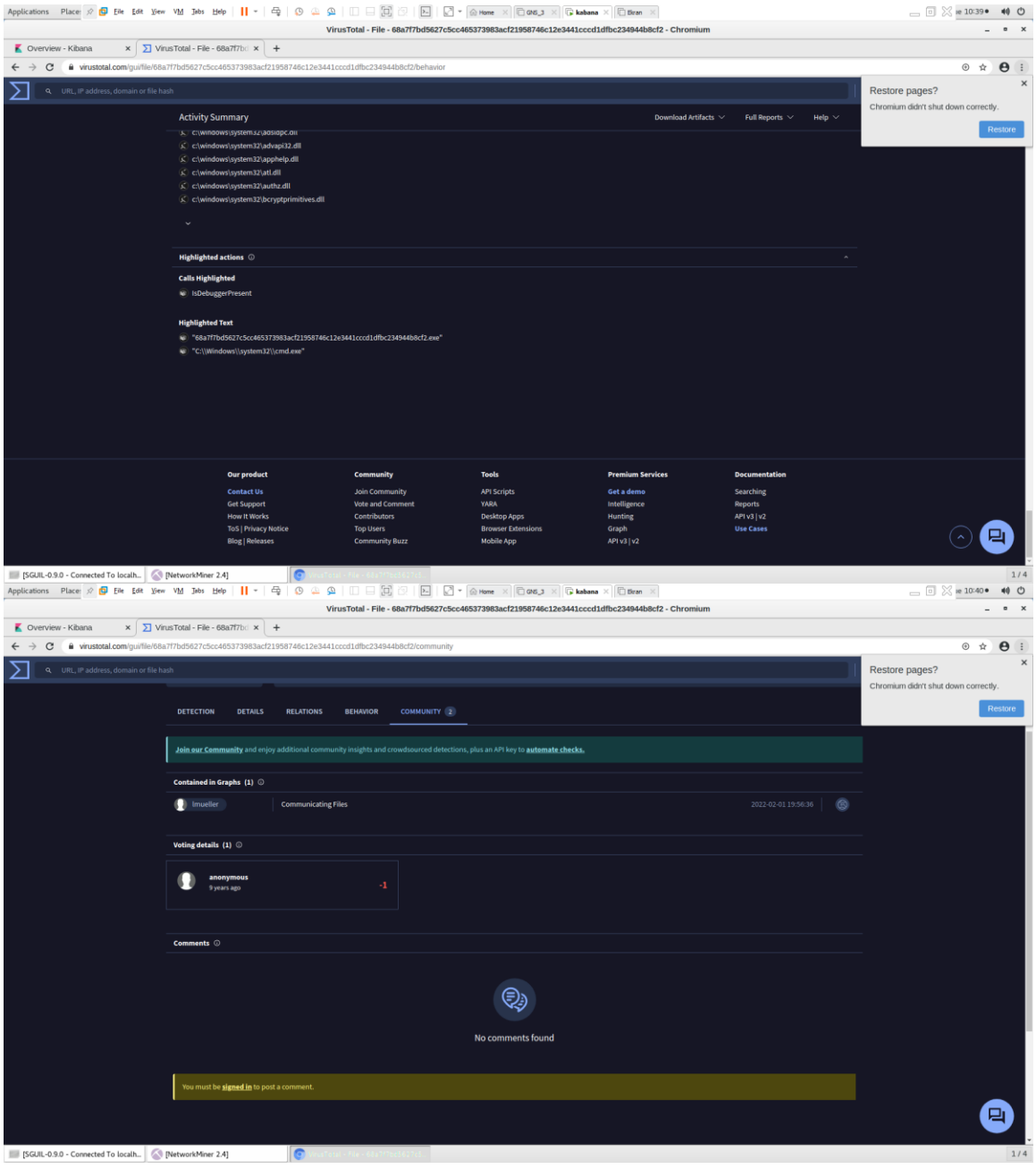

URL, IP address, domain or file hash
Activity Summary
Download Artifacts
Full Reports
Help
Files Deleted
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120D.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER121E.tmp.txt
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1558.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1652.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.txt
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A98.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A99.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1AAA.tmp.txt
C:\ProgramData\Microsoft\Windows\WER\Temp\WER266F.tmp.WERInternalMetadata.xml
Files With Modified Attributes
C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp\Cookies\
C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp\Cookies\index.dat
C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp\History
C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp\History\History.IE5\
C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp\History\History.IE5\index.dat
C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp\Temporary Internet Files
C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp\Temporary Internet Files\Content.IE5
C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp\Temporary Internet Files\Content.IE5\0744BOS8
C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp\Temporary Internet Files\Content.IE5\0744BOS8\desktop.ini
C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp\Temporary Internet Files\Content.IE5\2RNIQID3
Files Dropped
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7156.0
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7156.0\Crashpad
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7156.0\Crashpad\attachments
Restore pages?
Chromium didn't shut down correctly.
Restore
URL, IP address, domain or file hash
Activity Summary
Download Artifacts
Full Reports
Help
Files Dropped
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7156.0
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7156.0\Crashpad
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7156.0\Crashpad\attachments
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7156.0\Crashpad\metadata
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7156.0\Crashpad\reports
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7156.0\uninstall.cmd
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7156.0\updater.exe
C:\Program Files\Google3584_1277712301
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120D.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120D.tmp.WERInternalMetadata.xml
Registry actions
Registry Keys Opened
HKEY_CLASSES_ROOT\http\shell\open\command
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize\AppsUseLightTheme
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\AutoApproveOSDumps
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\BypassDataThrottling
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\BypassNetworkCostThrottling
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\BypassPowerThrottling
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Consent
Registry Keys Set
Restore pages?
Chromium didn't shut down correctly.
Restore
Activity Summary
Download Artifacts
Full Reports
Help
Registry Keys Set
HKLM
HKLM\.AIFC\OPENWITHPROGIDS
HKLM\.AIFF\OPENWITHPROGIDS
HKLM\.AIF\OPENWITHPROGIDS
HKLM\.APPLICATION\OPENWITHPROGIDS
HKLM\.ASF\OPENWITHPROGIDS
HKLM\.ASX\OPENWITHPROGIDS
HKLM\.AU\OPENWITHPROGIDS
HKLM\.AVI\OPENWITHPROGIDS
HKLM\.BMP\OPENWITHPROGIDS
Registry Keys Deleted
HKLM\S-1-5-18\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
HKU\S-1-5-18\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
Process and service actions
Processes Created
"C:\Users\<USER>\Desktop\file.exe"
C:\Windows\SysWOW64\WerFault.exe -u -p 6128 -s 528
C:\DOCUME~1\Miller\LOCALS~1\Temp\VhhobYGsB1SH5KAT3WNH.exe
C:\DOCUME~1\Miller\LOCALS~1\Temp\e759743ea7967ccccee0d27b9bfcbad2c25e6a0582036.exe
C:\DOCUME~1\Miller\LOCALS~1\Temp\e759743ea7967ccccee0d27b9bfcbanalysis_subject.exe
C:\PROGRA~1\MICROS~2\Office12\OUTLOOK.EXE
C:\Program Files\Java\jre6\bin\jqs.exe
C:\Users\Isabella\AppData\Local\Temp\0k2rTdbc.exe


URL, IP address, domain or file hash
Activity Summary
Download Artifacts
Full Reports
Help
Process and service actions
Processes Created
"C:\Users\<USER>\Desktop\file.exe"
C:\Windows\SysWOW64\WerFault.exe -u -p 6128 -s 528
C:\DOCUME~1\Miller\LOCALS~1\Temp\VhhobYGsB1SH5KAT3WNH.exe
C:\DOCUME~1\Miller\LOCALS~1\Temp\e759743ea7967ccccee0d27b9bfcbad2c25e6a9582036.exe
C:\DOCUME~1\Miller\LOCALS~1\Temp\e759743ea7967ccccee0d27b9bfcbanalysis_subject.exe
C:\PROGRA~1\MICROS~2\Office12\OUTLOOK.EXE
C:\Program Files\Java\jre6\bin\jqs.exe
C:\Users\Isabella\AppData\Local\Temp\0kZrTdbc.exe
C:\Users\Isabella\AppData\Local\Temp\e759743ea7967ccccee0d27b9bfcbanalysis_subject.exe
C:\Users\Mason\AppData\Local\Temp\e759743ea7967ccccee0d27b9bfcbanalysis_subject.exe
Shell Commands
"C:\Users\<USER>\Desktop\file.exe"
C:\Windows\SysWOW64\WerFault.exe -u -p 6128 -s 528
"C:\Program Files\Java\jre6\bin\jqs.exe" -service -config "C:\Program Files\Java\jre6\lib\deploy\jqs\jqs.conf"
"c:\Program Files\Microsoft Office\Office12\outlook.exe"
C:\DOCUME~1\Miller\LOCALS~1\Temp\VhhobYGsB1SH5KAT3WNH.exe
C:\DOCUME~1\Miller\LOCALS~1\Temp\e759743ea7967ccccee0d27b9bfcbad2c25e6a9582036.exe
C:\DOCUME~1\Miller\LOCALS~1\Temp\e759743ea7967ccccee0d27b9bfcbanalysis_subject.exe
C:\PROGRA~1\MICROS~2\Office12\OUTLOOK.EXE /recycle
C:\Users\Isabella\AppData\Local\Temp\0kZrTdbc.exe
C:\Users\Isabella\AppData\Local\Temp\e759743ea7967ccccee0d27b9bfcbanalysis_subject.exe
Processes Injected
%SAMPLEPATH%\68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2.exe
Restore pages?
Chromium didn't shut down correctly.
Restore

Applications
Places
File
Edit
View
VM
Tabs
Help
Home
GNS_3
kabana
Ekran
10:38
VirusTotal - File - 68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2 - Chromium
Overview - Kibana
VirusTotal - File - 68a7f7bd
virustotal.com/gui/file/68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2/behavior
URL, IP address, domain or file hash
Activity Summary
Download Artifacts
Full Reports
Help
C:\Users\Isabella\AppData\Local\Temp\0kZrTdbc.exe
C:\Users\Isabella\AppData\Local\Temp\e759743ea7967ccccee0d27b9bfcbanalysis_subject.exe
Processes Injected
%SAMPLEPATH%\68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2.exe
%SAMPLEPATH%\E759743EA7967CCCCEE0D27B9BFCBAA1.exe
%SAMPLEPATH%\file.exe
C:\Program Files\Google\3960_983182981\bin\updater.exe
\\?\C:\Windows\system32\wbem\WMIADAP.EXE
Processes Terminated
%SAMPLEPATH%\68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2.exe
%SAMPLEPATH%\E759743EA7967CCCCEE0D27B9BFCBAA1.exe
%SAMPLEPATH%\file.exe
C:\Program Files\Google\3960_983182981\bin\updater.exe
C:\Windows\System32\UI0Detect.exe
C:\Windows\System32\wuapihost.exe
68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2.exe
1792 - "68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2.exe"
2620 - C:\Windows\SysWOW64\WerFault.exe -u -p 1792 -s 380
Processes Tree
1400 - "C:\Users\<USER>\Desktop\file.exe"
6128 - "C:\Users\<USER>\Desktop\file.exe"
5612 - C:\Windows\SysWOW64\WerFault.exe -u -p 6128 -s 528
124 - C:\DOCUME~1\Miller\LOCALS~1\Temp\e759743ea7967ccccee0d27b9bfcbad2c25e6a9582036.exe
692 - C:\DOCUME~1\Miller\LOCALS~1\Temp\e759743ea7967ccccee0d27b9bfcbad2c25e6a9582036.exe
496 - C:\WINDOWS\system32\winlogon.exe
732 - C:\WINDOWS\system32\svchost.exe
Restore pages?
Chromium didn't shut down correctly.
Restore
[SGUIL-0.9.0 - Connected To localh...
[NetworkMiner 2.4]
1 / 4

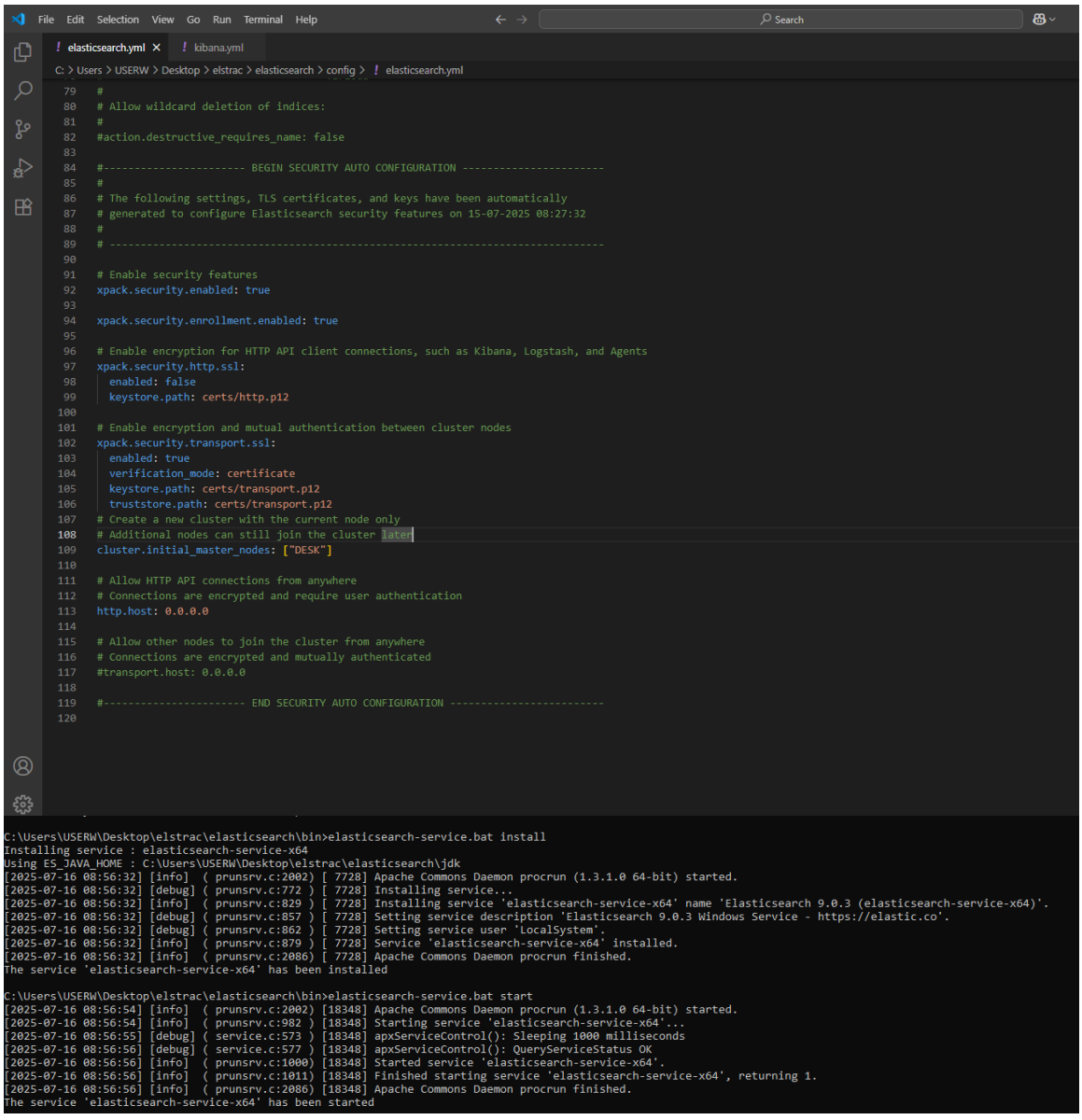

VirusTotal - File - 68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2 - Chromium
virustotal.com/gui/file/68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2/behavior
Restore pages?
Chromium didn't shut down correctly.
Restore
Activity Summary
Download Artifacts
Full Reports
Help
6128 - "C:\Users\<USER>\Desktop\file.exe"
5612 - C:\Windows\SysWOW64\WerFault.exe -u -p 6128 -s 528
124 - C:\DOCUME~1\Miller\LOCALS~1\Temp\e759743ea7967cccceе0d27b9bfcbad2c25e6a9582036.exe
692 - C:\DOCUME~1\Miller\LOCALS~1\Temp\e759743ea7967cccceе0d27b9bfcbad2c25e6a9582036.exe
496 - C:\WINDOWS\system32\winlogon.exe
732 - C:\WINDOWS\system32\svchost.exe
324 - \SystemRoot\System32\smss.exe
540 - C:\WINDOWS\system32\services.exe
552 - C:\WINDOWS\system32\lsass.exe
Synchronization mechanisms & Signals
Mutexes Opened
00000000000000000000000041
00000000000000000000000042
67BED94201D2CAB0000001441
67BED94201D2CAB0000001442
67FA740C01D2CAB00000021C1
67FA740C01D2CAB00000021C2
67FCD66601D2CAB0000002281
67FCD66601D2CAB0000002282
683D35E401D2CAB0000003141
683D35E401D2CAB0000003142
Mutexes Created
Local\WERReportingForProcess6128
oWQsLlXaMH
[SGUIL-0.9.0 - Connected To localh...
[NetworkMiner 2.4]
1 / 4

VirusTotal - File - 68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2 - Chromium
virustotal.com/gui/file/68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2/behavior
Restore pages?
Chromium didn't shut down correctly.
Restore
Activity Summary
Download Artifacts
Full Reports
Help
31579F2201D51C4A000000DC1
349E913E01D4FB54000002A81
Modules loaded
Runtime Modules
c:\users\isabella\appdata\loca
c:\windows\apppatch\acadproc.dll
c:\windows\apppatch\acgenral.dll
c:\windows\system32\activeds.dll
c:\windows\system32\adsldpc.dll
c:\windows\system32\advapi32.dll
c:\windows\system32\apphelp.dll
c:\windows\system32\atl.dll
c:\windows\system32\authz.dll
c:\windows\system32\bcryptprimitives.dll
Highlighted actions
Calls Highlighted
IsDebuggerPresent
Highlighted Text
"68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2.exe"
"C:\\Windows\\system32\\cmd.exe"
[SGUIL-0.9.0 - Connected To localh...
[NetworkMiner 2.4]
1 / 4


VirusTotal - File - 68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2 - Chromium
virustotal.com/gui/file/68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2/behavior
Restore pages?
Chromium didn't shut down correctly.
Restore
Activity Summary
Download Artifacts
Full Reports
Help
c:\windows\system32\advapi32.dll
c:\windows\system32\apphelp.dll
c:\windows\system32\atl.dll
c:\windows\system32\authz.dll
c:\windows\system32\bcryptprimitives.dll
Highlighted actions
Calls Highlighted
IsDebuggerPresent
Highlighted Text
"68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2.exe"
"C:\\Windows\\system32\\cmd.exe"
Our product
Contact Us
Get Support
How It Works
ToS | Privacy Notice
Blog | Releases
Community
Join Community
Vote and Comment
Contributors
Top Users
Community Buzz
Tools
API Scripts
YARA
Desktop Apps
Browser Extensions
Mobile App
Premium Services
Get a demo
Intelligence
Hunting
Graph
API v3 | v2
Documentation
Searching
Reports
API v3 | v2
Use Cases
[SGUIL-0.9.0 - Connected To localh...
[NetworkMiner 2.4]
1 / 4
VirusTotal - File - 68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2 - Chromium
virustotal.com/gui/file/68a7f7bd5627c5cc465373983acf21958746c12e3441cccd1dfbc234944b8cf2/community
Restore pages?
Chromium didn't shut down correctly.
Restore
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 2
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Contained in Graphs (1)
lmueller
Communicating Files
2022-02-01 19:56:36
Voting details (1)
anonymous
9 years ago
-1
Comments
No comments found
You must be signed in to post a comment.
[SGUIL-0.9.0 - Connected To localh...
[NetworkMiner 2.4]
1 / 4

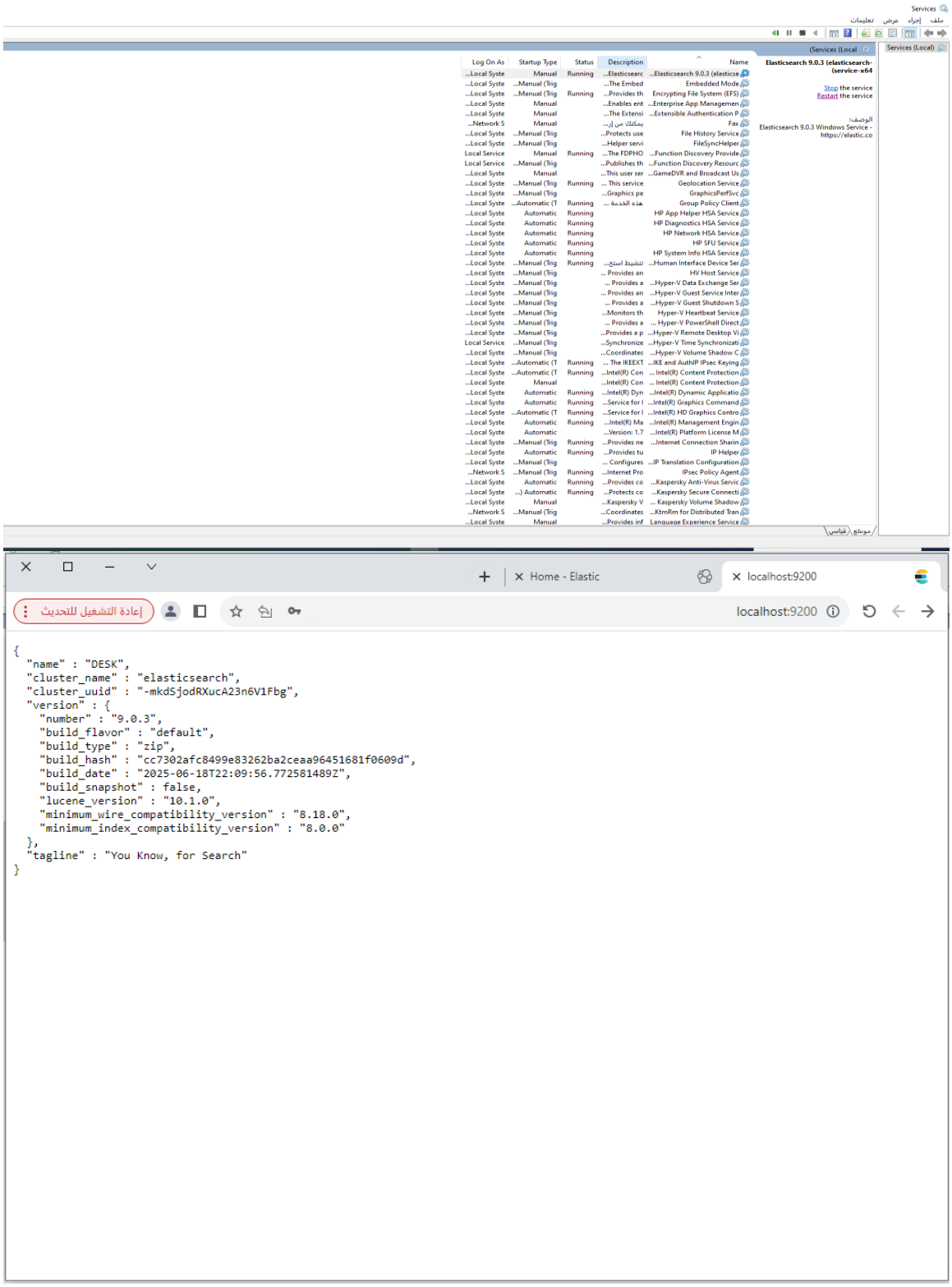
secondly using elsticsearch :-

this is file of elsticsearch.yml that we edited then we installed the services to pc

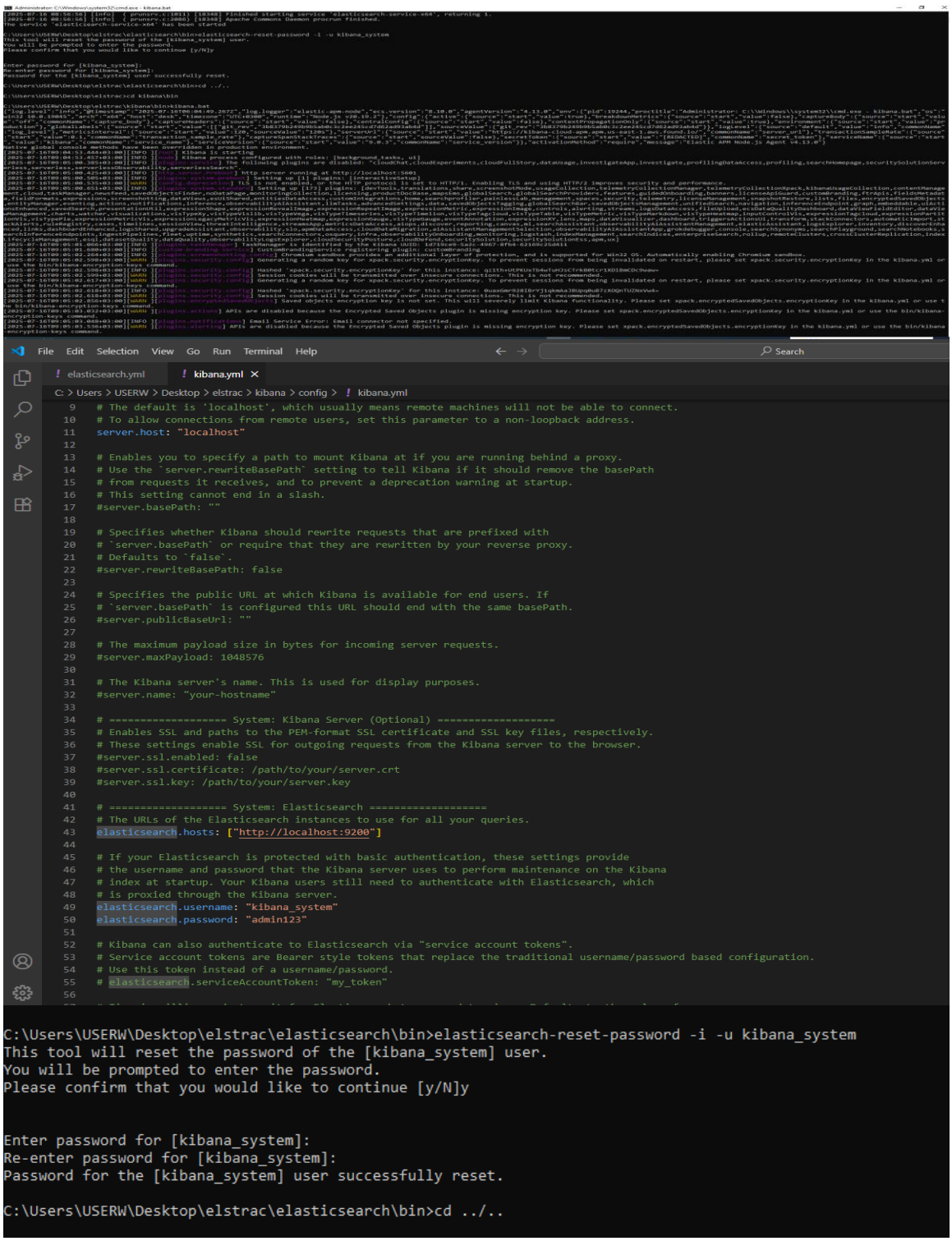


Then we will start the services and loging

To localhost:9200

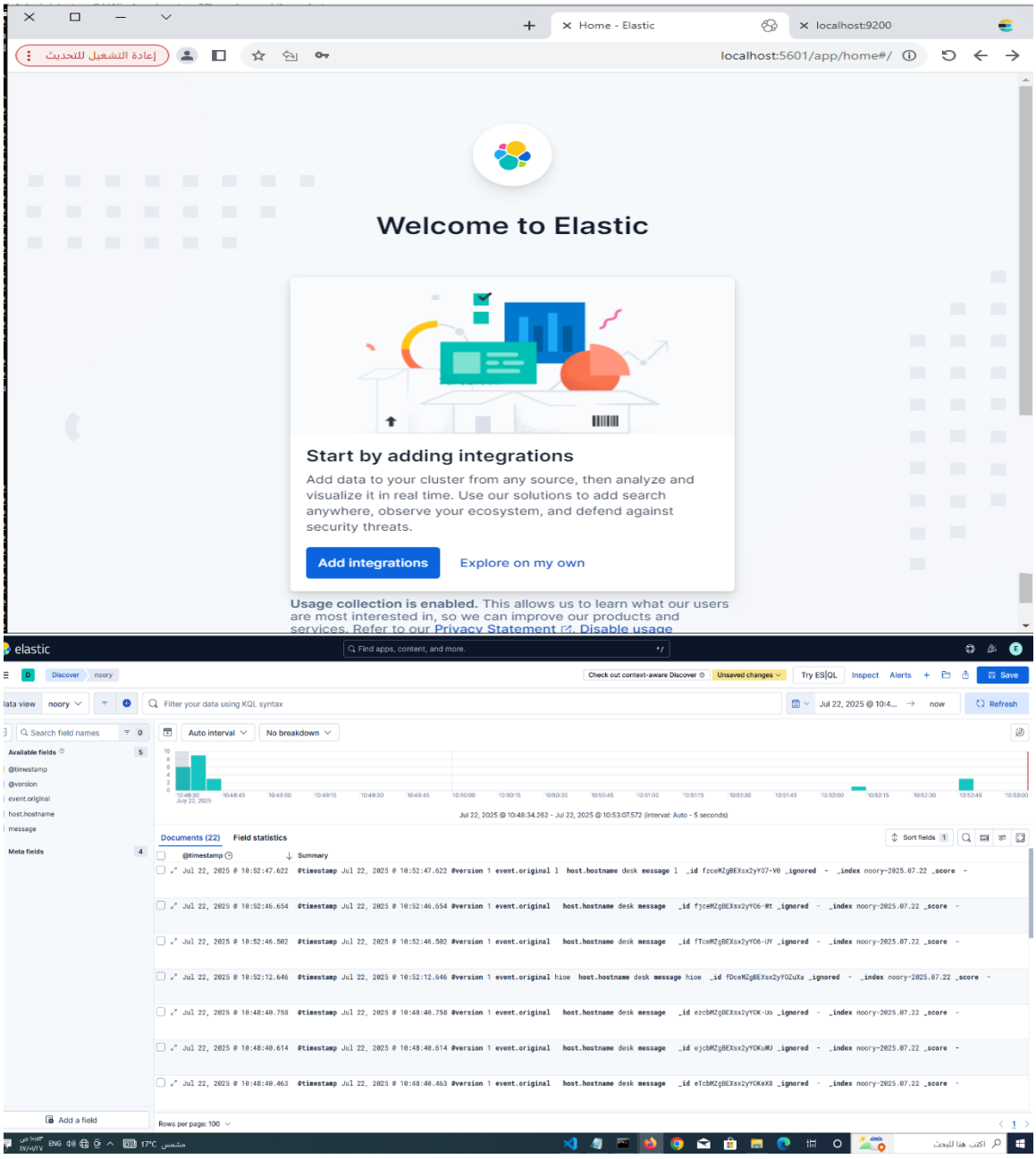


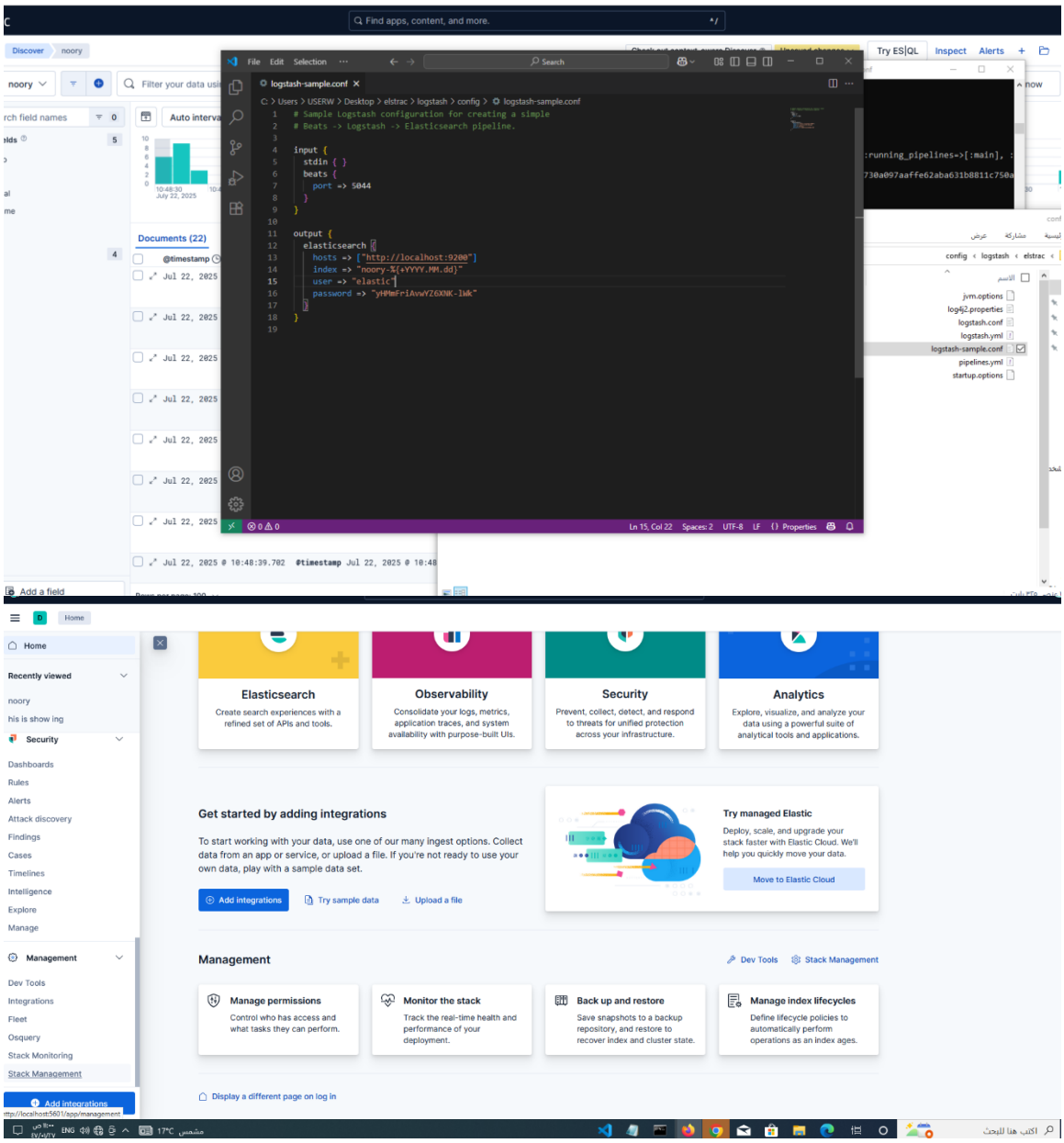
this command is to restet default password after that we will use kibana and edited file of kibana.yaml



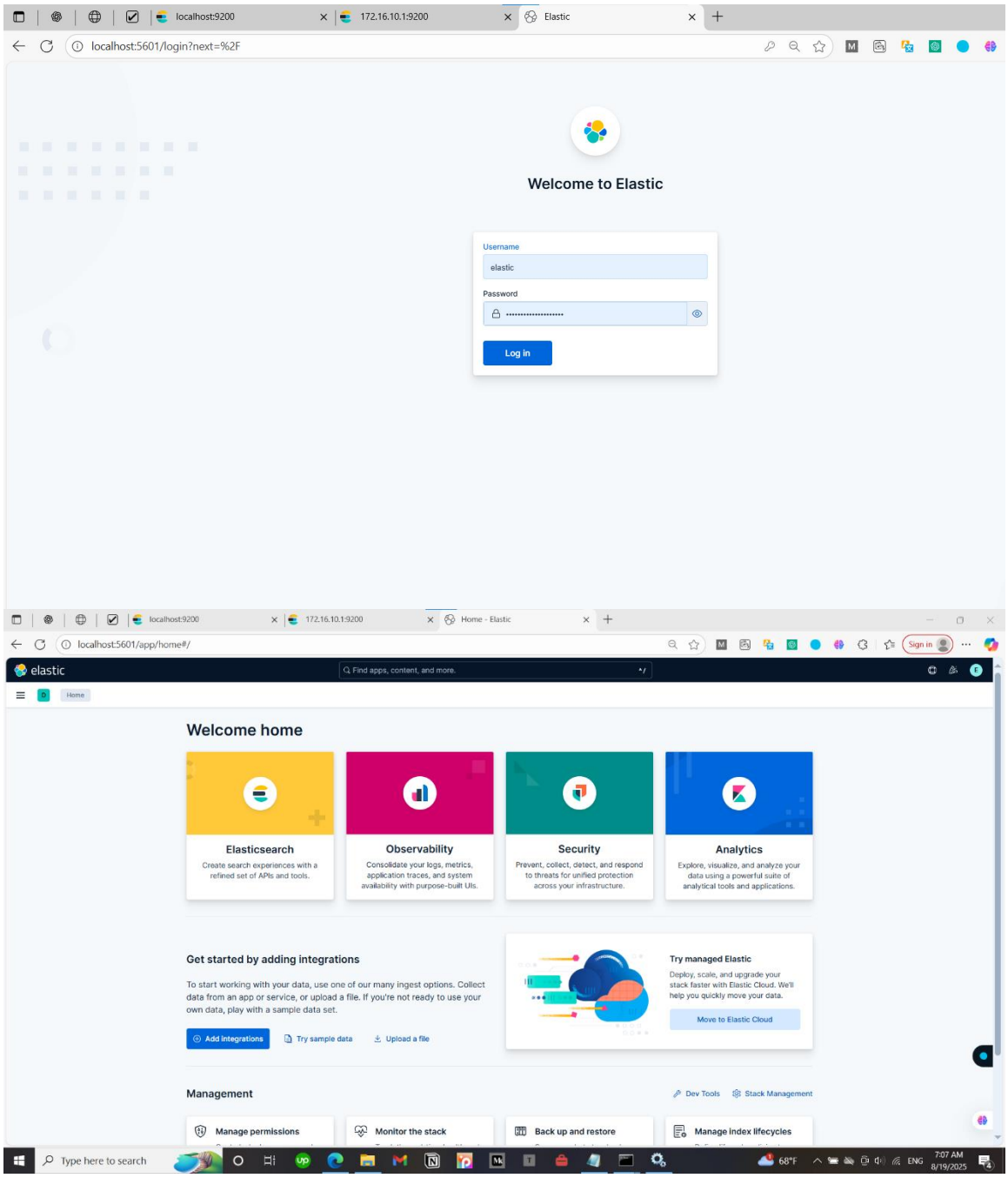
After that we will login to kibanab after run it by login to

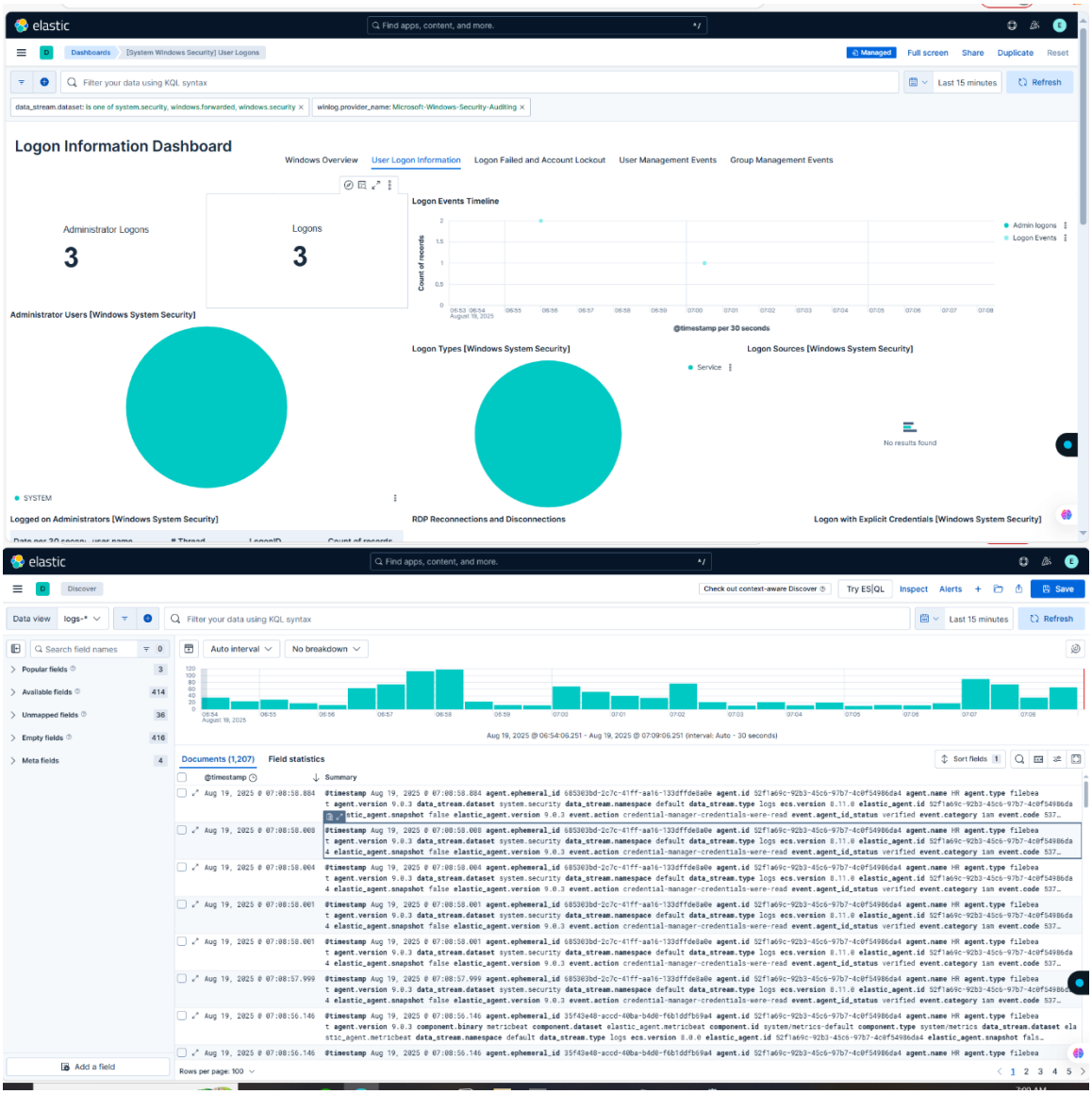
Localhost:5601



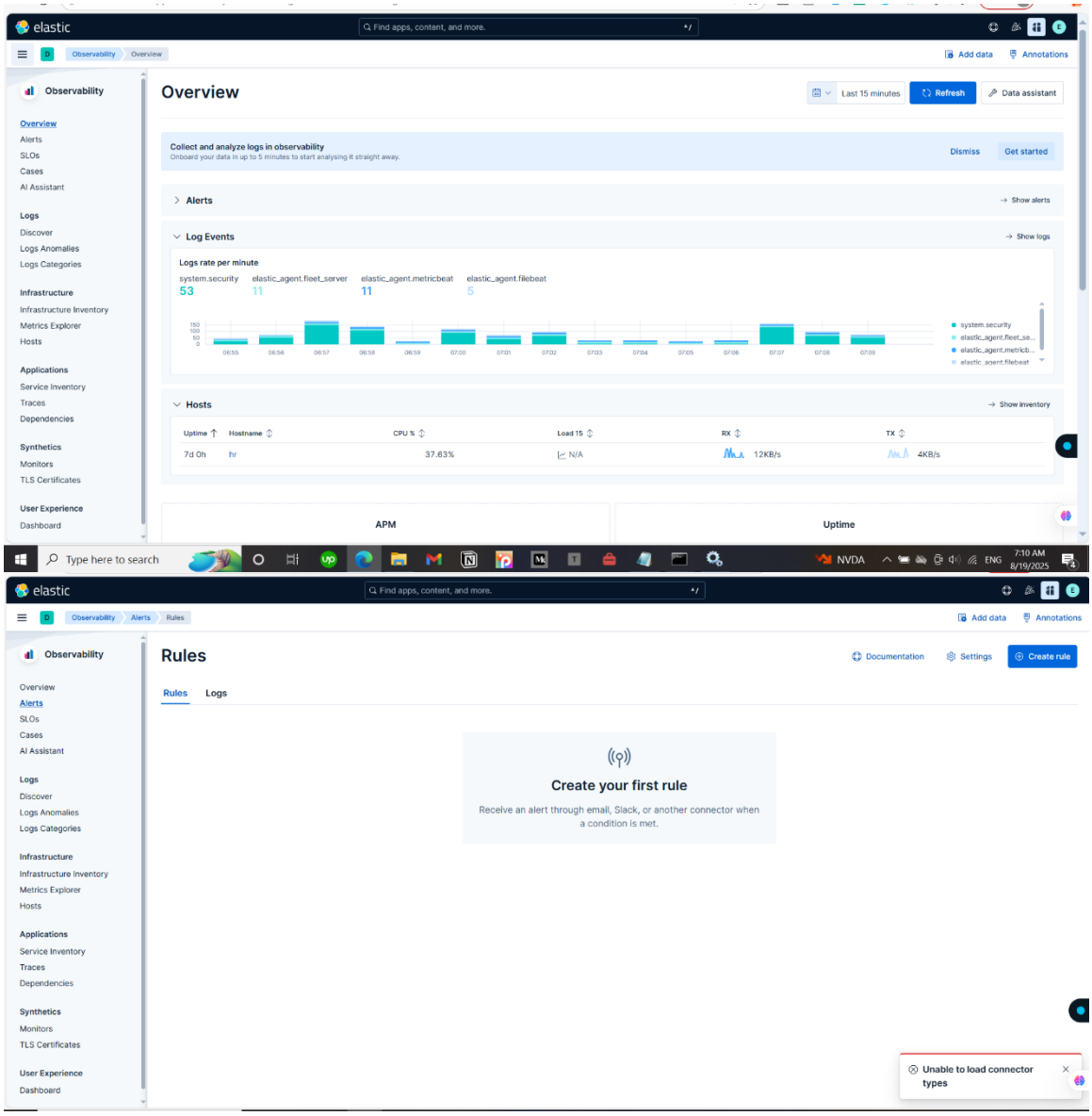


as we will see that is run successfully again will will login as and will inter the user name elstic and the password that we reset it from

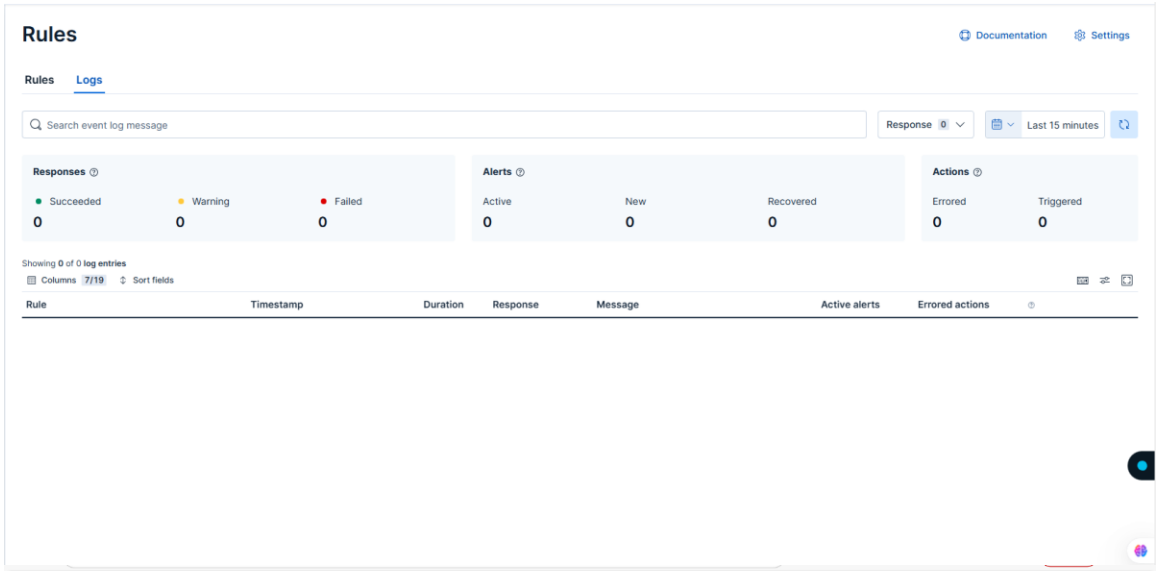

localhost:9200
172.16.10.1:9200
Elastic
localhost:5601/login?next=%2F
Welcome to Elastic
Username
elastic
Password
Log in
localhost:5601/app/home#/
Home - Elastic
Sign in
elastic
Find apps, content, and more.
Home
Welcome home
Elasticsearch
Create search experiences with a refined set of APIs and tools.
Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.
Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.
Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.
Get started by adding integrations
To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.
Add integrations
Try sample data
Upload a file
Try managed Elastic
Deploy, scale, and upgrade your stack faster with Elastic Cloud. We'll help you quickly move your data.
Move to Elastic Cloud
Management
Dev Tools
Stack Management
Manage permissions
Monitor the stack
Back up and restore
Manage index lifecycles
Type here to search
68°F
ENG
7:07 AM
8/19/2025

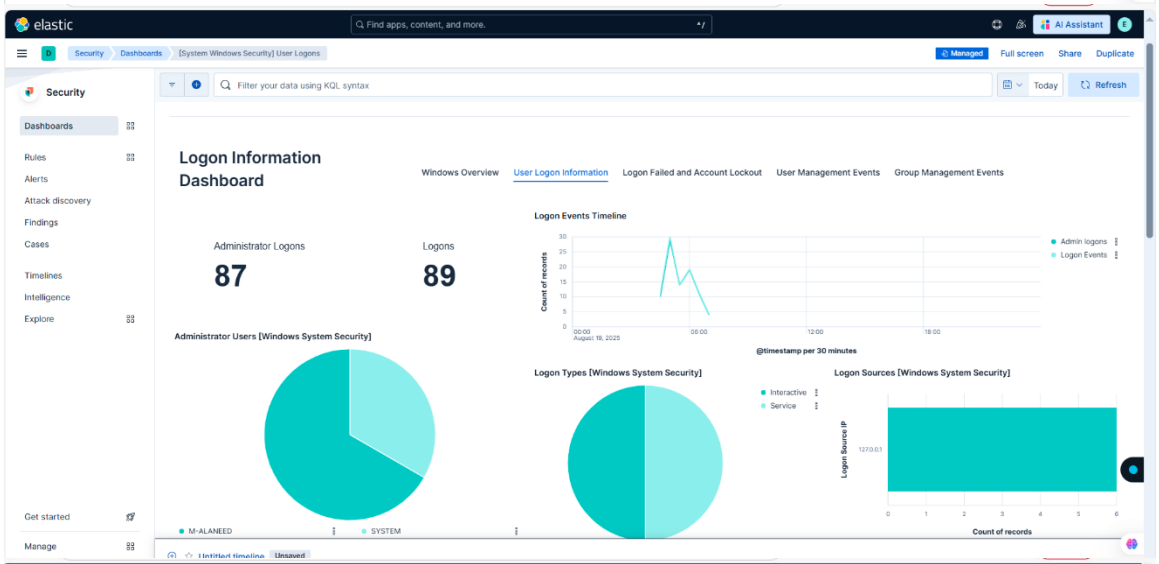

elastic
Find apps, content, and more.
Dashboards
[System Windows Security] User Logons
Managed
Full screen
Share
Duplicate
Reset
Filter your data using KQL syntax
Last 15 minutes
Refresh
data_stream.dataset: is one of system.security, windows.forwarded, windows.security
winlog.provider_name: Microsoft-Windows-Security-Auditing
Logon Information Dashboard
Windows Overview
User Logon Information
Logon Failed and Account Lockout
User Management Events
Group Management Events
Administrator Logons
3
Logons
3
Logon Events Timeline
Count of records
Admin logons
Logon Events
@timestamp per 30 seconds
Administrator Users [Windows System Security]
SYSTEM
Logon Types [Windows System Security]
Logon Sources [Windows System Security]
Service
No results found
Logged on Administrators [Windows System Security]
RDP Reconnections and Disconnections
Logon with Explicit Credentials [Windows System Security]

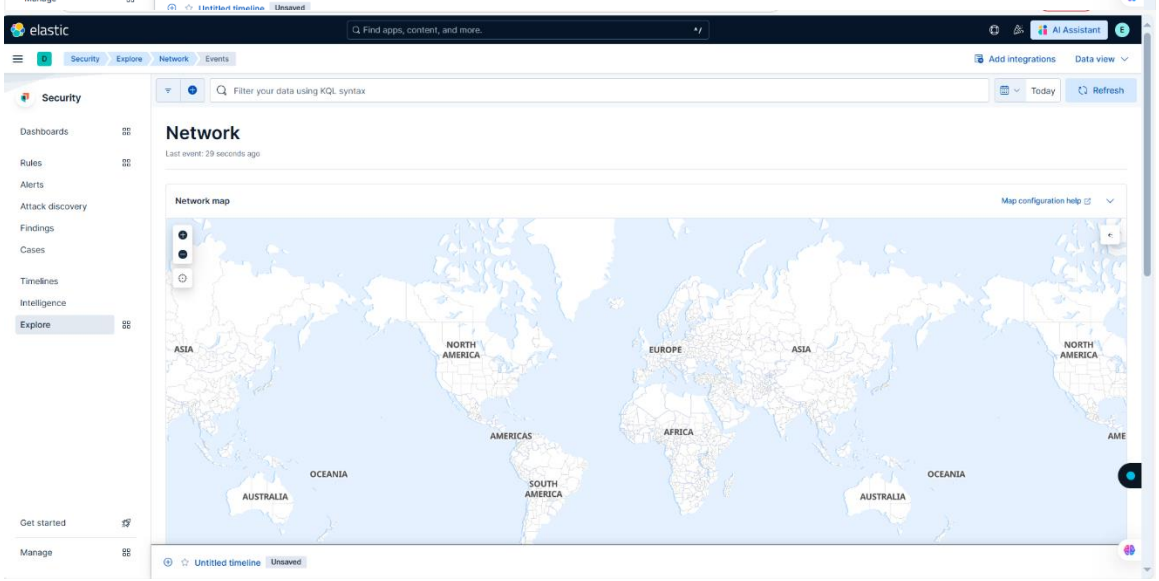
elastic
Find apps, content, and more.
Discover
Check out context-aware Discover
Try ES|QL
Inspect
Alerts
Save
Data view
logs-*
Filter your data using KQL syntax
Last 15 minutes
Refresh
Search field names
Popular fields 3
Available fields 414
Unmapped fields 36
Empty fields 416
Meta fields 4
Add a field
Auto interval
No breakdown
Aug 19, 2025 @ 06:54:06.251 - Aug 19, 2025 @ 07:09:06.251 (interval: Auto - 30 seconds)
Documents (1,207)
Field statistics
Sort fields
@timestamp
Summary
Rows per page: 100

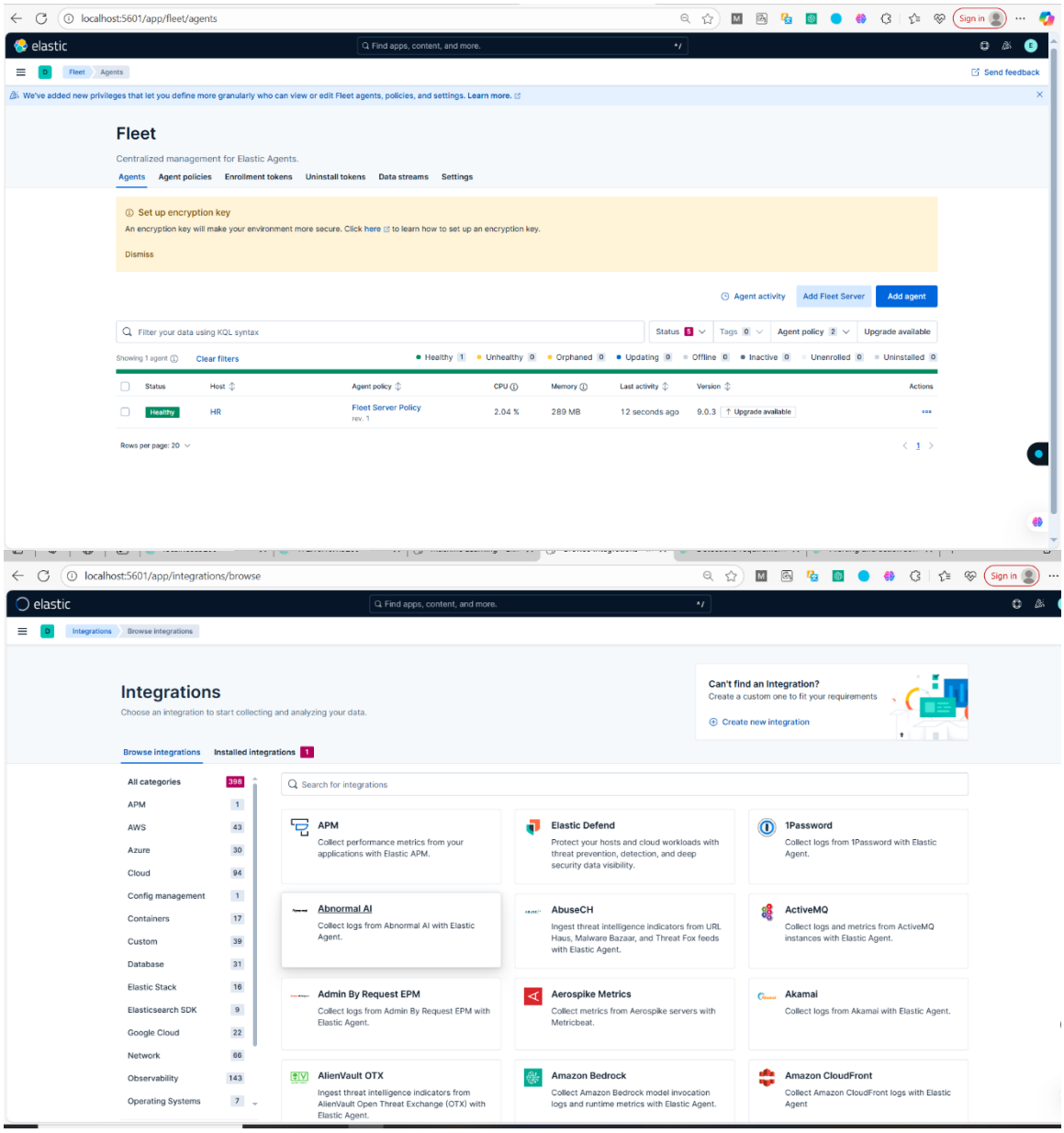

elastic
Find apps, content, and more.
Observability
Overview
Add data
Annotations
Observability
Overview
Alerts
SLOs
Cases
AI Assistant
Logs
Discover
Logs Anomalies
Logs Categories
Infrastructure
Infrastructure Inventory
Metrics Explorer
Hosts
Applications
Service Inventory
Traces
Dependencies
Synthetics
Monitors
TLS Certificates
User Experience
Dashboard
Overview
Last 15 minutes
Refresh
Data assistant
Collect and analyze logs in observability
Onboard your data in up to 5 minutes to start analysing it straight away.
Dismiss
Get started
Alerts
Show alerts
Log Events
Show logs
Logs rate per minute
system.security
53
elastic_agent.fleet_server
11
elastic_agent.metricbeat
11
elastic_agent.filebeat
5
Hosts
Show inventory
Uptime
Hostname
CPU %
Load 15
RX
TX
7d 0h
hr
37.63%
N/A
12KB/s
4KB/s
APM
Uptime
Type here to search
NVDA
ENG
7:10 AM
8/19/2025

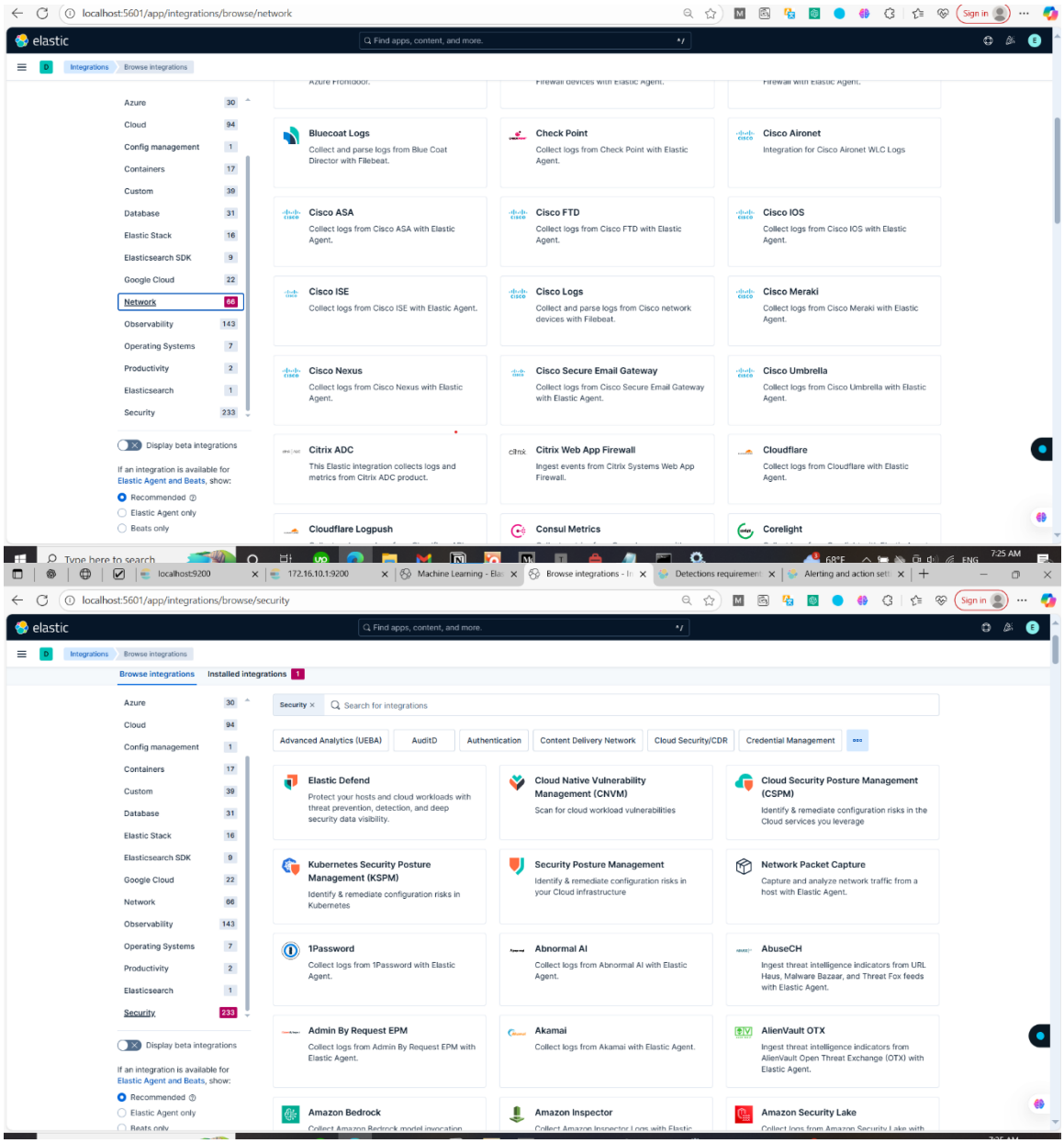
elastic
Find apps, content, and more.
Observability
Alerts
Rules
Add data
Annotations
Observability
Overview
Alerts
SLOs
Cases
AI Assistant
Logs
Discover
Logs Anomalies
Logs Categories
Infrastructure
Infrastructure Inventory
Metrics Explorer
Hosts
Applications
Service Inventory
Traces
Dependencies
Synthetics
Monitors
TLS Certificates
User Experience
Dashboard
Rules
Documentation
Settings
Create rule
Rules
Logs
Create your first rule
Receive an alert through email, Slack, or another connector when a condition is met.
Unable to load connector types


Rules
Documentation
Settings
Rules
Logs
Search event log message
Response 0
Last 15 minutes
Responses
Succeeded
0
Warning
0
Failed
0
Alerts
Active
0
New
0
Recovered
0
Actions
Errored
0
Triggered
0
Showing 0 of 0 log entries
Columns 7/19
Sort fields
Rule
Timestamp
Duration
Response
Message
Active alerts
Errored actions


elastic
Find apps, content, and more.
AI Assistant
Security
Dashboards
[System Windows Security] User Logons
Managed
Full screen
Share
Duplicate
Filter your data using KQL syntax
Today
Refresh
Logon Information Dashboard
Windows Overview
User Logon Information
Logon Failed and Account Lockout
User Management Events
Group Management Events
Administrator Logons
87
Logons
89
Logon Events Timeline
Admin logons
Logon Events
Count of records
@timestamp per 30 minutes
Administrator Users [Windows System Security]
M-ALANEED
SYSTEM
Logon Types [Windows System Security]
Interactive
Service
Logon Sources [Windows System Security]
Logon Source IP
Count of records
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Timelines
Intelligence
Explore
Get started
Manage


elastic
Find apps, content, and more.
AI Assistant
Security
Explore
Network
Events
Add integrations
Data view
Filter your data using KQL syntax
Today
Refresh
Network
Last event: 29 seconds ago
Network map
Map configuration help
ASIA
NORTH AMERICA
EUROPE
ASIA
NORTH AMERICA
AMERICAS
AFRICA
OCEANIA
AUSTRALIA
SOUTH AMERICA
OCEANIA
AUSTRALIA
Untitled timeline
Unsaved


localhost:5601/app/fleet/agents
elastic
Find apps, content, and more.
Fleet
Agents
Send feedback
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Uninstall tokens
Data streams
Settings
Set up encryption key
An encryption key will make your environment more secure. Click here to learn how to set up an encryption key.
Dismiss
Agent activity
Add Fleet Server
Add agent
Filter your data using KQL syntax
Status
Tags
Agent policy
Upgrade available
Showing 1 agent
Clear filters
Healthy
Unhealthy
Orphaned
Updating
Offline
Inactive
Unenrolled
Uninstalled
Status
Host
Agent policy
CPU
Memory
Last activity
Version
Actions
Healthy
HR
Fleet Server Policy
rev. 1
2.04 %
289 MB
12 seconds ago
9.0.3
Upgrade available
Rows per page: 20
1
localhost:5601/app/integrations/browse
elastic
Find apps, content, and more.
Integrations
Browse integrations
Integrations
Choose an integration to start collecting and analyzing your data.
Can't find an Integration?
Create a custom one to fit your requirements
Create new integration
Browse integrations
Installed integrations
1
All categories
398
APM
1
AWS
43
Azure
30
Cloud
94
Config management
1
Containers
17
Custom
39
Database
31
Elastic Stack
16
Elasticsearch SDK
9
Google Cloud
22
Network
66
Observability
143
Operating Systems
7
Search for integrations
APM
Collect performance metrics from your applications with Elastic APM.
Elastic Defend
Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.
1Password
Collect logs from 1Password with Elastic Agent.
Abnormal AI
Collect logs from Abnormal AI with Elastic Agent.
AbuseCH
Ingest threat intelligence indicators from URL Haus, Malware Bazaar, and Threat Fox feeds with Elastic Agent.
ActiveMQ
Collect logs and metrics from ActiveMQ instances with Elastic Agent.
Admin By Request EPM
Collect logs from Admin By Request EPM with Elastic Agent.
Aerospike Metrics
Collect metrics from Aerospike servers with Metricbeat.
Akamai
Collect logs from Akamai with Elastic Agent.
AlienVault OTX
Ingest threat intelligence indicators from AlienVault Open Threat Exchange (OTX) with Elastic Agent.
Amazon Bedrock
Collect Amazon Bedrock model invocation logs and runtime metrics with Elastic Agent.
Amazon CloudFront
Collect Amazon CloudFront logs with Elastic Agent

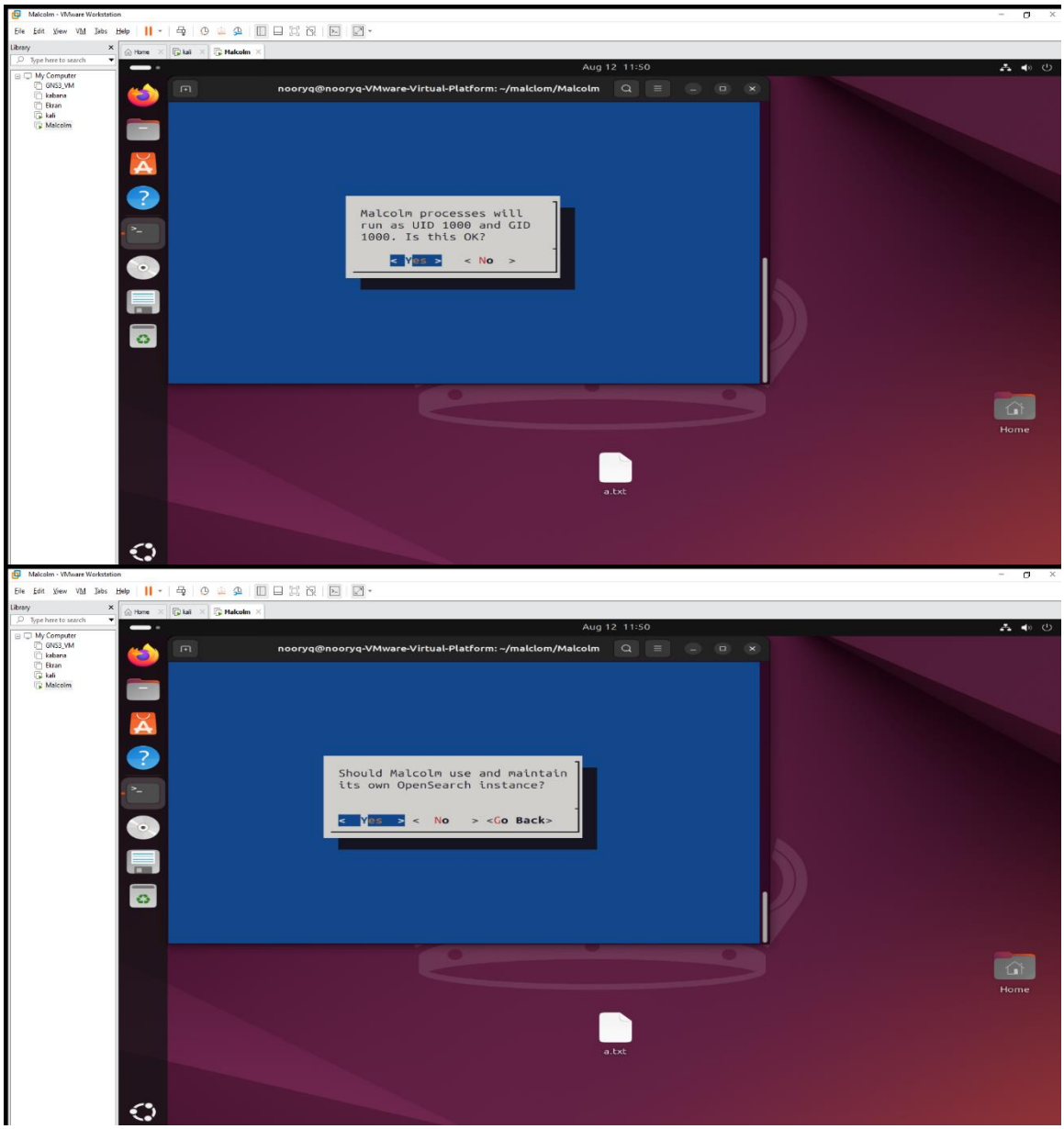


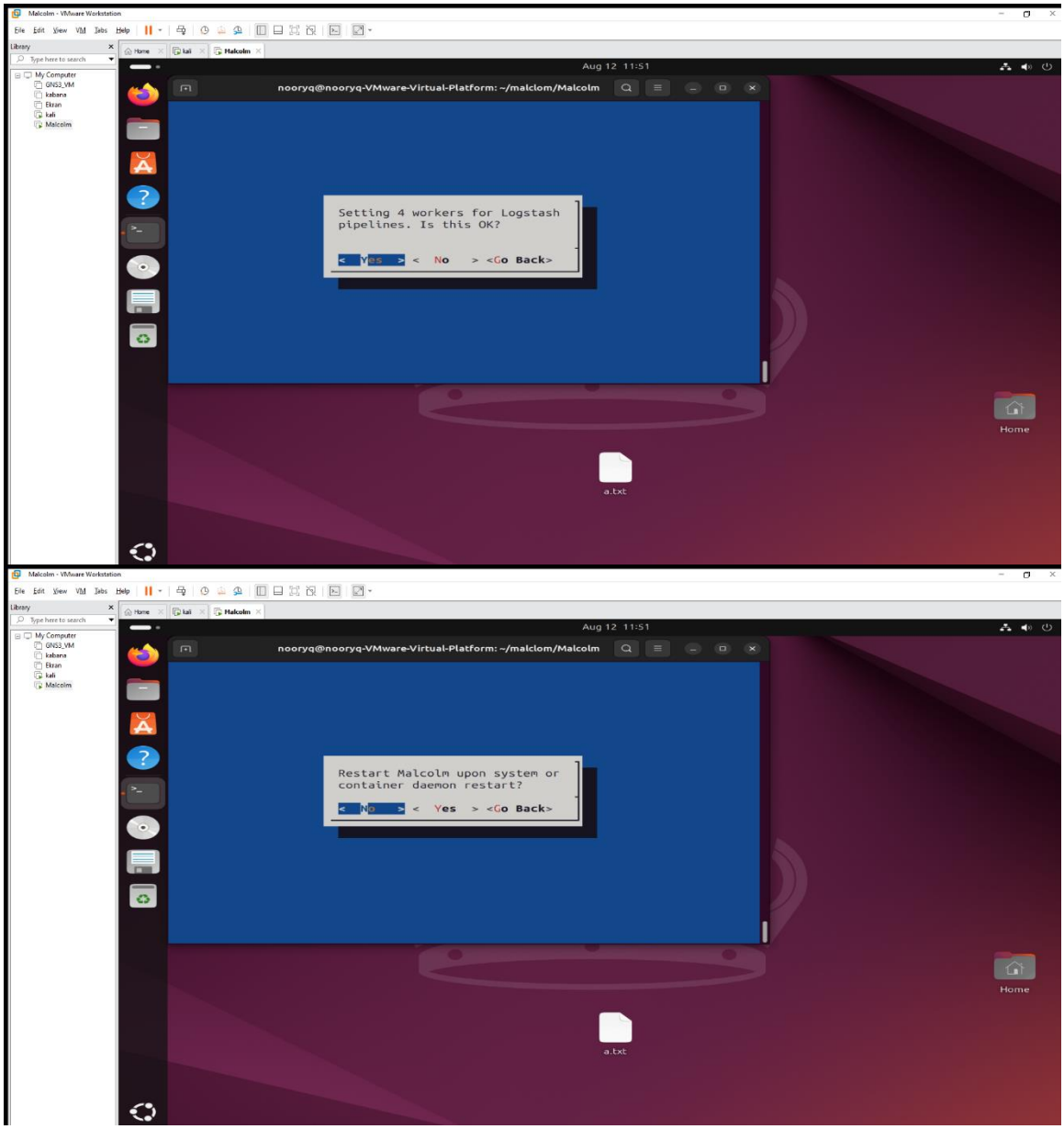
This is all what that we use in kibana and elsticsearch and how we configure it and so …..

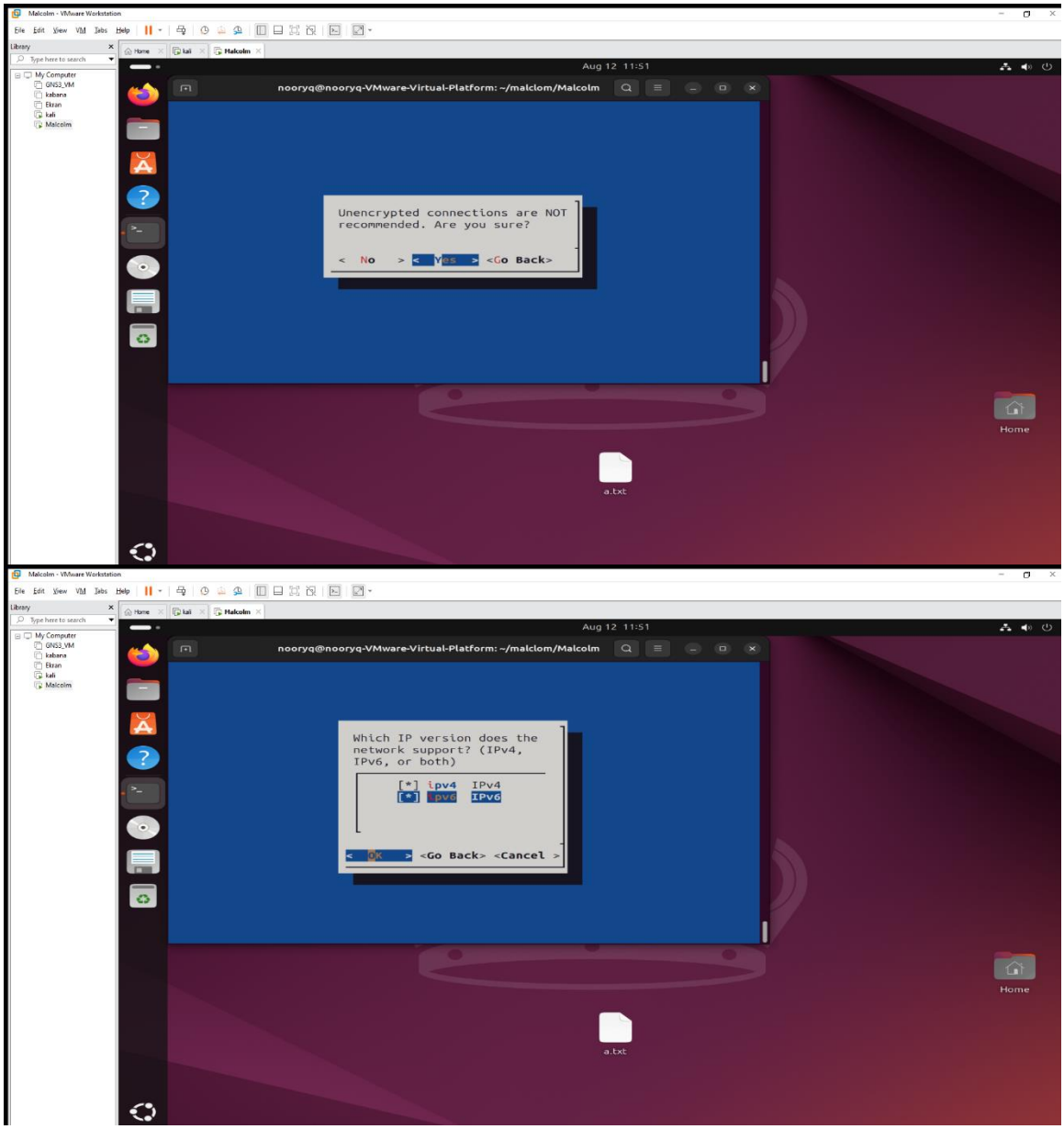
Then we install Ubuntu and configure in it Malcolm for dedication in first computer from right that next to window … the user name of Ubuntu is nooryq and password is noory777#

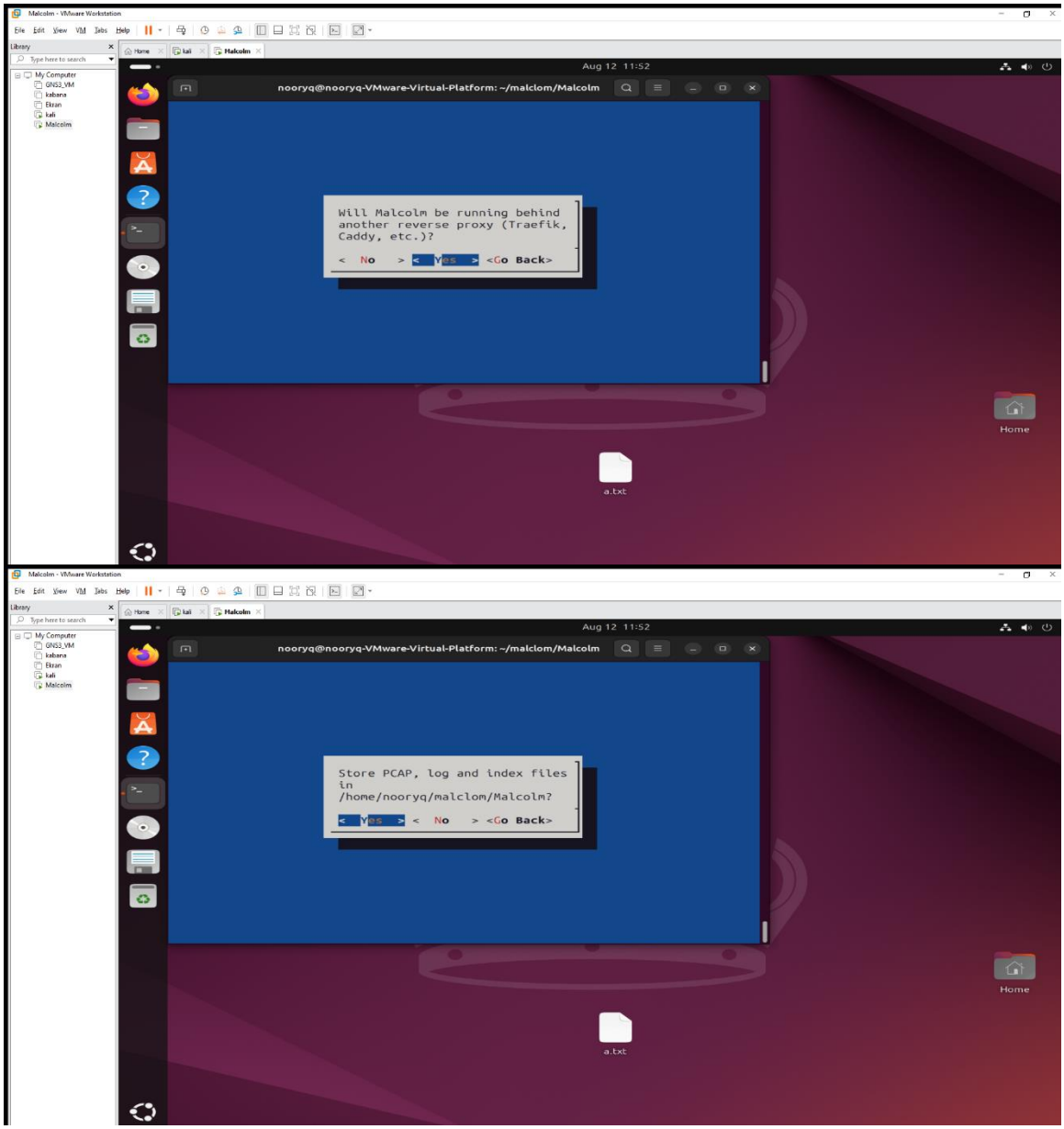
I install Malcolm in file named malclom/Malcolm then we type this command to run malcolm

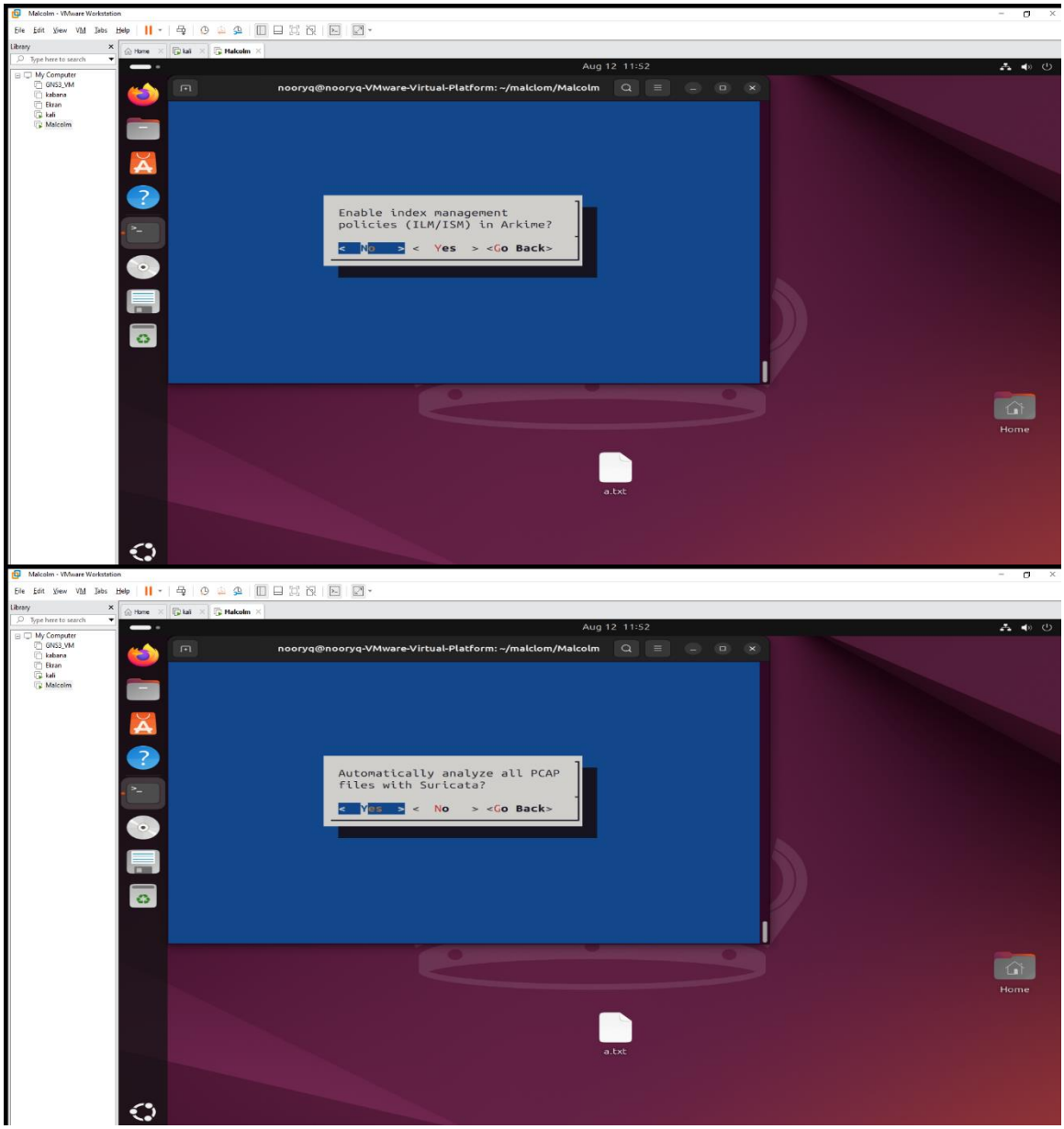
Sudo / malclom/Malcolm/ .secript install.py then it will appear as this



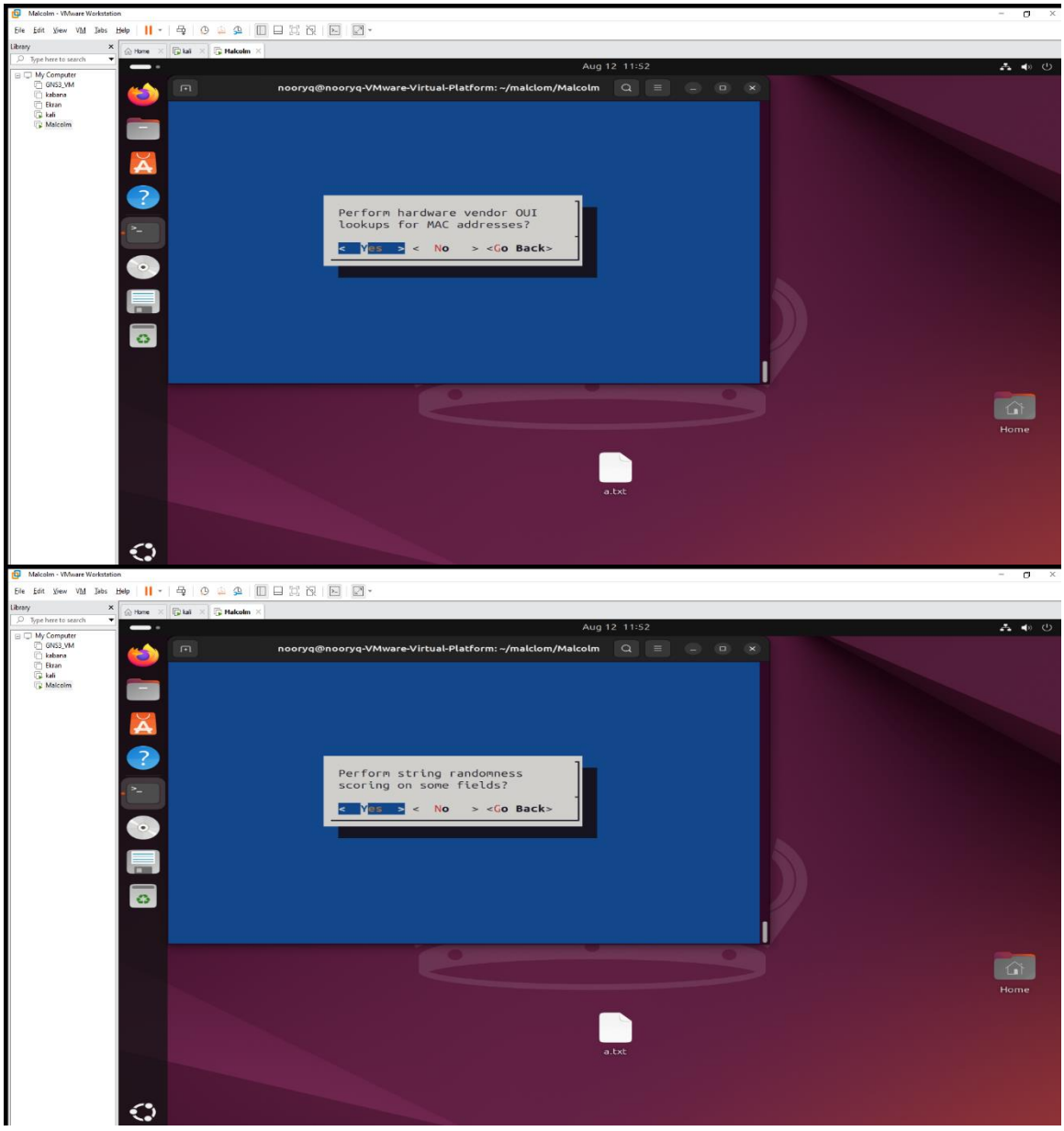

Malcolm - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS3_VM
kabana
Ekran
kali
Malcolm
Home
kali
Malcolm
Aug 12 11:51
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Setting 4 workers for Logstash pipelines. Is this OK?
< Yes > < No > <Go Back>
Home
a.txt
Malcolm - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS3_VM
kabana
Ekran
kali
Malcolm
Home
kali
Malcolm
Aug 12 11:51
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Restart Malcolm upon system or container daemon restart?
< No > < Yes > <Go Back>
Home
a.txt


Malcolm - VMware Workstation
Aug 12 11:51
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Unencrypted connections are NOT recommended. Are you sure?
< No > < Yes > <Go Back>
Home
a.txt
Malcolm - VMware Workstation
Aug 12 11:51
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Which IP version does the network support? (IPv4, IPv6, or both)
[*] ipv4 IPv4
[*] ipv6 IPv6
< OK > <Go Back> <Cancel >
Home
a.txt

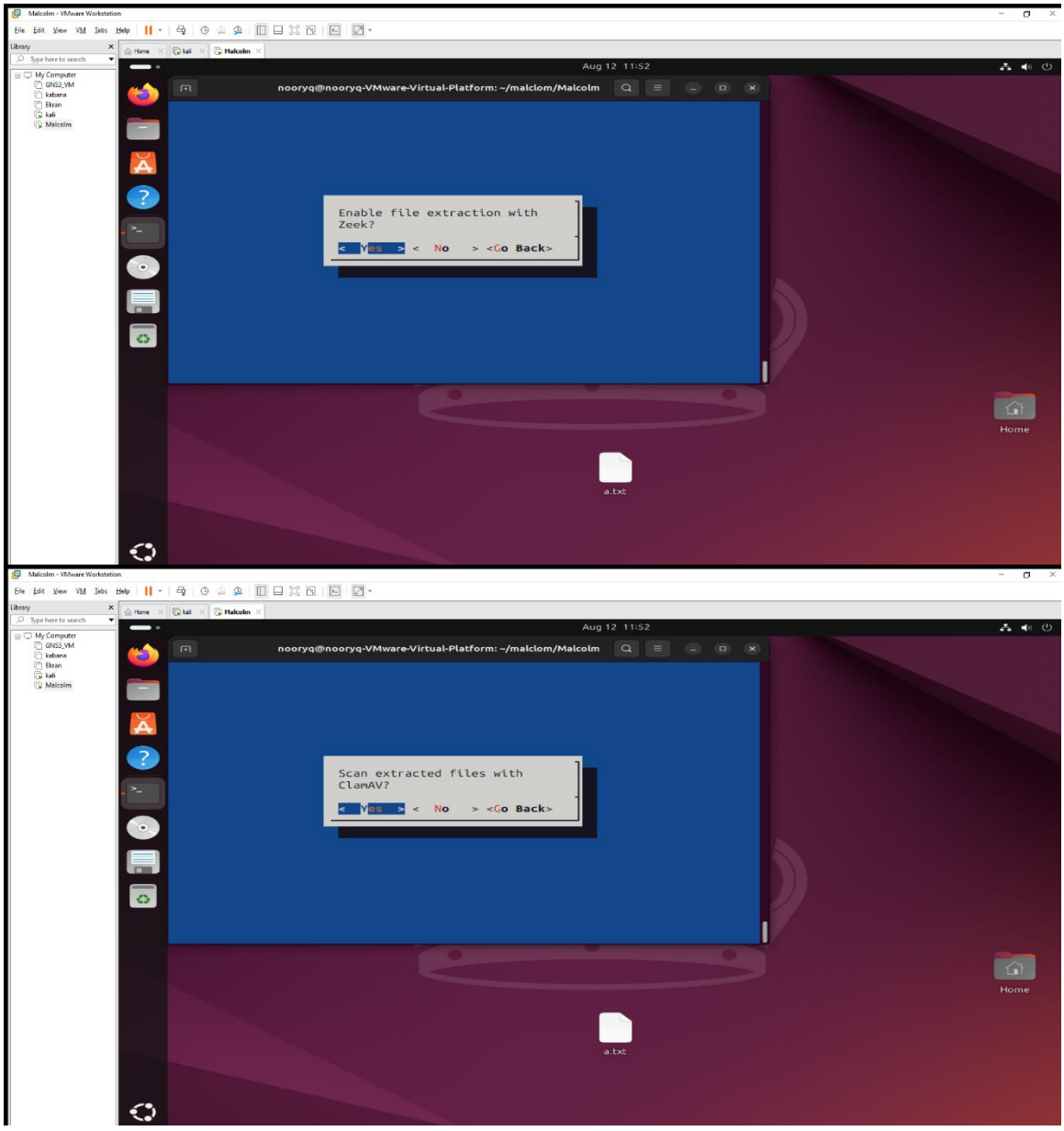

Malcolm - VMware Workstation
Aug 12 11:52
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Will Malcolm be running behind another reverse proxy (Traefik, Caddy, etc.)?
< No > < Yes > <Go Back>
Home
a.txt
Malcolm - VMware Workstation
Aug 12 11:52
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Store PCAP, log and index files in /home/nooryq/malclom/Malcolm?
< Yes > < No > <Go Back>
Home
a.txt

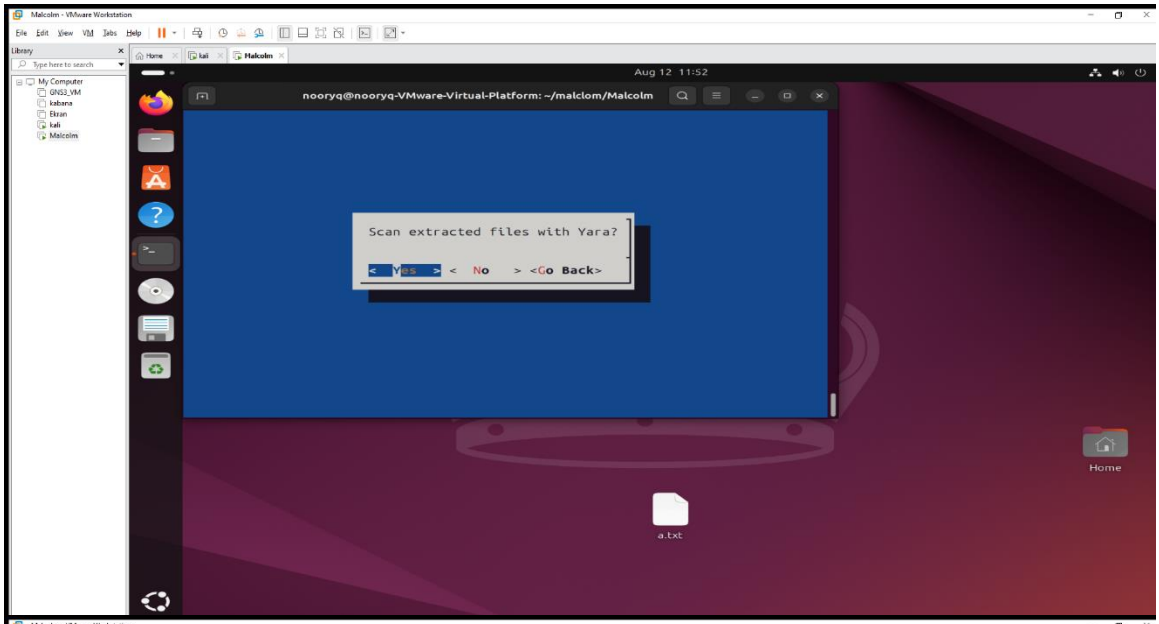

Malcolm - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS3_VM
kabana
Ekran
kali
Malcolm
Home
kali
Malcolm
Aug 12 11:52
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Enable index management
policies (ILM/ISM) in Arkime?
< No > < Yes > <Go Back>
Home
a.txt

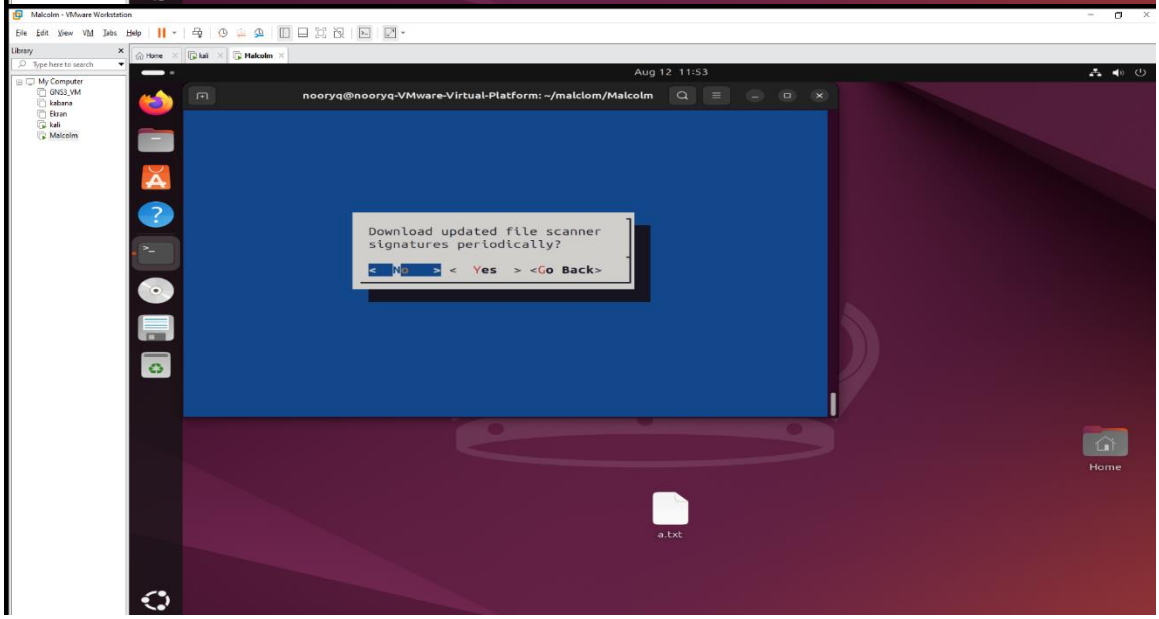
Malcolm - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS3_VM
kabana
Ekran
kali
Malcolm
Home
kali
Malcolm
Aug 12 11:52
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Automatically analyze all PCAP
files with Suricata?
< Yes > < No > <Go Back>
Home
a.txt

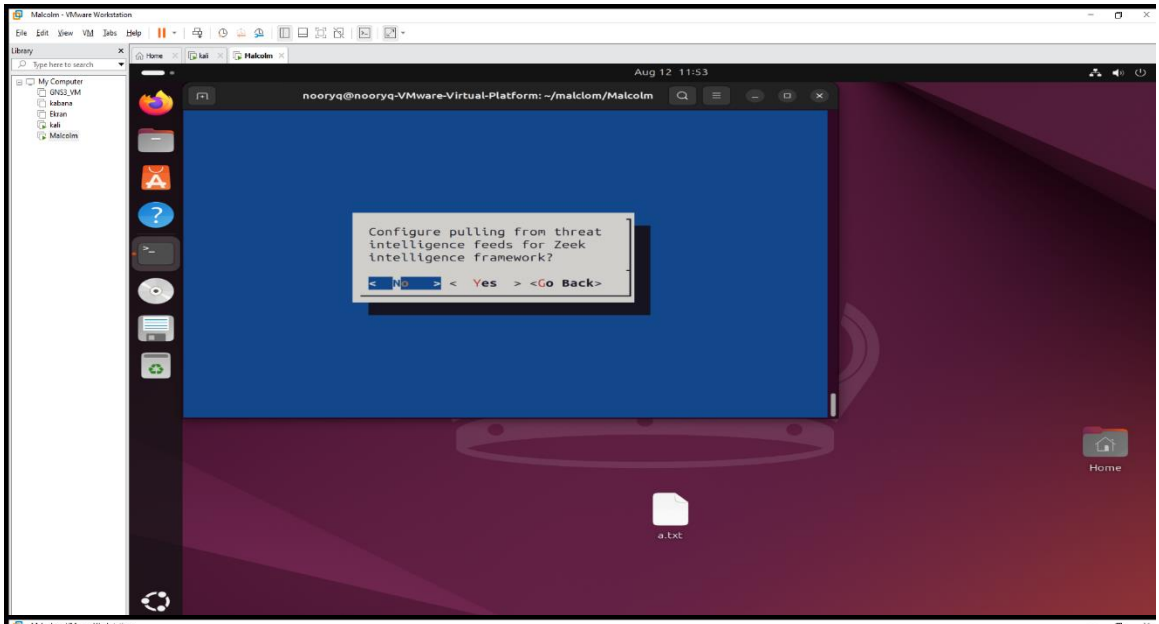

Malcolm - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS3_VM
kabana
Ekran
kali
Malcolm
Home
kali
Malcolm
Aug 12 11:52
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Perform hardware vendor OUI lookups for MAC addresses?
< Yes > < No > <Go Back>
Home
a.txt

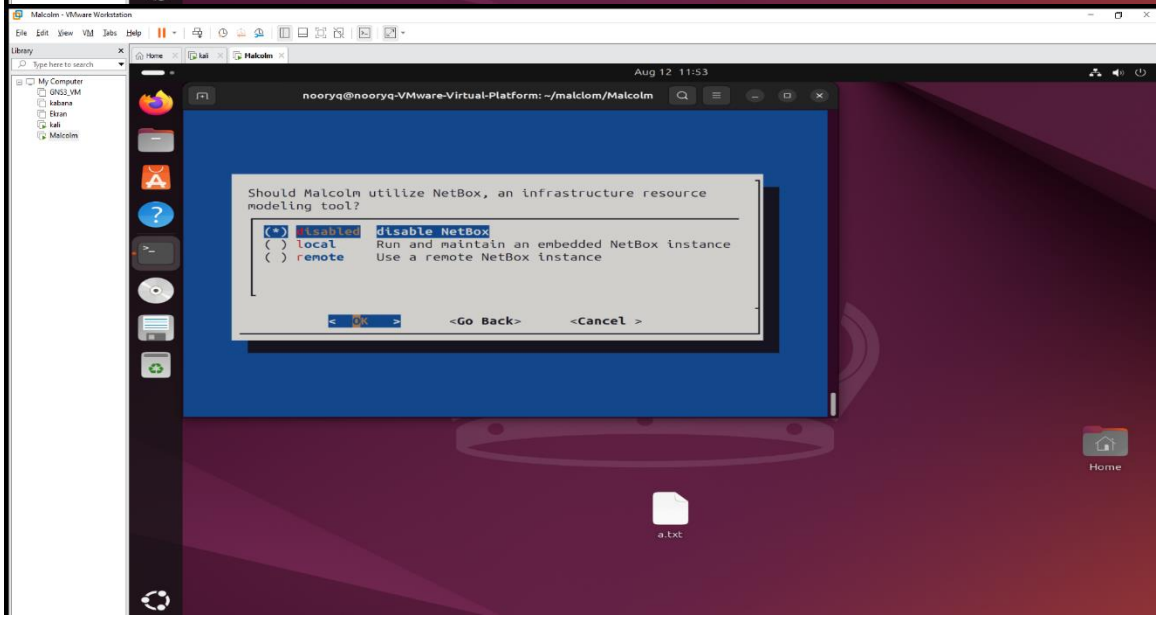
Malcolm - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS3_VM
kabana
Ekran
kali
Malcolm
Home
kali
Malcolm
Aug 12 11:52
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Perform string randomness scoring on some fields?
< Yes > < No > <Go Back>
Home
a.txt

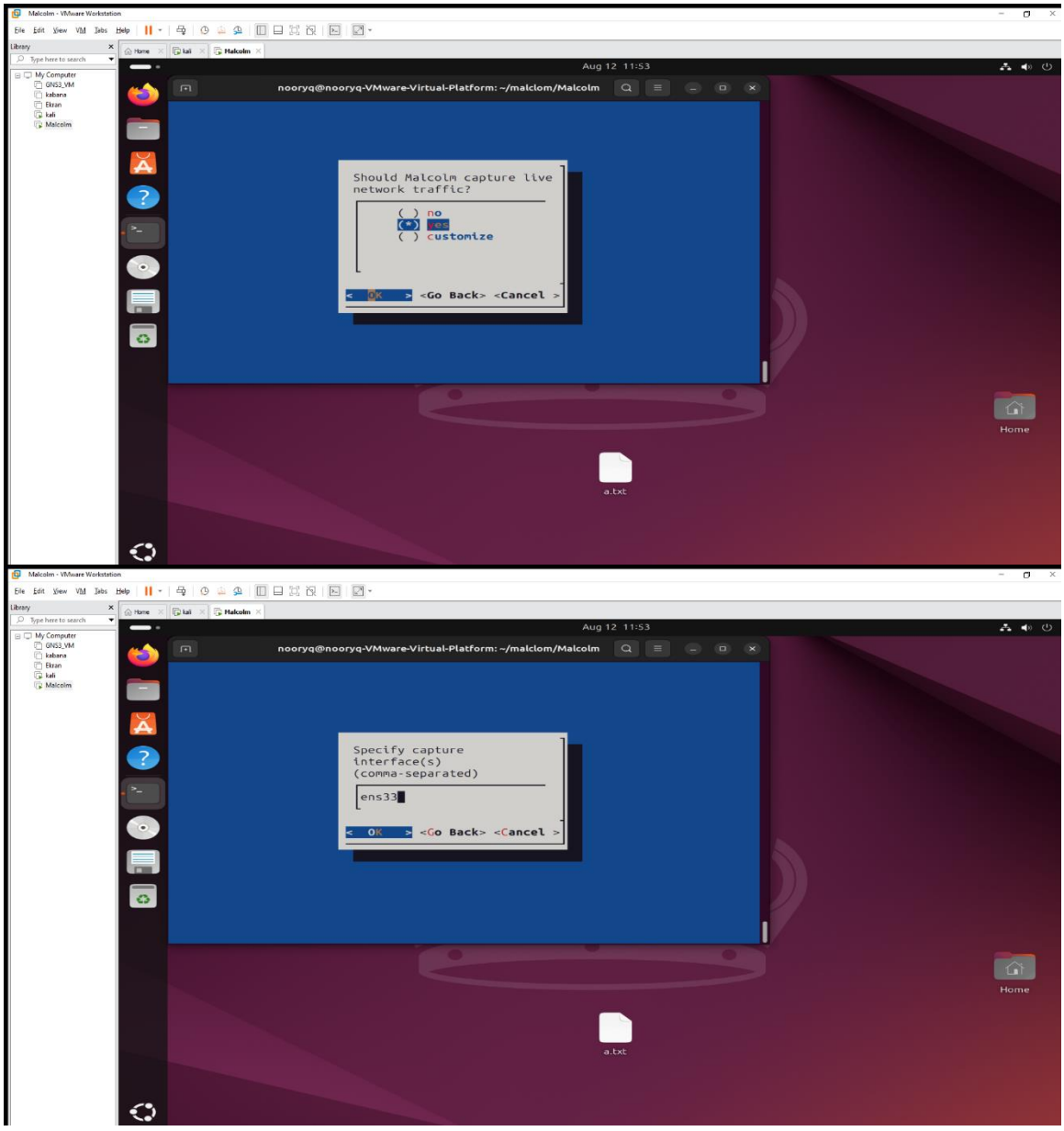

Malcolm - VMware Workstation
Aug 12 11:52
nooryq@nooryq-VMware-Virtual-Platform: ~/malcolm/Malcolm
Enable file extraction with Zeek?
< Yes > < No > <Go Back>
Home
a.txt
Malcolm - VMware Workstation
Aug 12 11:52
nooryq@nooryq-VMware-Virtual-Platform: ~/malcolm/Malcolm
Scan extracted files with ClamAV?
< Yes > < No > <Go Back>
Home
a.txt


Malcolm - VMware Workstation
Aug 12 11:52
nooryq@nooryq-VMware-Virtual-Platform: ~/malcolm/Malcolm
Scan extracted files with Yara?
< Yes > < No > <Go Back>
Home
a.txt


Malcolm - VMware Workstation
Aug 12 11:53
nooryq@nooryq-VMware-Virtual-Platform: ~/malcolm/Malcolm
Download updated file scanner signatures periodically?
< No > < Yes > <Go Back>
Home
a.txt

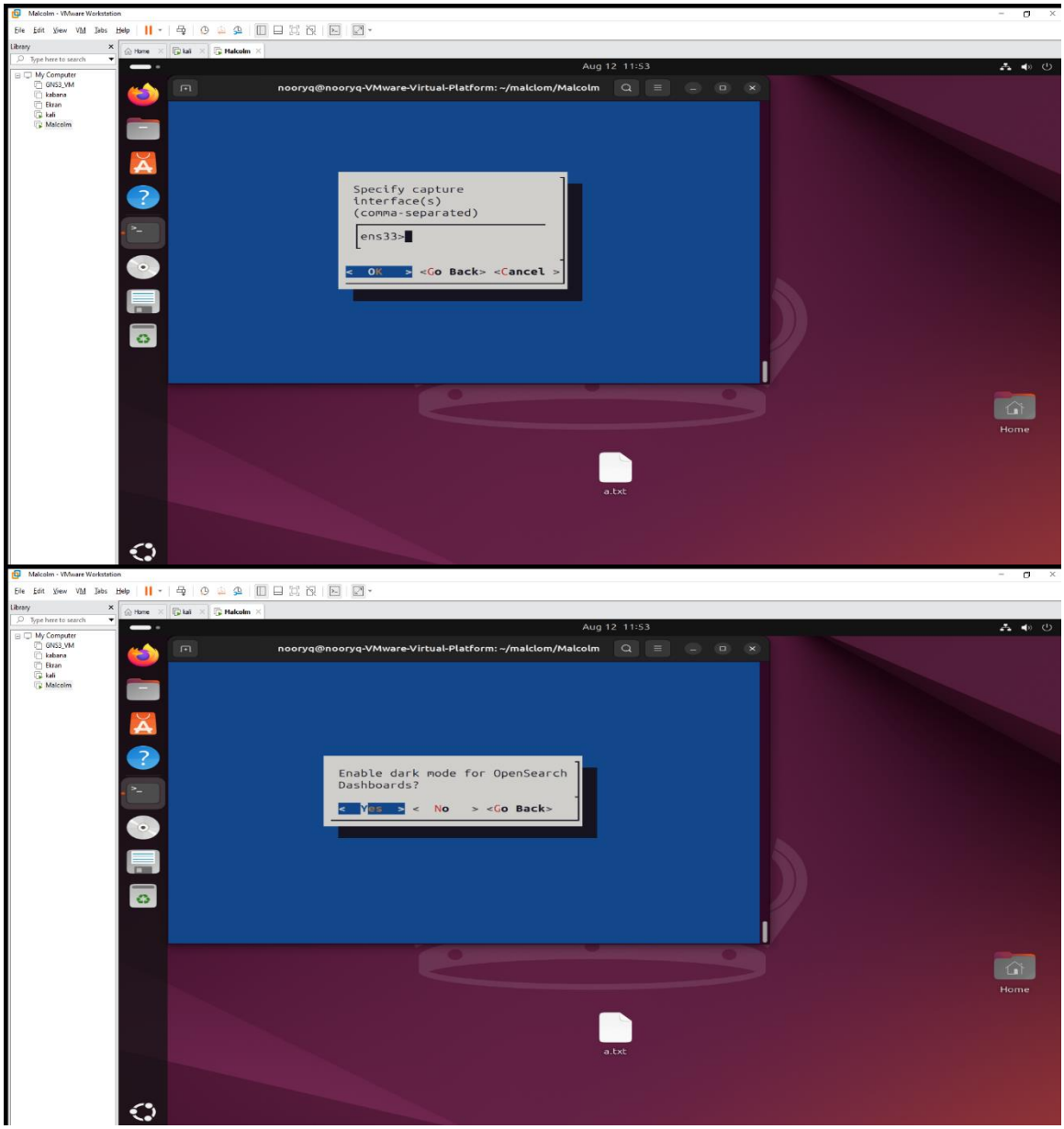

Malcolm - VMware Workstation
Aug 12 11:53
nooryq@nooryq-VMware-Virtual-Platform: ~/malcolm/Malcolm
Configure pulling from threat intelligence feeds for Zeek intelligence framework?
< No > < Yes > <Go Back>
Home
a.txt


Malcolm - VMware Workstation
Aug 12 11:53
nooryq@nooryq-VMware-Virtual-Platform: ~/malcolm/Malcolm
Should Malcolm utilize NetBox, an infrastructure resource modeling tool?
(*) disabled disable NetBox
( ) local Run and maintain an embedded NetBox instance
( ) remote Use a remote NetBox instance
< Ok > <Go Back> <Cancel >
Home
a.txt

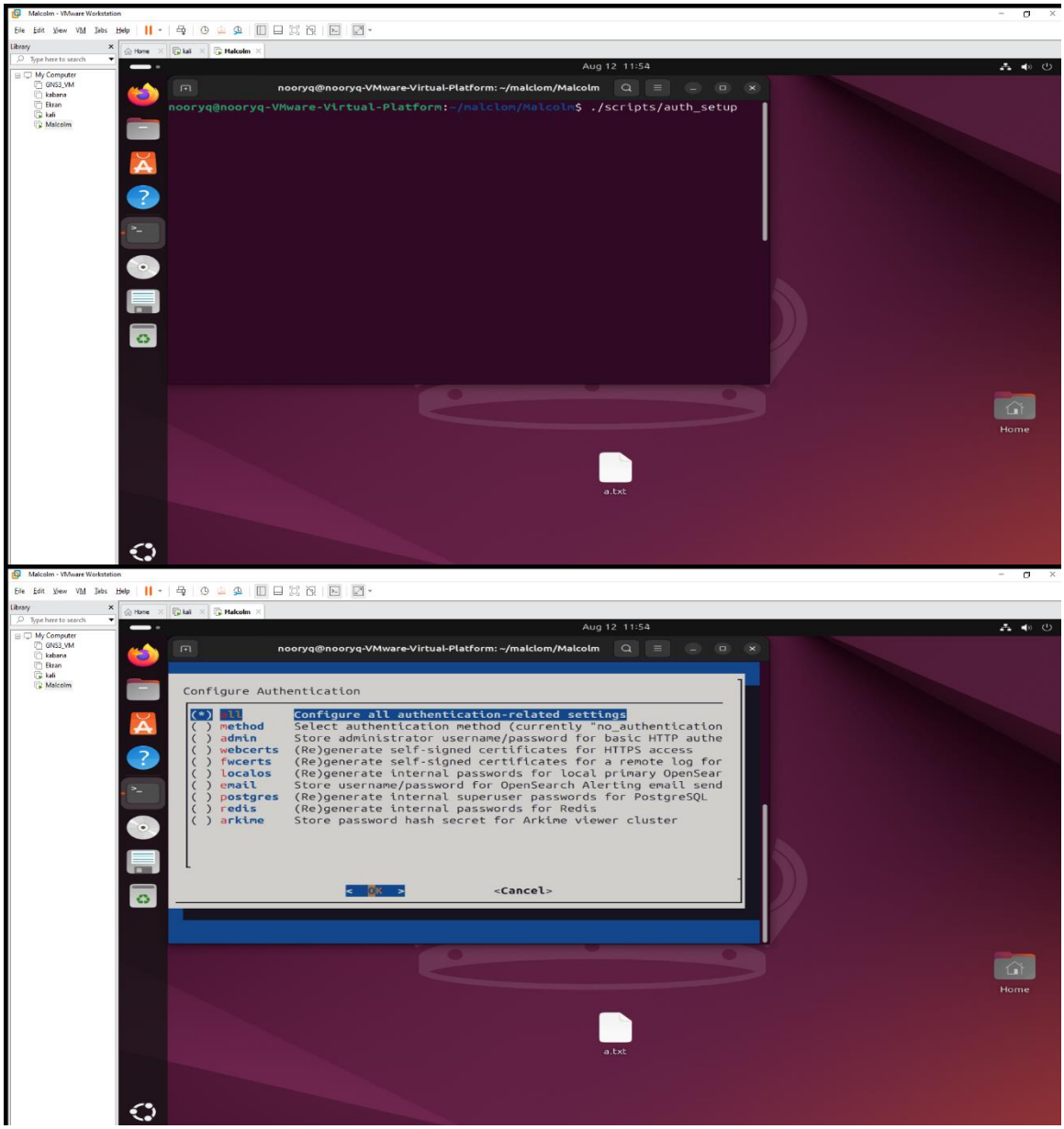

Malcolm - VMware Workstation
Aug 12 11:53
nooryq@nooryq-VMware-Virtual-Platform: ~/malcolm/Malcolm
Should Malcolm capture live network traffic?
( ) no
(*) yes
( ) customize
< OK > <Go Back> <Cancel >
Home
a.txt

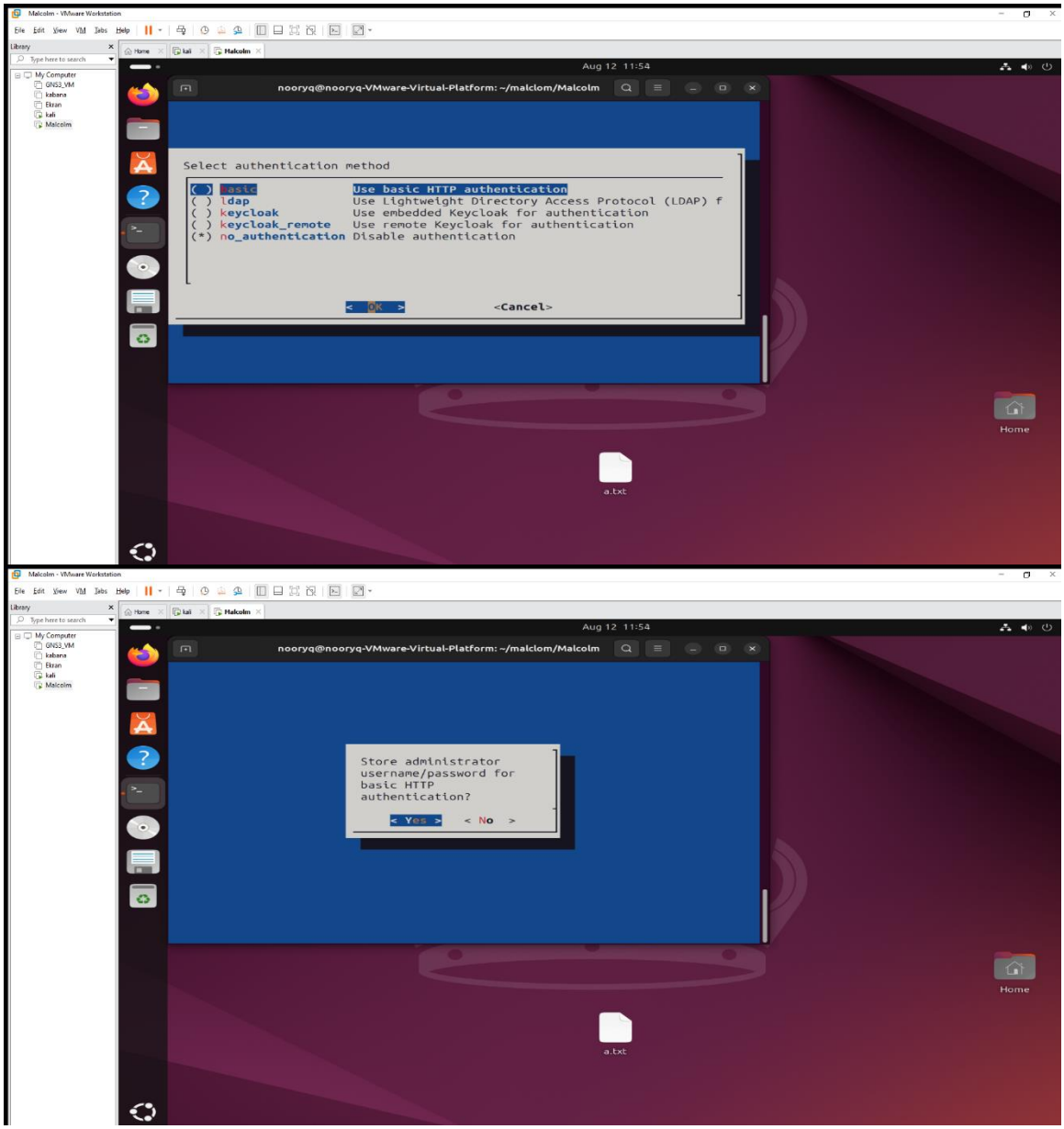
Malcolm - VMware Workstation
Aug 12 11:53
nooryq@nooryq-VMware-Virtual-Platform: ~/malcolm/Malcolm
Specify capture interface(s) (comma-separated)
ens33
< OK > <Go Back> <Cancel >
Home
a.txt

by follow all this step as it show

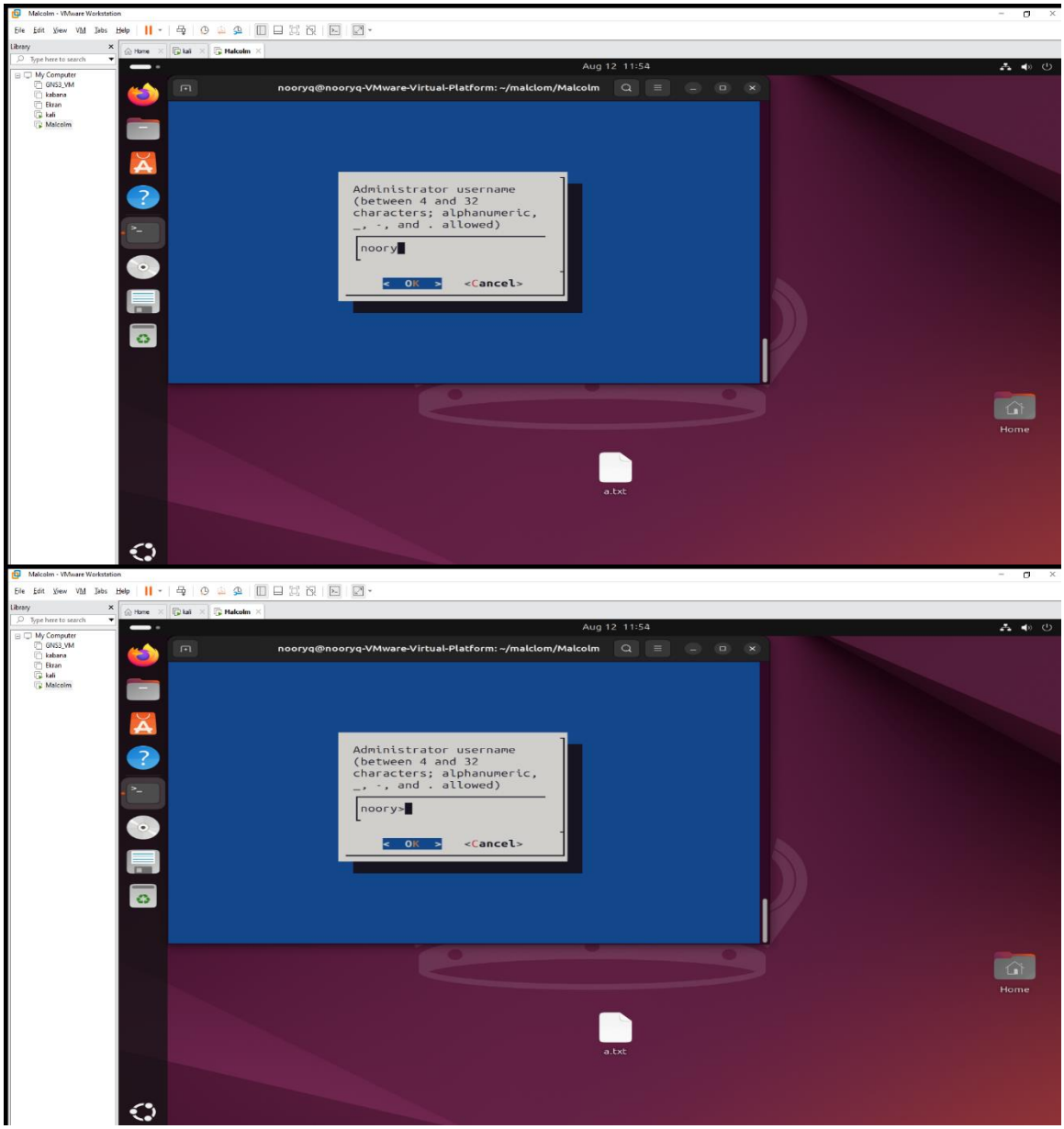


after install services then config auth_setup by follow all this steps

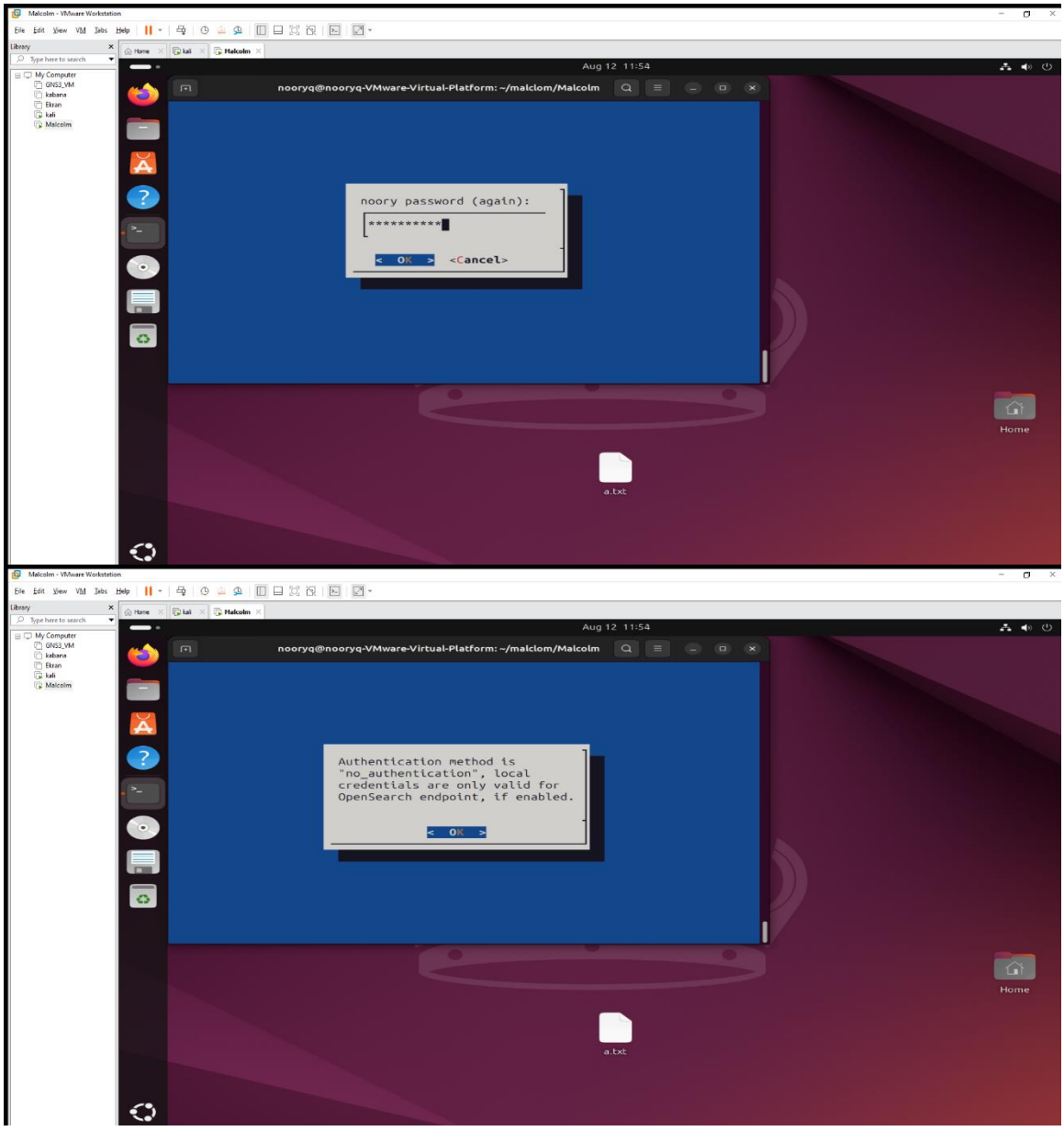



Malcolm - VMware Workstation
Aug 12 11:54
nooryq@nooryq-VMware-Virtual-Platform: ~/malcIom/Malcolm
Select authentication method
(*) basic Use basic HTTP authentication
( ) ldap Use Lightweight Directory Access Protocol (LDAP) f
( ) keycloak Use embedded Keycloak for authentication
( ) keycloak_remote Use remote Keycloak for authentication
(*) no_authentication Disable authentication
< OK >
<Cancel>
Home
a.txt

Malcolm - VMware Workstation
Aug 12 11:54
nooryq@nooryq-VMware-Virtual-Platform: ~/malcIom/Malcolm
Store administrator username/password for basic HTTP authentication?
< Yes >
< No >
Home
a.txt

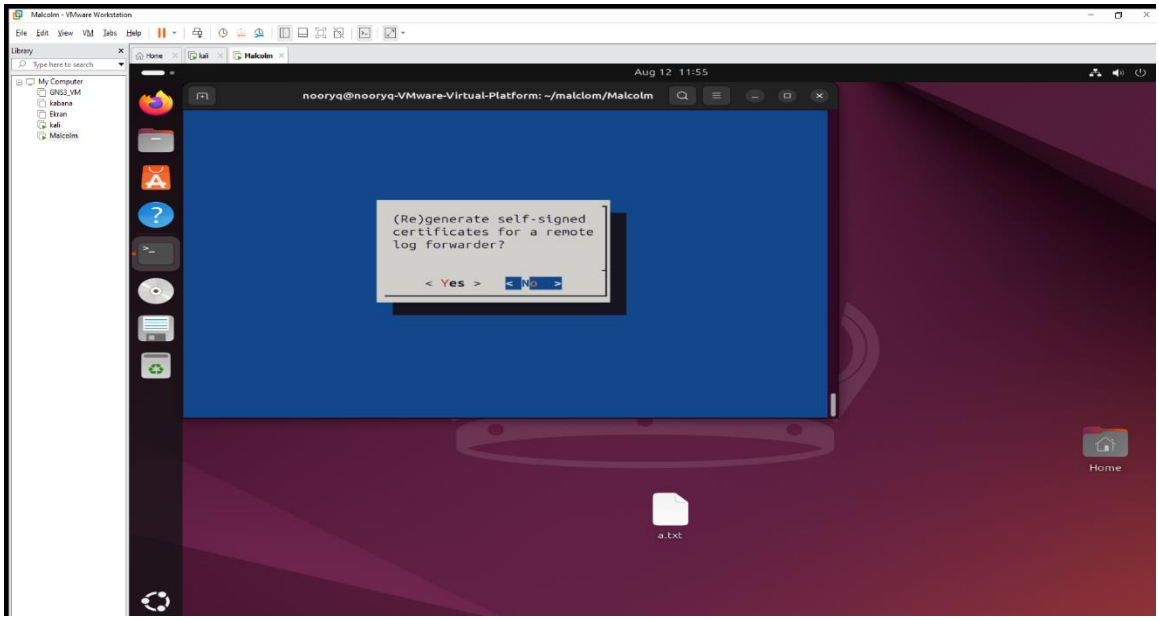

Malcolm - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS3_VM
kabana
Ekran
kali
Malcolm
Home
kali
Malcolm
Aug 12 11:54
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Administrator username
(between 4 and 32
characters; alphanumeric,
_, -, and . allowed)
noory
< OK >
<Cancel>
Home
a.txt

Malcolm - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS3_VM
kabana
Ekran
kali
Malcolm
Home
kali
Malcolm
Aug 12 11:54
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Administrator username
(between 4 and 32
characters; alphanumeric,
_, -, and . allowed)
noory>
< OK >
<Cancel>
Home
a.txt

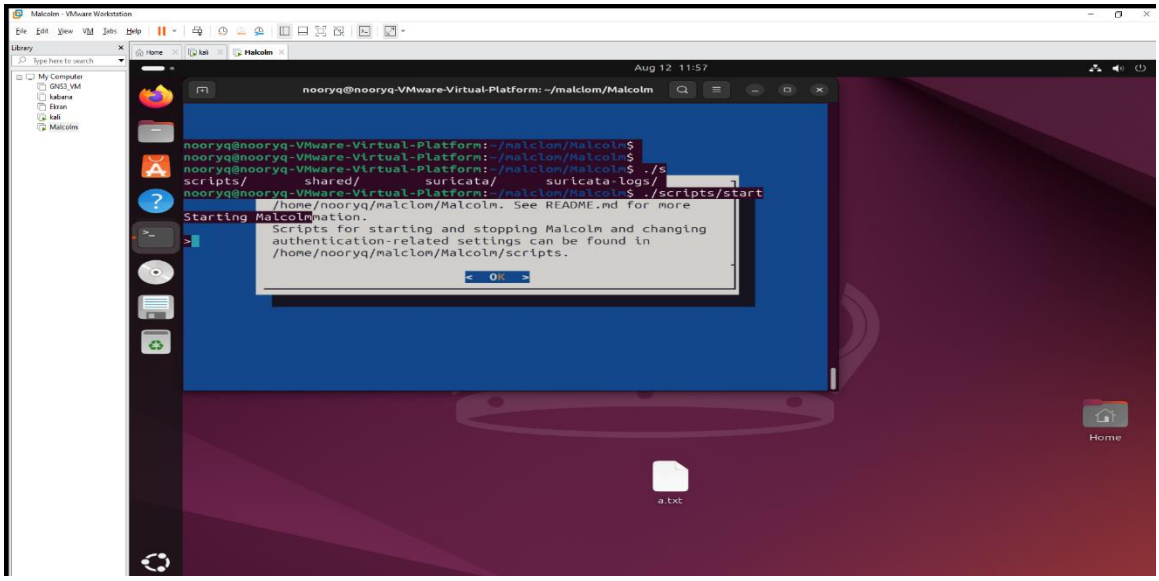

Malcolm - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS3_VM
kabana
Ekran
kali
Malcolm
Home
kali
Malcolm
Aug 12 11:54
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
noory password (again):
****
< OK >
<Cancel>
Home
a.txt

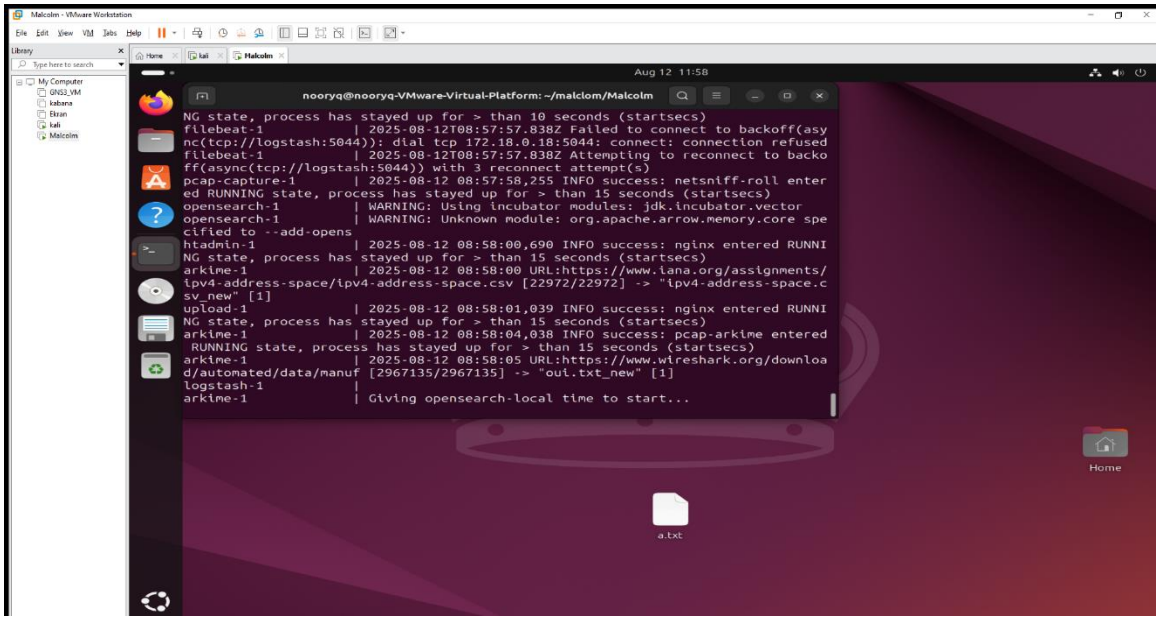
Malcolm - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS3_VM
kabana
Ekran
kali
Malcolm
Home
kali
Malcolm
Aug 12 11:54
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
Authentication method is
"no_authentication", local
credentials are only valid for
OpenSearch endpoint, if enabled.
< OK >
Home
a.txt

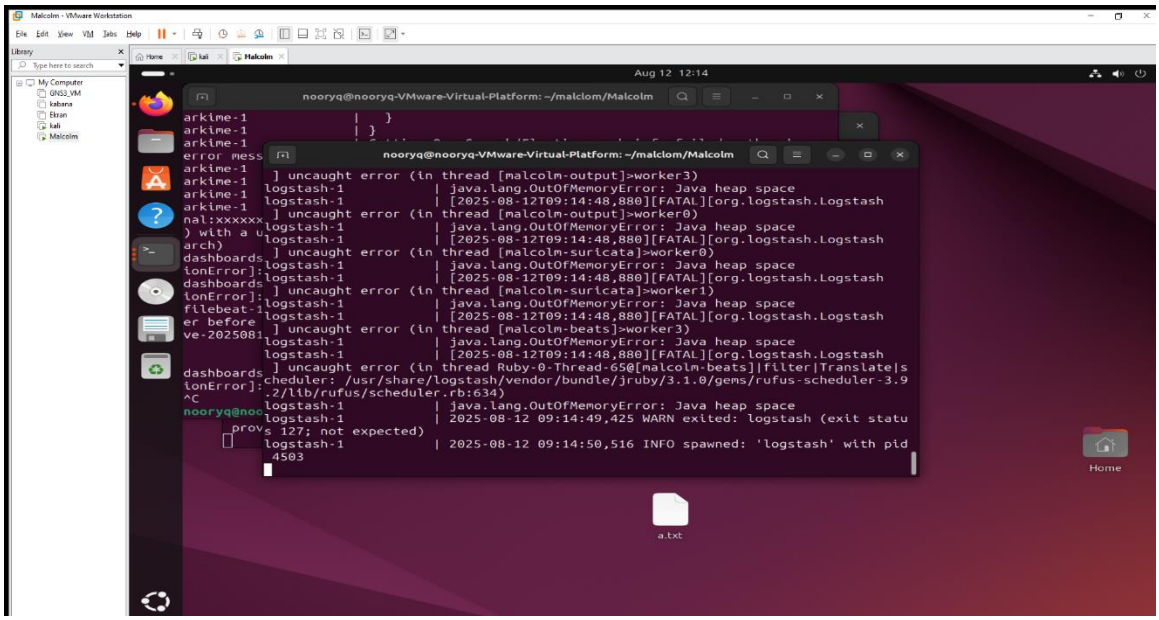
th

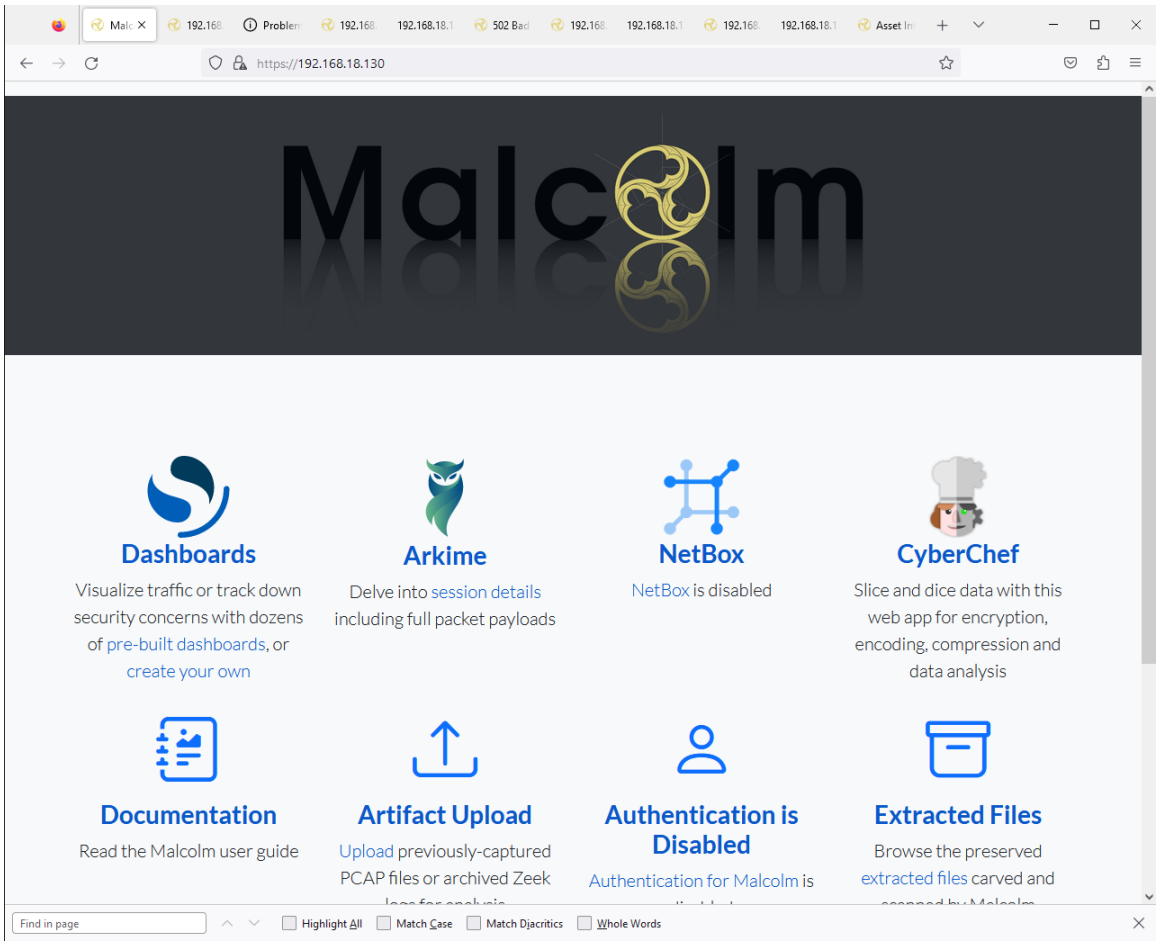


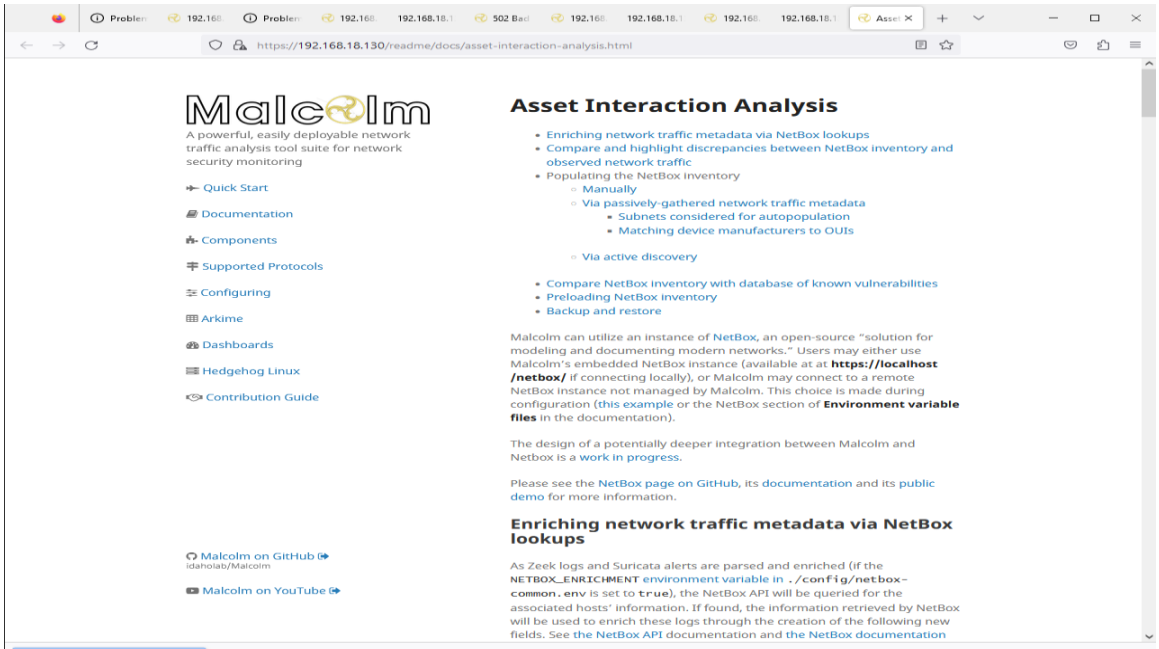
then we will start Malcolm by typing ./script start

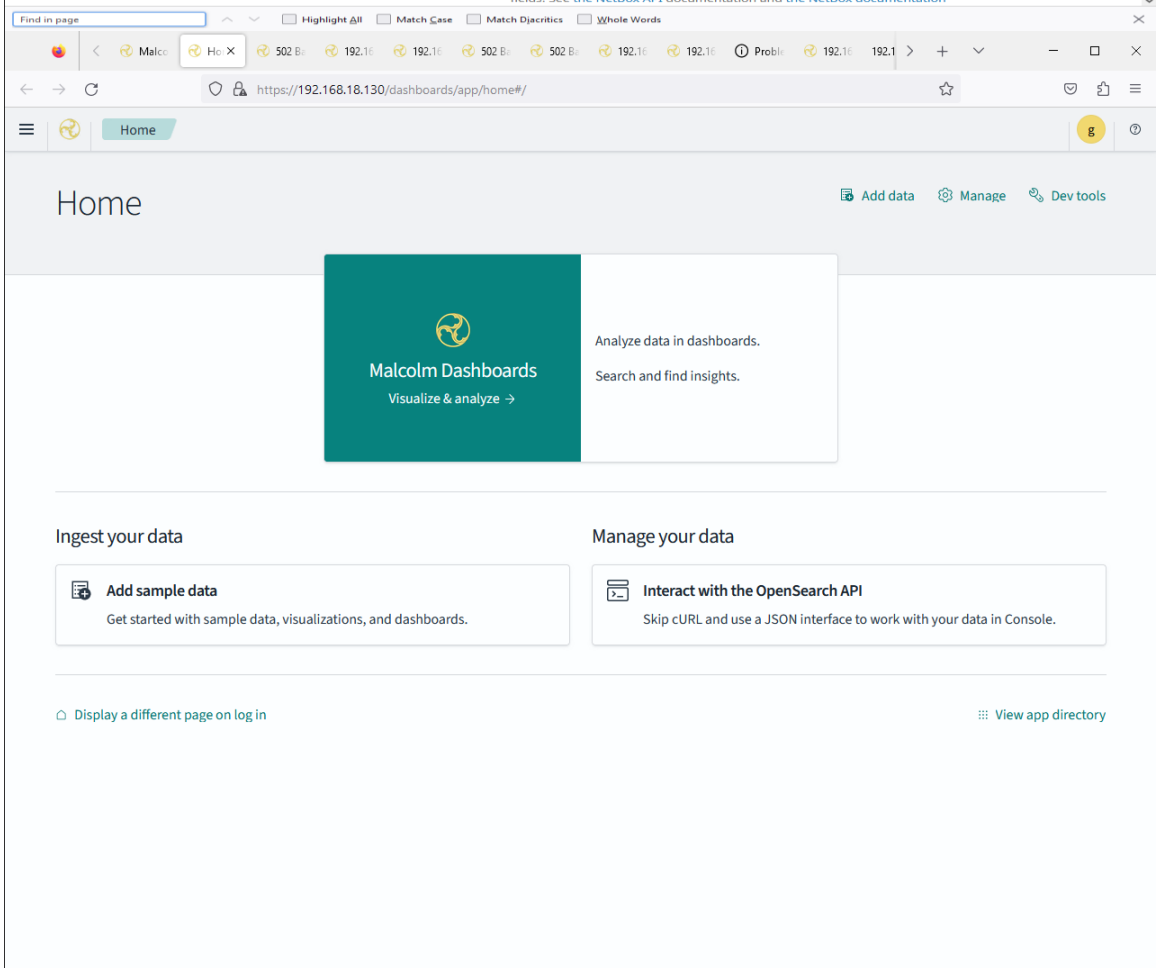


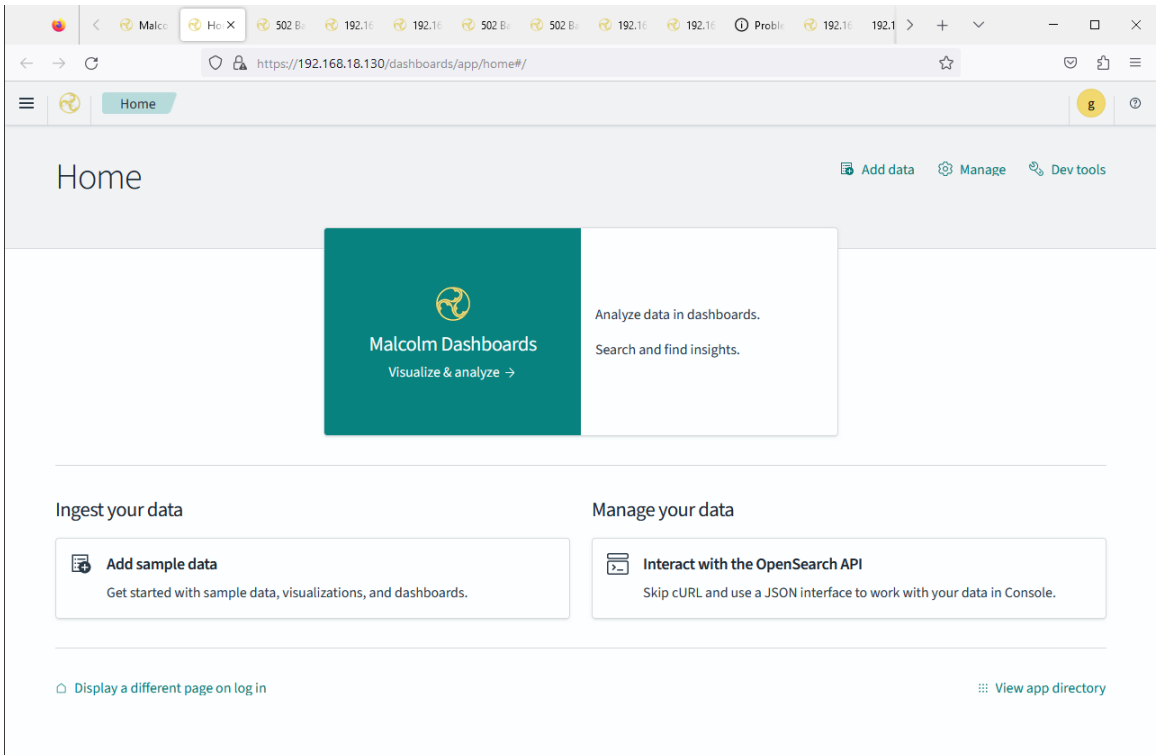

Malcolm - VMware Workstation
Aug 12 11:58
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
NG state, process has stayed up for > than 10 seconds (startsecs)
filebeat-1 | 2025-08-12T08:57:57.838Z Failed to connect to backoff(asy
nc(tcp://logstash:5044)): dial tcp 172.18.0.18:5044: connect: connection refused
filebeat-1 | 2025-08-12T08:57:57.838Z Attempting to reconnect to backo
ff(async(tcp://logstash:5044)) with 3 reconnect attempt(s)
pcap-capture-1 | 2025-08-12 08:57:58,255 INFO success: netsniff-roll enter
ed RUNNING state, process has stayed up for > than 15 seconds (startsecs)
opensearch-1 | WARNING: Using incubator modules: jdk.incubator.vector
opensearch-1 | WARNING: Unknown module: org.apache.arrow.memory.core spe
cified to --add-opens
htadmin-1 | 2025-08-12 08:58:00,690 INFO success: nginx entered RUNNI
NG state, process has stayed up for > than 15 seconds (startsecs)
arkime-1 | 2025-08-12 08:58:00 URL:https://www.iana.org/assignments/
ipv4-address-space/ipv4-address-space.csv [22972/22972] -> "ipv4-address-space.c
sv_new" [1]
upload-1 | 2025-08-12 08:58:01,039 INFO success: nginx entered RUNNI
NG state, process has stayed up for > than 15 seconds (startsecs)
arkime-1 | 2025-08-12 08:58:04,038 INFO success: pcap-arkime entered
RUNNING state, process has stayed up for > than 15 seconds (startsecs)
arkime-1 | 2025-08-12 08:58:05 URL:https://www.wireshark.org/downloa
d/automated/data/manuf [2967135/2967135] -> "oui.txt_new" [1]
logstash-1 |
arkime-1 | Giving opensearch-local time to start...
Home
a.txt

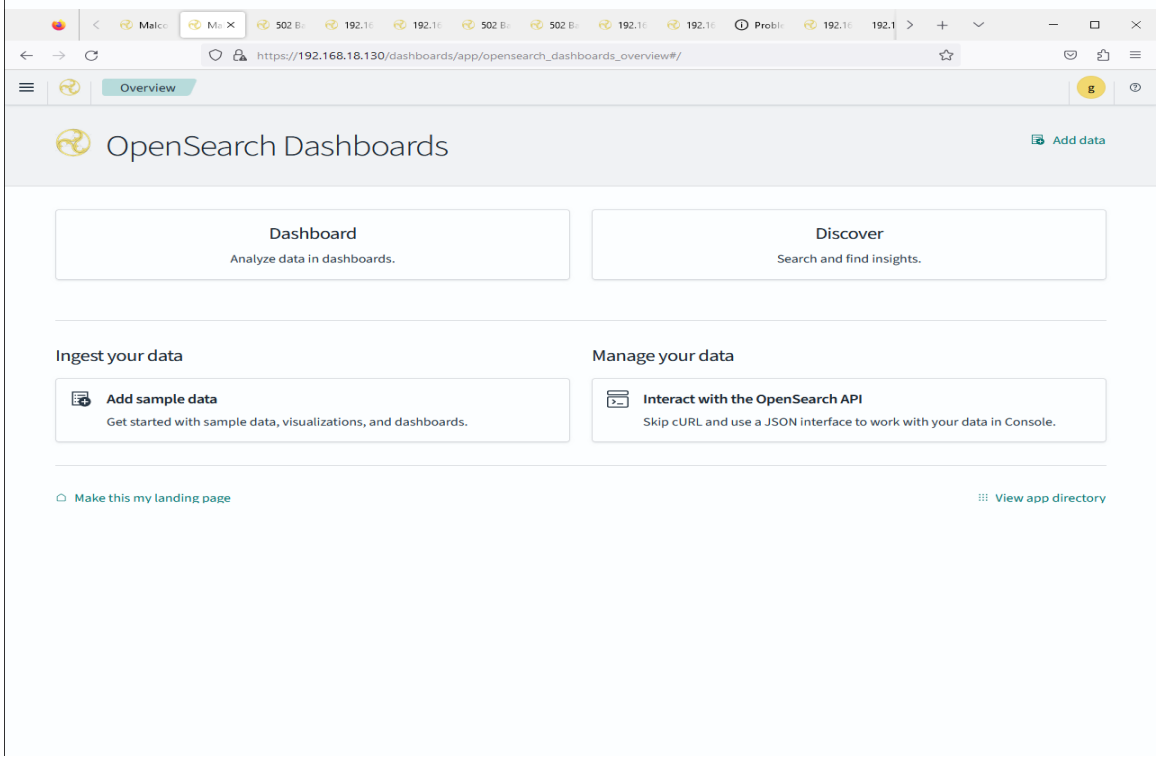

Malcolm - VMware Workstation
Aug 12 12:14
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
arkime-1 | }
arkime-1 | }
nooryq@nooryq-VMware-Virtual-Platform: ~/malclom/Malcolm
] uncaught error (in thread [malcolm-output]>worker3)
logstash-1 | java.lang.OutOfMemoryError: Java heap space
logstash-1 | [2025-08-12T09:14:48,880][FATAL][org.logstash.Logstash
] uncaught error (in thread [malcolm-output]>worker0)
logstash-1 | java.lang.OutOfMemoryError: Java heap space
logstash-1 | [2025-08-12T09:14:48,880][FATAL][org.logstash.Logstash
] uncaught error (in thread [malcolm-suricata]>worker0)
logstash-1 | java.lang.OutOfMemoryError: Java heap space
logstash-1 | [2025-08-12T09:14:48,880][FATAL][org.logstash.Logstash
] uncaught error (in thread [malcolm-suricata]>worker1)
logstash-1 | java.lang.OutOfMemoryError: Java heap space
logstash-1 | [2025-08-12T09:14:48,880][FATAL][org.logstash.Logstash
] uncaught error (in thread [malcolm-beats]>worker3)
logstash-1 | java.lang.OutOfMemoryError: Java heap space
logstash-1 | [2025-08-12T09:14:48,880][FATAL][org.logstash.Logstash
] uncaught error (in thread Ruby-0-Thread-65@[malcolm-beats]|filter|Translate|s
cheduler: /usr/share/logstash/vendor/bundle/jruby/3.1.0/gems/rufus-scheduler-3.9
.2/lib/rufus/scheduler.rb:634)
logstash-1 | java.lang.OutOfMemoryError: Java heap space
logstash-1 | 2025-08-12 09:14:49,425 WARN exited: logstash (exit statu
s 127; not expected)
logstash-1 | 2025-08-12 09:14:50,516 INFO spawned: 'logstash' with pid
4503
Home
a.txt

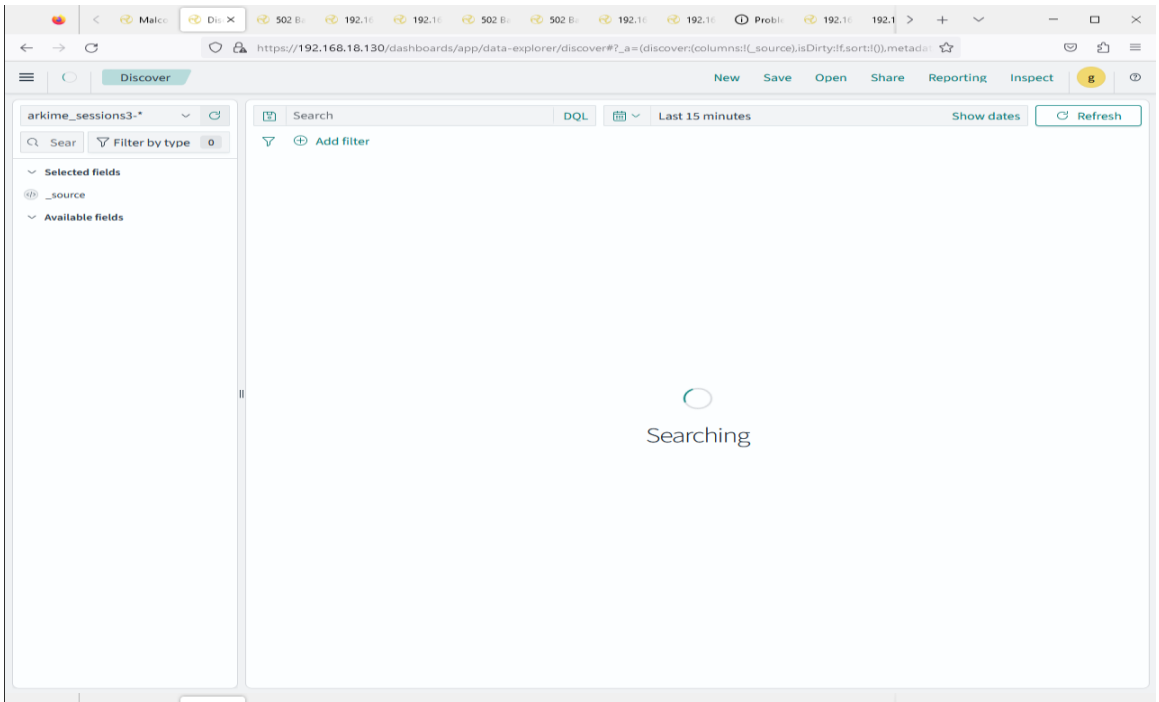

https://192.168.18.130
Malcolm
Dashboards
Visualize traffic or track down security concerns with dozens of pre-built dashboards, or create your own
Arkime
Delve into session details including full packet payloads
NetBox
NetBox is disabled
CyberChef
Slice and dice data with this web app for encryption, encoding, compression and data analysis
Documentation
Read the Malcolm user guide
Artifact Upload
Upload previously-captured PCAP files or archived Zeek
Authentication is Disabled
Authentication for Malcolm is
Extracted Files
Browse the preserved extracted files carved and
Find in page
Highlight All
Match Case
Match Diacritics
Whole Words

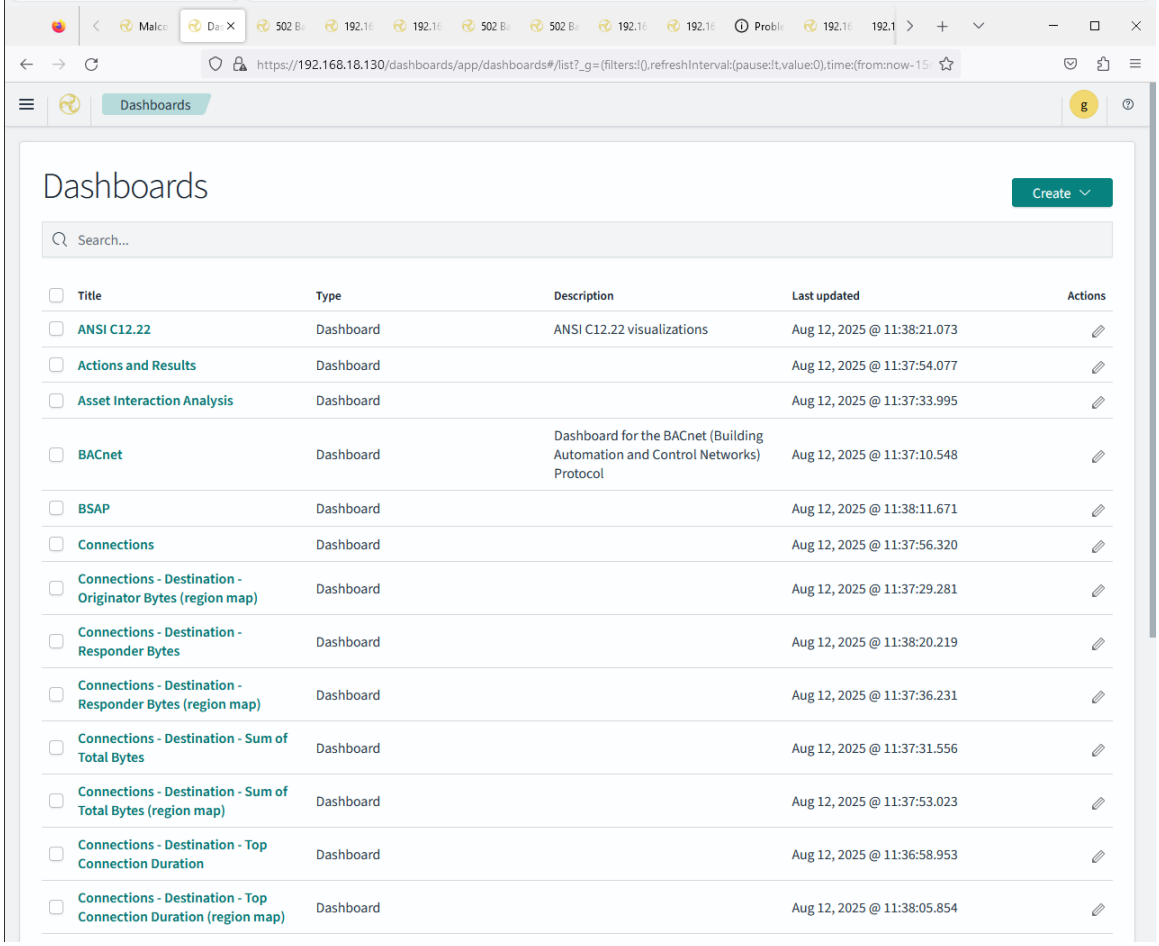

https://192.168.18.130/readme/docs/asset-interaction-analysis.html
Malcolm
A powerful, easily deployable network traffic analysis tool suite for network security monitoring
Quick Start
Documentation
Components
Supported Protocols
Configuring
Arkime
Dashboards
Hedgehog Linux
Contribution Guide
Malcolm on GitHub
idaholab/Malcolm
Malcolm on YouTube
Asset Interaction Analysis
Enriching network traffic metadata via NetBox lookups
Compare and highlight discrepancies between NetBox inventory and observed network traffic
Populating the NetBox inventory
Manually
Via passively-gathered network traffic metadata
Subnets considered for autopopulation
Matching device manufacturers to OUIs
Via active discovery
Compare NetBox inventory with database of known vulnerabilities
Preloading NetBox inventory
Backup and restore
Malcolm can utilize an instance of NetBox, an open-source "solution for modeling and documenting modern networks." Users may either use Malcolm's embedded NetBox instance (available at at https://localhost/netbox/ if connecting locally), or Malcolm may connect to a remote NetBox instance not managed by Malcolm. This choice is made during configuration (this example or the NetBox section of Environment variable files in the documentation).
The design of a potentially deeper integration between Malcolm and Netbox is a work in progress.
Please see the NetBox page on GitHub, its documentation and its public demo for more information.
Enriching network traffic metadata via NetBox lookups
As Zeek logs and Suricata alerts are parsed and enriched (if the NETBOX_ENRICHMENT environment variable in ./config/netbox-common.env is set to true), the NetBox API will be queried for the associated hosts' information. If found, the information retrieved by NetBox will be used to enrich these logs through the creation of the following new fields. See the NetBox API documentation and the NetBox documentation


https://192.168.18.130/dashboards/app/home#/
Home
Home
Add data
Manage
Dev tools
Malcolm Dashboards
Visualize & analyze
Analyze data in dashboards.
Search and find insights.
Ingest your data
Add sample data
Get started with sample data, visualizations, and dashboards.
Manage your data
Interact with the OpenSearch API
Skip cURL and use a JSON interface to work with your data in Console.
Display a different page on log in
View app directory


https://192.168.18.130/dashboards/app/home#/
Home
Home
Add data
Manage
Dev tools
Malcolm Dashboards
Visualize & analyze →
Analyze data in dashboards.
Search and find insights.
Ingest your data
Add sample data
Get started with sample data, visualizations, and dashboards.
Manage your data
Interact with the OpenSearch API
Skip cURL and use a JSON interface to work with your data in Console.
Display a different page on log in
View app directory


https://192.168.18.130/dashboards/app/opensearch_dashboards_overview#/
Overview
OpenSearch Dashboards
Add data
Dashboard
Analyze data in dashboards.
Discover
Search and find insights.
Ingest your data
Add sample data
Get started with sample data, visualizations, and dashboards.
Manage your data
Interact with the OpenSearch API
Skip cURL and use a JSON interface to work with your data in Console.
Make this my landing page
View app directory



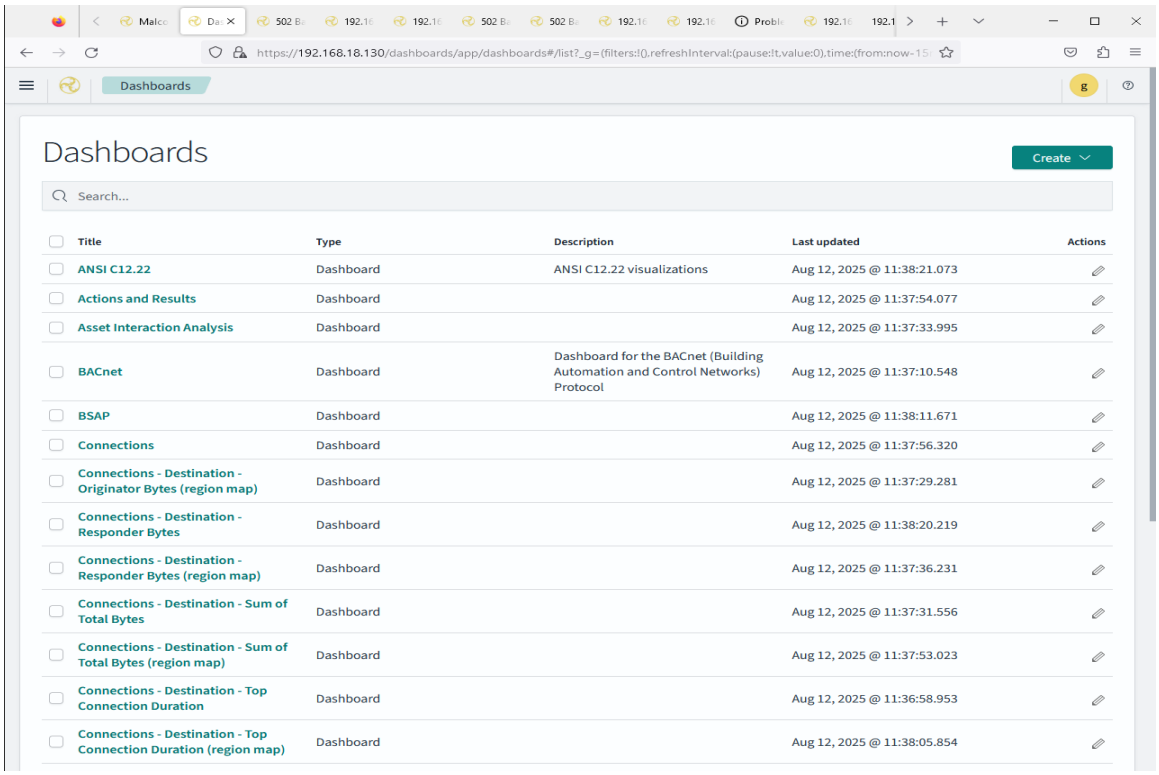


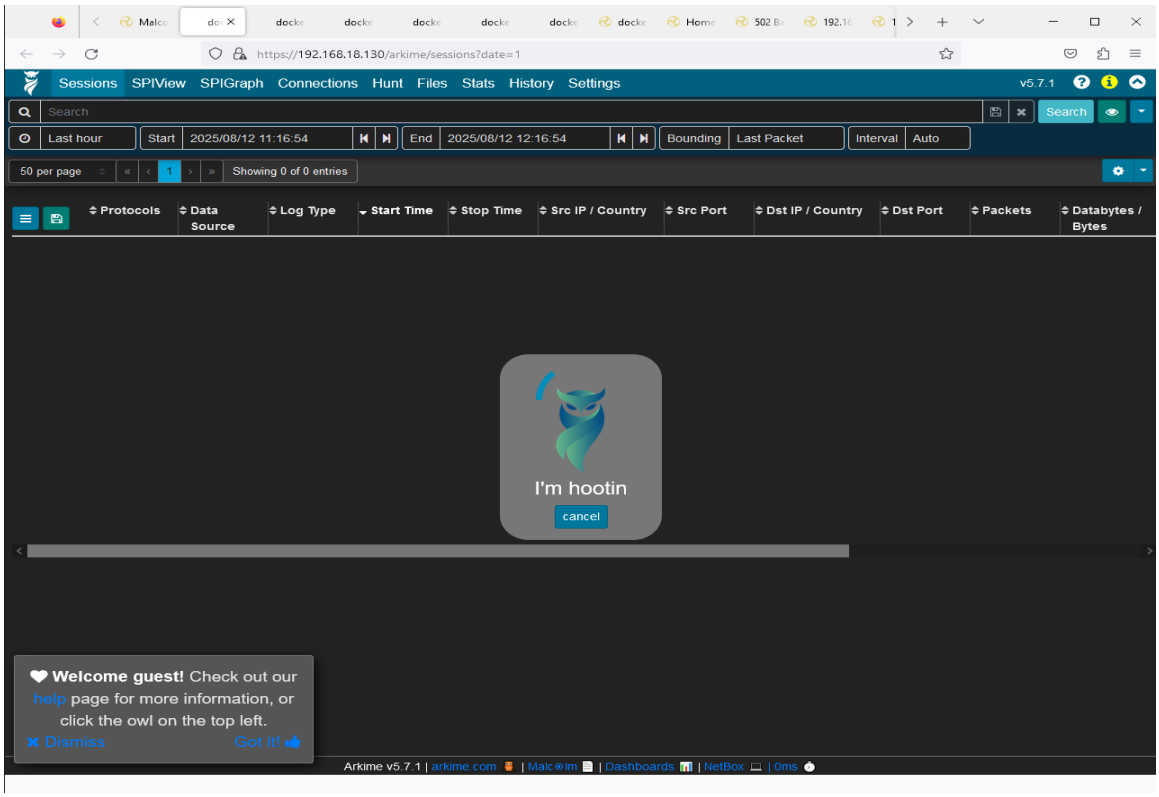
Dashboards

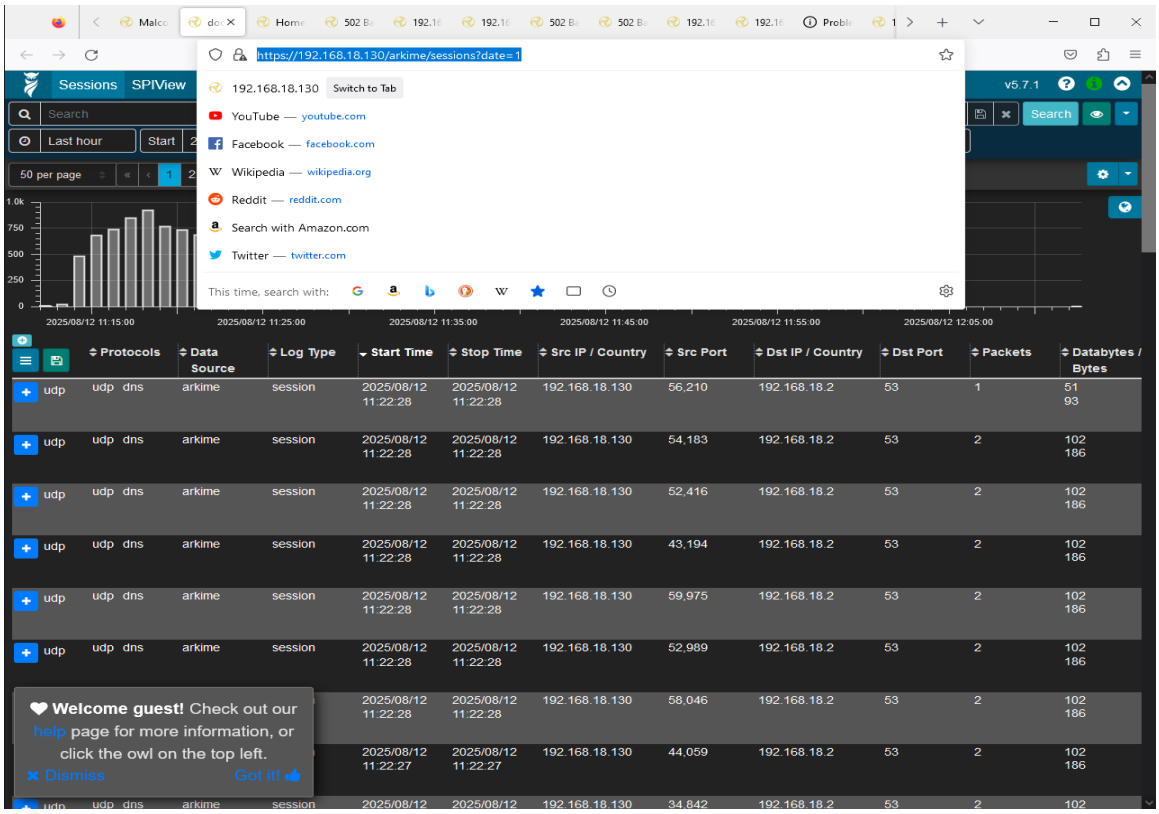
Create

Search...

Title	Type	Description	Last updated	Actions
ANSI C12.22	Dashboard	ANSI C12.22 visualizations	Aug 12, 2025 @ 11:38:21.073	
Actions and Results	Dashboard		Aug 12, 2025 @ 11:37:54.077	
Asset Interaction Analysis	Dashboard		Aug 12, 2025 @ 11:37:33.995	
BACnet	Dashboard	Dashboard for the BACnet (Building Automation and Control Networks) Protocol	Aug 12, 2025 @ 11:37:10.548	
BSAP	Dashboard		Aug 12, 2025 @ 11:38:11.671	
Connections	Dashboard		Aug 12, 2025 @ 11:37:56.320	
Connections - Destination - Originator Bytes (region map)	Dashboard		Aug 12, 2025 @ 11:37:29.281	
Connections - Destination - Responder Bytes	Dashboard		Aug 12, 2025 @ 11:38:20.219	
Connections - Destination - Responder Bytes (region map)	Dashboard		Aug 12, 2025 @ 11:37:36.231	
Connections - Destination - Sum of Total Bytes	Dashboard		Aug 12, 2025 @ 11:37:31.556	
Connections - Destination - Sum of Total Bytes (region map)	Dashboard		Aug 12, 2025 @ 11:37:53.023	
Connections - Destination - Top Connection Duration	Dashboard		Aug 12, 2025 @ 11:36:58.953	
Connections - Destination - Top Connection Duration (region map)	Dashboard		Aug 12, 2025 @ 11:38:05.854	


https://192.168.18.130/dashboards/app/dashboards#/list?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15
Dashboards
Dashboards
Create
Search...
Title
Type
Description
Last updated
Actions
ANSI C12.22
Dashboard
ANSI C12.22 visualizations
Aug 12, 2025 @ 11:38:21.073
Actions and Results
Dashboard
Aug 12, 2025 @ 11:37:54.077
Asset Interaction Analysis
Dashboard
Aug 12, 2025 @ 11:37:33.995
BACnet
Dashboard
Dashboard for the BACnet (Building Automation and Control Networks) Protocol
Aug 12, 2025 @ 11:37:10.548
BSAP
Dashboard
Aug 12, 2025 @ 11:38:11.671
Connections
Dashboard
Aug 12, 2025 @ 11:37:56.320
Connections - Destination - Originator Bytes (region map)
Dashboard
Aug 12, 2025 @ 11:37:29.281
Connections - Destination - Responder Bytes
Dashboard
Aug 12, 2025 @ 11:38:20.219
Connections - Destination - Responder Bytes (region map)
Dashboard
Aug 12, 2025 @ 11:37:36.231
Connections - Destination - Sum of Total Bytes
Dashboard
Aug 12, 2025 @ 11:37:31.556
Connections - Destination - Sum of Total Bytes (region map)
Dashboard
Aug 12, 2025 @ 11:37:53.023
Connections - Destination - Top Connection Duration
Dashboard
Aug 12, 2025 @ 11:36:58.953
Connections - Destination - Top Connection Duration (region map)
Dashboard
Aug 12, 2025 @ 11:38:05.854

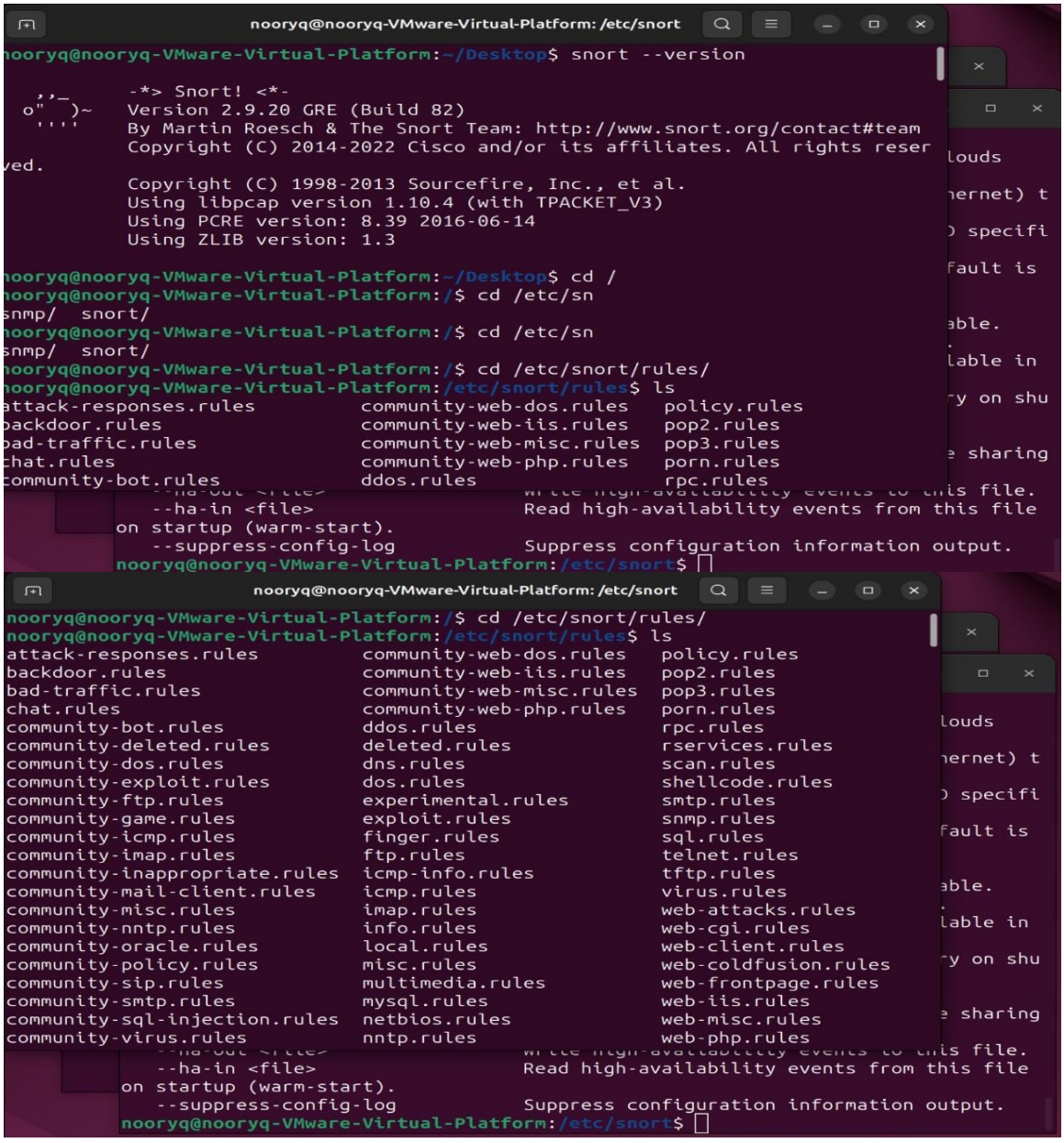

https://192.168.18.130/arkime/sessions?date=1
Sessions
SPIView
SPIGraph
Connections
Hunt
Files
Stats
History
Settings
v5.7.1
Search
Search
Last hour
Start
2025/08/12 11:16:54
End
2025/08/12 12:16:54
Bounding
Last Packet
Interval
Auto
50 per page
Showing 0 of 0 entries
Protocols
Data Source
Log Type
Start Time
Stop Time
Src IP / Country
Src Port
Dst IP / Country
Dst Port
Packets
Databytes / Bytes
I'm hootin
cancel
Welcome guest! Check out our help page for more information, or click the owl on the top left.
Dismiss
Got it!
Arkime v5.7.1 | arkime.com | Malc⊛lm | Dashboards | NetBox | 0ms



Protocols	Data Source	Log Type	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes
udp	udp dns	arkime	session	2025/08/12 11:22:28	2025/08/12 11:22:28	192.168.18.130	56,210	192.168.18.2	53	1	51 93
udp	udp dns	arkime	session	2025/08/12 11:22:28	2025/08/12 11:22:28	192.168.18.130	54,183	192.168.18.2	53	2	102 186
udp	udp dns	arkime	session	2025/08/12 11:22:28	2025/08/12 11:22:28	192.168.18.130	52,416	192.168.18.2	53	2	102 186
udp	udp dns	arkime	session	2025/08/12 11:22:28	2025/08/12 11:22:28	192.168.18.130	43,194	192.168.18.2	53	2	102 186
udp	udp dns	arkime	session	2025/08/12 11:22:28	2025/08/12 11:22:28	192.168.18.130	59,975	192.168.18.2	53	2	102 186
udp	udp dns	arkime	session	2025/08/12 11:22:28	2025/08/12 11:22:28	192.168.18.130	52,989	192.168.18.2	53	2	102 186
udp	udp dns	arkime	session	2025/08/12 11:22:28	2025/08/12 11:22:28	192.168.18.130	58,046	192.168.18.2	53	2	102 186
udp	udp dns	arkime	session	2025/08/12 11:22:27	2025/08/12 11:22:27	192.168.18.130	44,059	192.168.18.2	53	2	102 186
udp	udp dns	arkime	session	2025/08/12	2025/08/12	192.168.18.130	34,842	192.168.18.2	53	2	102

After that we used snort :

We have install snort in the same pc in Ubuntu



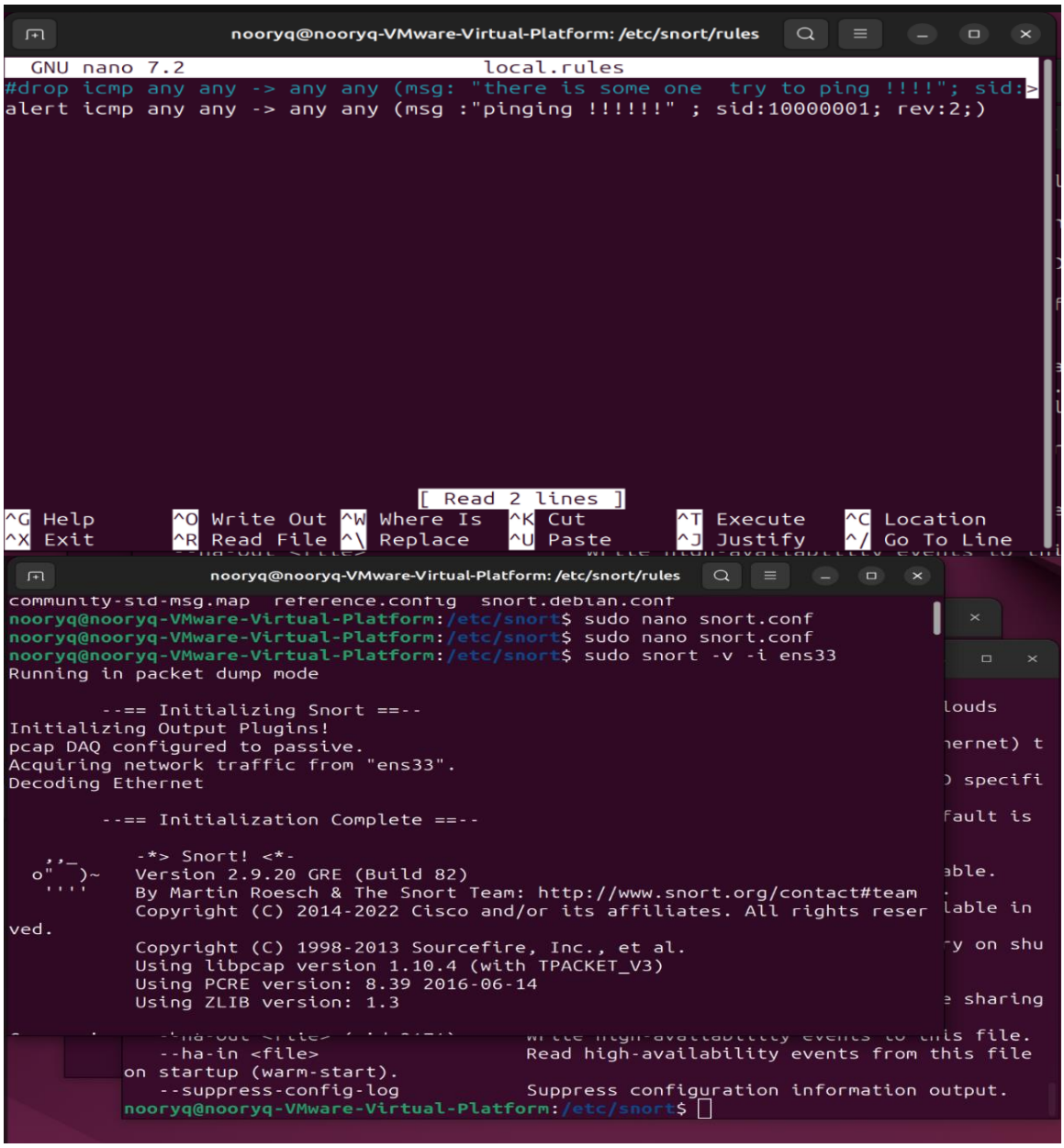
```
community-exploit.rules         dos.rules                   shellcode.rules
community-ftp.rules             experimental.rules          smtp.rules
community-game.rules            exploit.rules               snmp.rules
community-icmp.rules            finger.rules                sql.rules
community-imap.rules            ftp.rules                   telnet.rules
community-inappropriate.rules   icmp-info.rules             tftp.rules
community-mail-client.rules     icmp.rules                  virus.rules
community-misc.rules            imap.rules                  web-attacks.rules
community-nntp.rules            info.rules                  web-cgi.rules
community-oracle.rules          local.rules                 web-client.rules
community-policy.rules          misc.rules                  web-coldfusion.rules
community-sip.rules             multimedia.rules            web-frontpage.rules
community-smtp.rules            mysql.rules                 web-iis.rules
community-sql-injection.rules   netbios.rules               web-misc.rules
community-virus.rules           nntp.rules                  web-php.rules
community-web-attacks.rules     oracle.rules                x11.rules
community-web-cgi.rules         other-ids.rules
community-web-client.rules      p2p.rules
nooryq@nooryq-VMware-Virtual-Platform:/etc/snort/rules$ sudo nano local.rules
[sudo] password for nooryq:
Sorry, try again.
[sudo] password for nooryq:
nooryq@nooryq-VMware-Virtual-Platform:/etc/snort/rules$ cd /etc/snort/
nooryq@nooryq-VMware-Virtual-Platform:/etc/snort$ ls
```

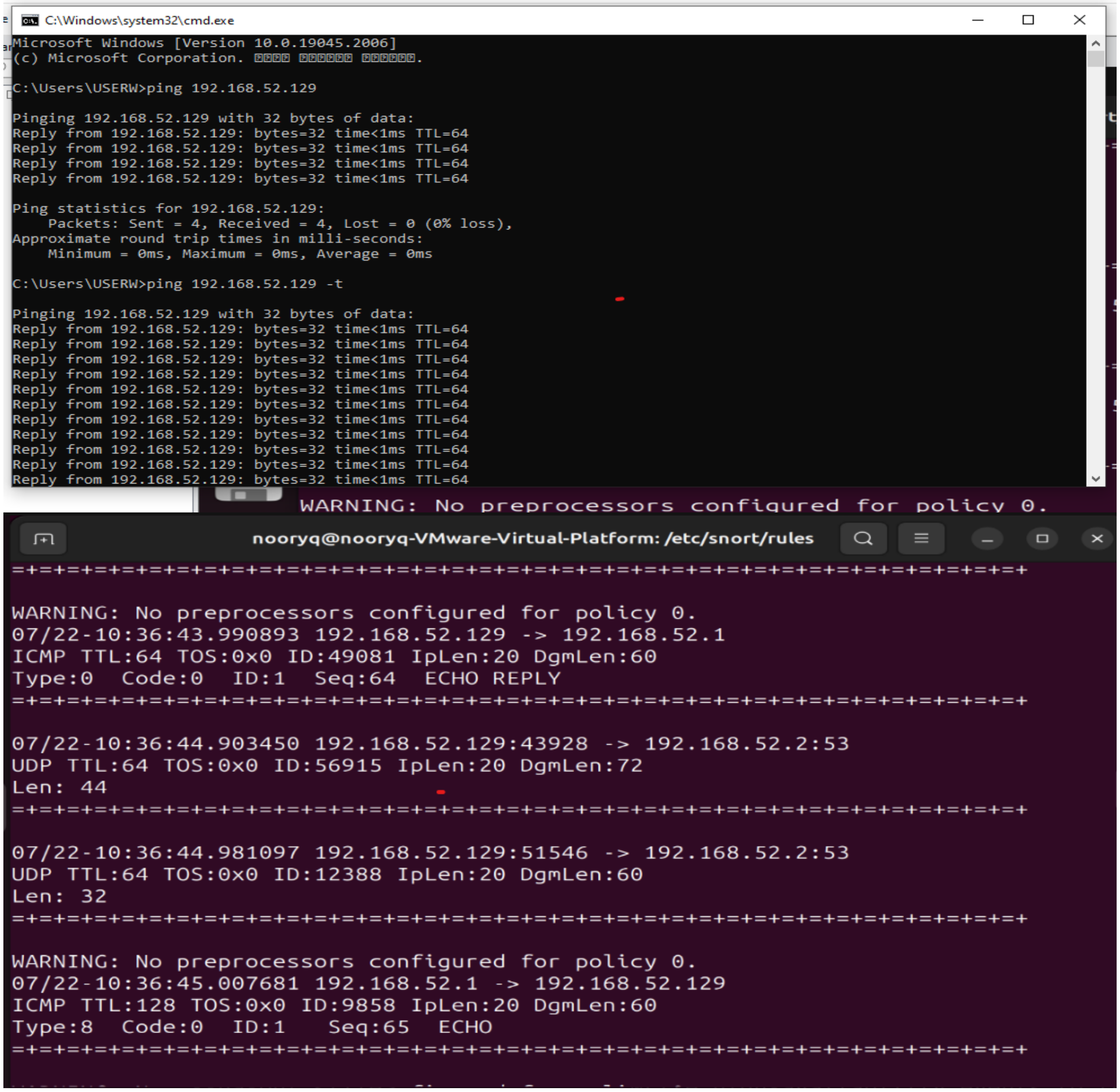
nooryq@nooryq-VMware-Virtual-Platform: /etc/snort/rules

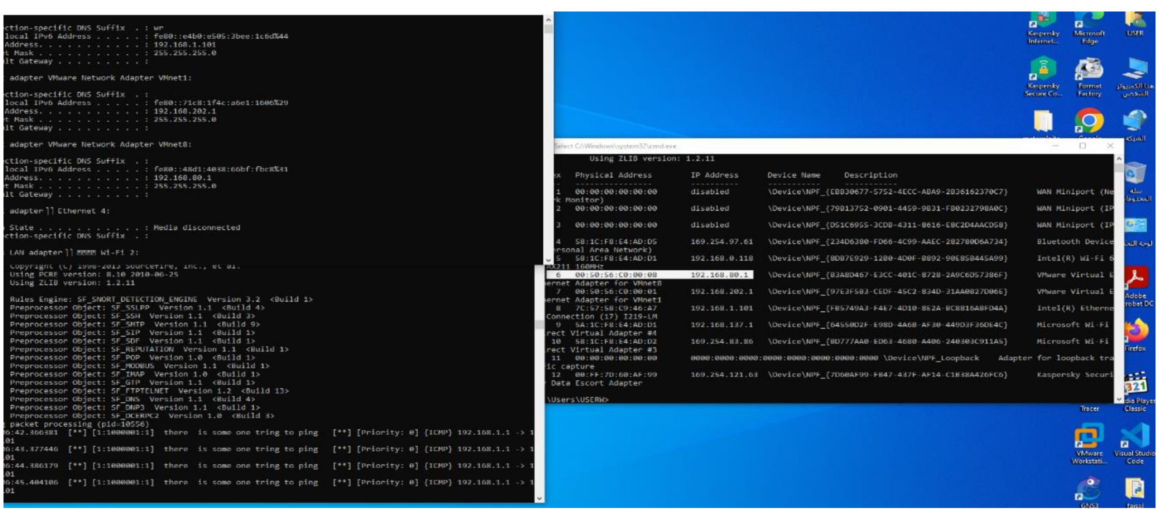
```
  GNU nano 7.2                          local.rules
#drop icmp any any -> any any (msg: "there is some one  try to ping !!!!"; sid:>
alert icmp any any -> any any (msg :"pinging !!!!!!" ; sid:10000001; rev:2;)
```

```
                        [ Read 2 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

This is how to maka now rule




C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation.
C:\Users\USERW>ping 192.168.52.129
Pinging 192.168.52.129 with 32 bytes of data:
Reply from 192.168.52.129: bytes=32 time<1ms TTL=64
Reply from 192.168.52.129: bytes=32 time<1ms TTL=64
Reply from 192.168.52.129: bytes=32 time<1ms TTL=64
Reply from 192.168.52.129: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.52.129:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\USERW>ping 192.168.52.129 -t
Pinging 192.168.52.129 with 32 bytes of data:
Reply from 192.168.52.129: bytes=32 time<1ms TTL=64
WARNING: No preprocessors configured for policy 0.
nooryq@nooryq-VMware-Virtual-Platform: /etc/snort/rules
WARNING: No preprocessors configured for policy 0.
07/22-10:36:43.990893 192.168.52.129 -> 192.168.52.1
ICMP TTL:64 TOS:0x0 ID:49081 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:64 ECHO REPLY
07/22-10:36:44.903450 192.168.52.129:43928 -> 192.168.52.2:53
UDP TTL:64 TOS:0x0 ID:56915 IpLen:20 DgmLen:72
Len: 44
07/22-10:36:44.981097 192.168.52.129:51546 -> 192.168.52.2:53
UDP TTL:64 TOS:0x0 ID:12388 IpLen:20 DgmLen:60
Len: 32
WARNING: No preprocessors configured for policy 0.
07/22-10:36:45.007681 192.168.52.1 -> 192.168.52.129
ICMP TTL:128 TOS:0x0 ID:9858 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:65 ECHO

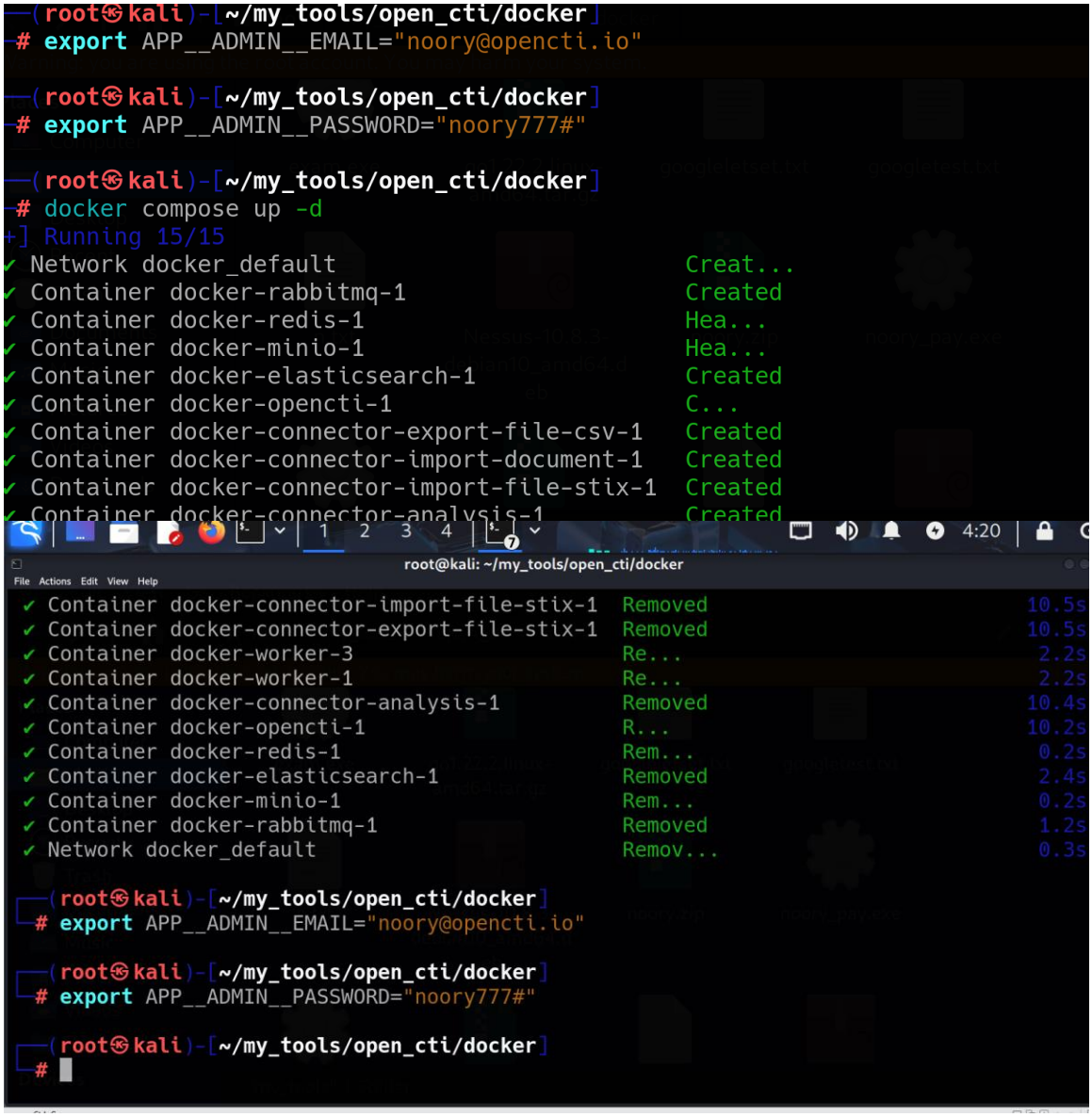


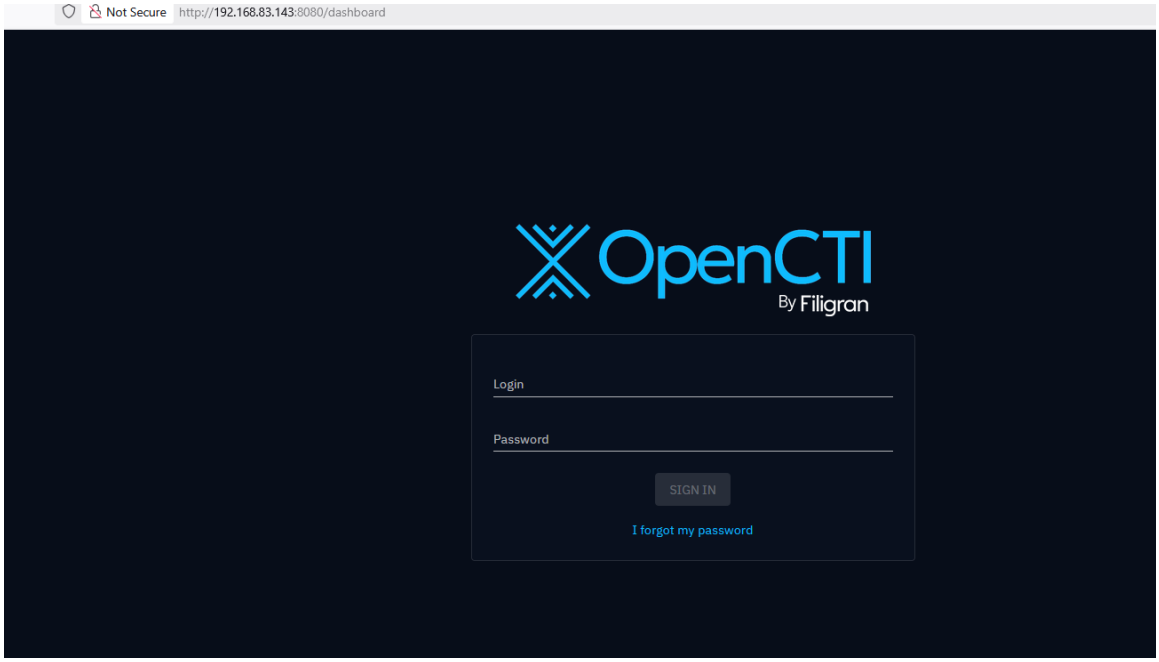
After that in all kali of red team I have install opencti

By run kali and type su to switch to root then type cd /

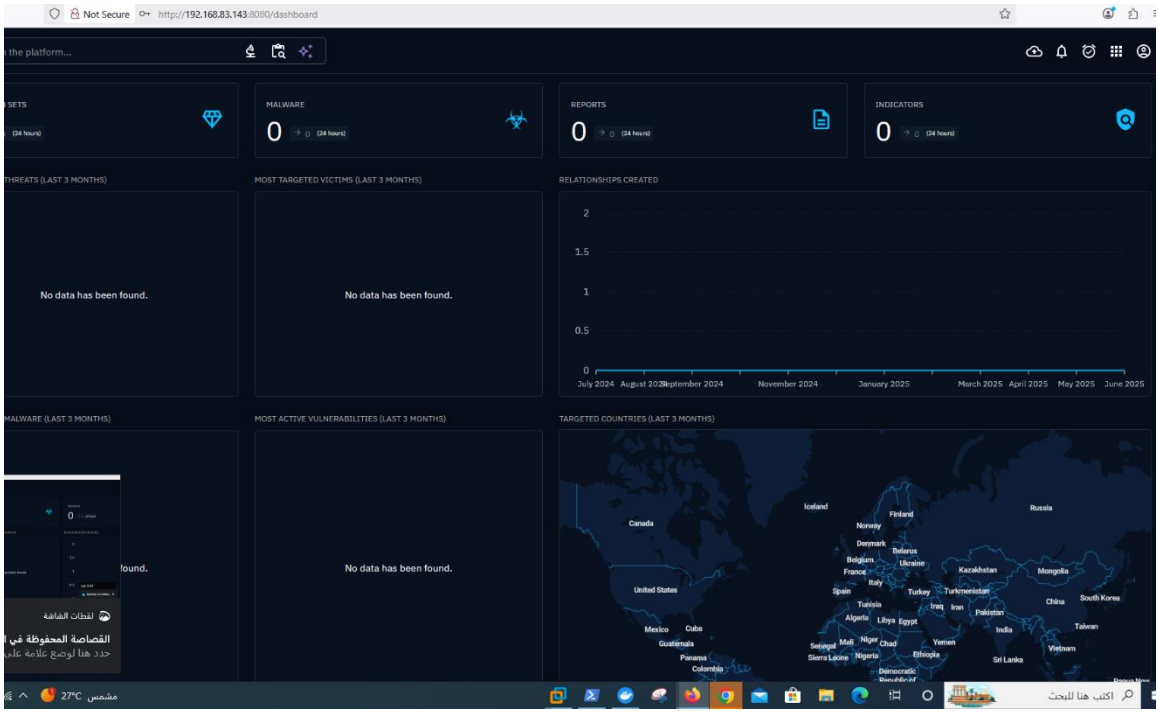
After that go to file name my_tools/opencti/docker

In this file type docker compose up –d



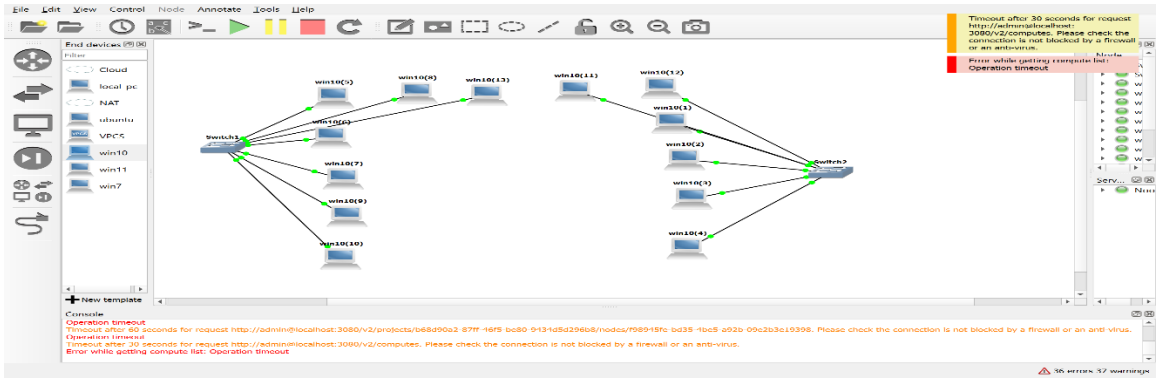


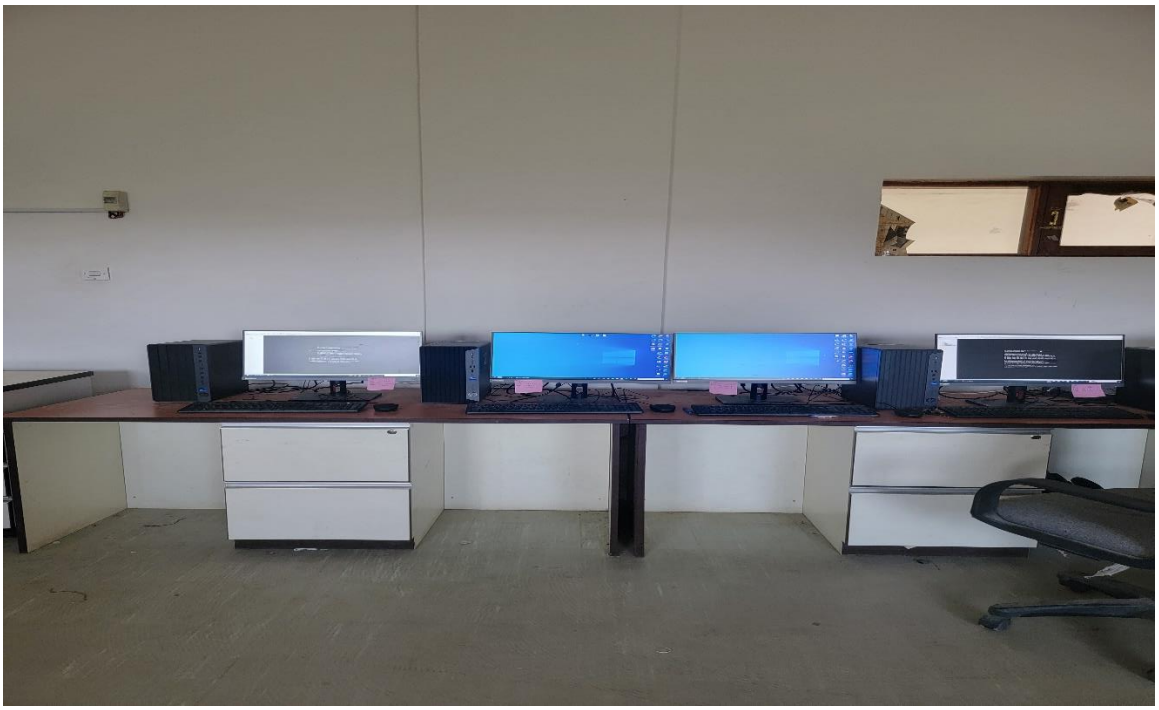
After that inter the user name and the password I edit user name and password to admin admin but you can see what is use name and password in the same file location by type cat ./env

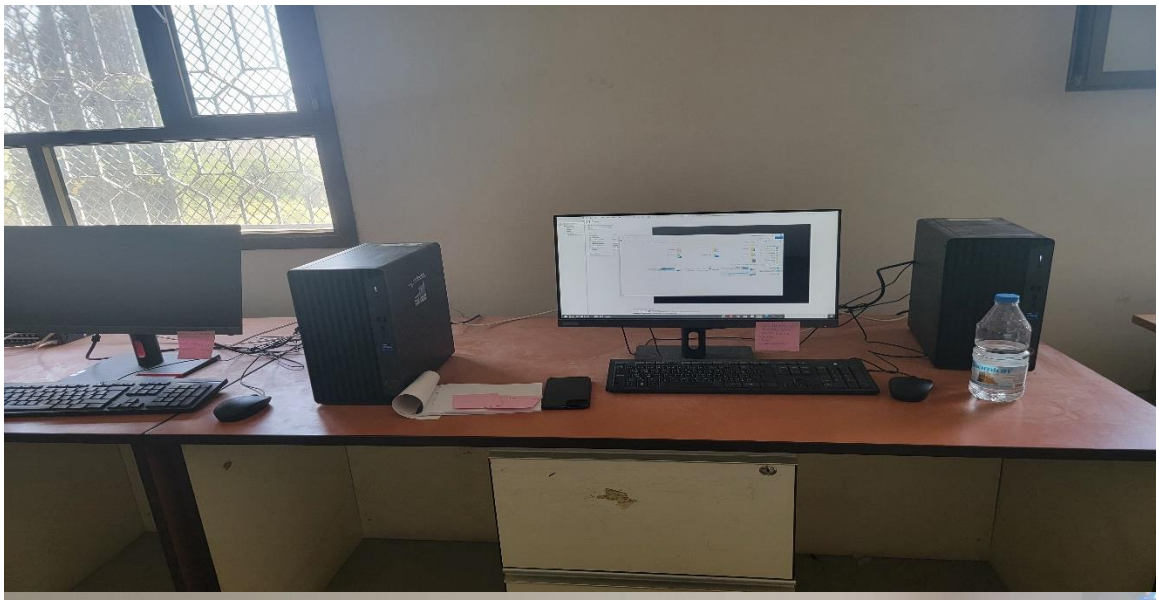


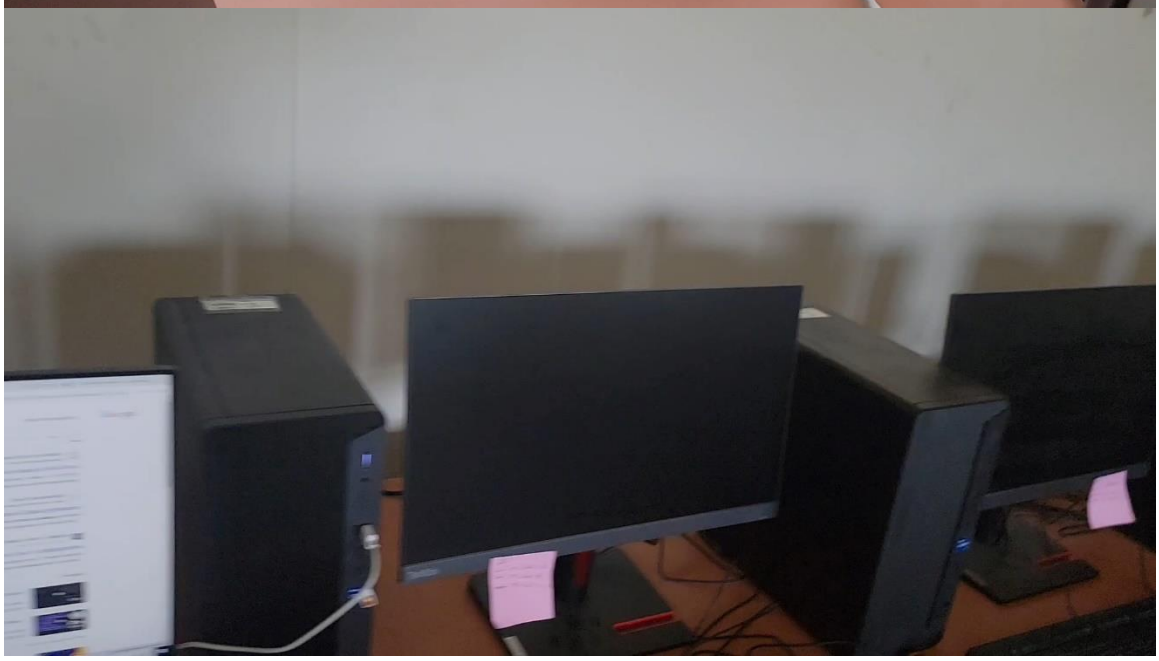
After running opencti add the connactors as you want to use this threat intelligence

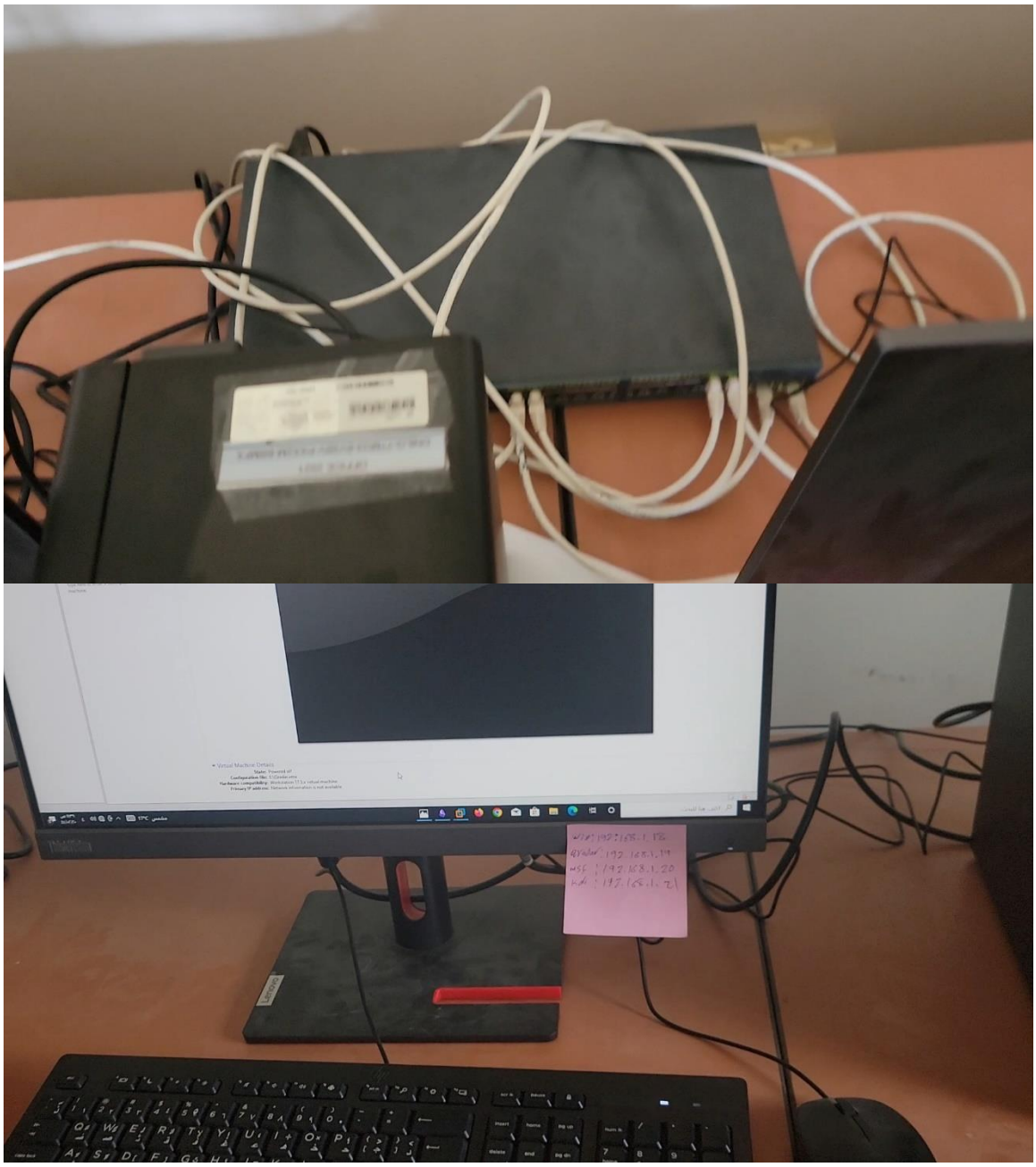
We have prepare the lab from scratch by connect devices and install services and prepare os in each pc and connect each them as this phote



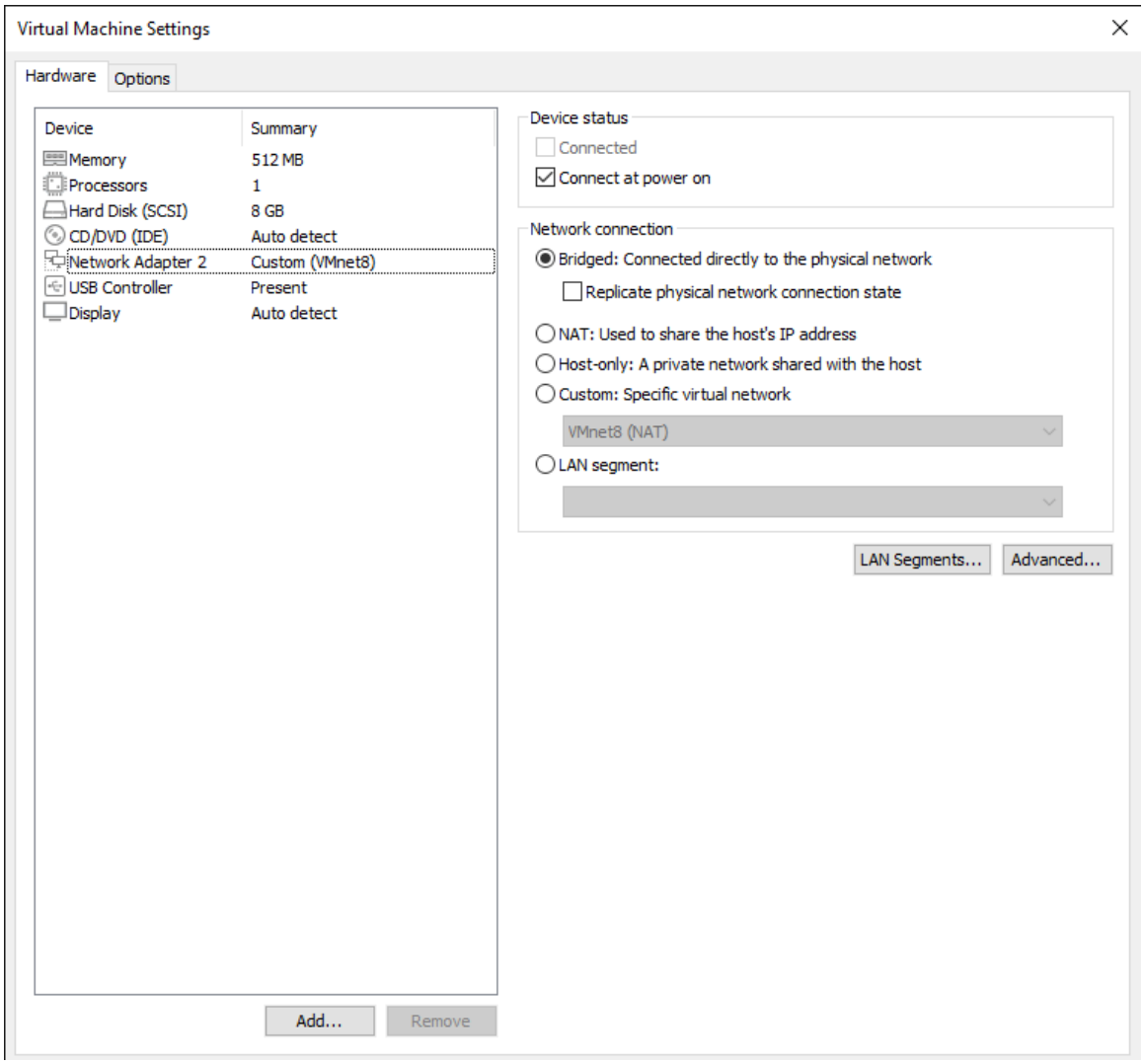


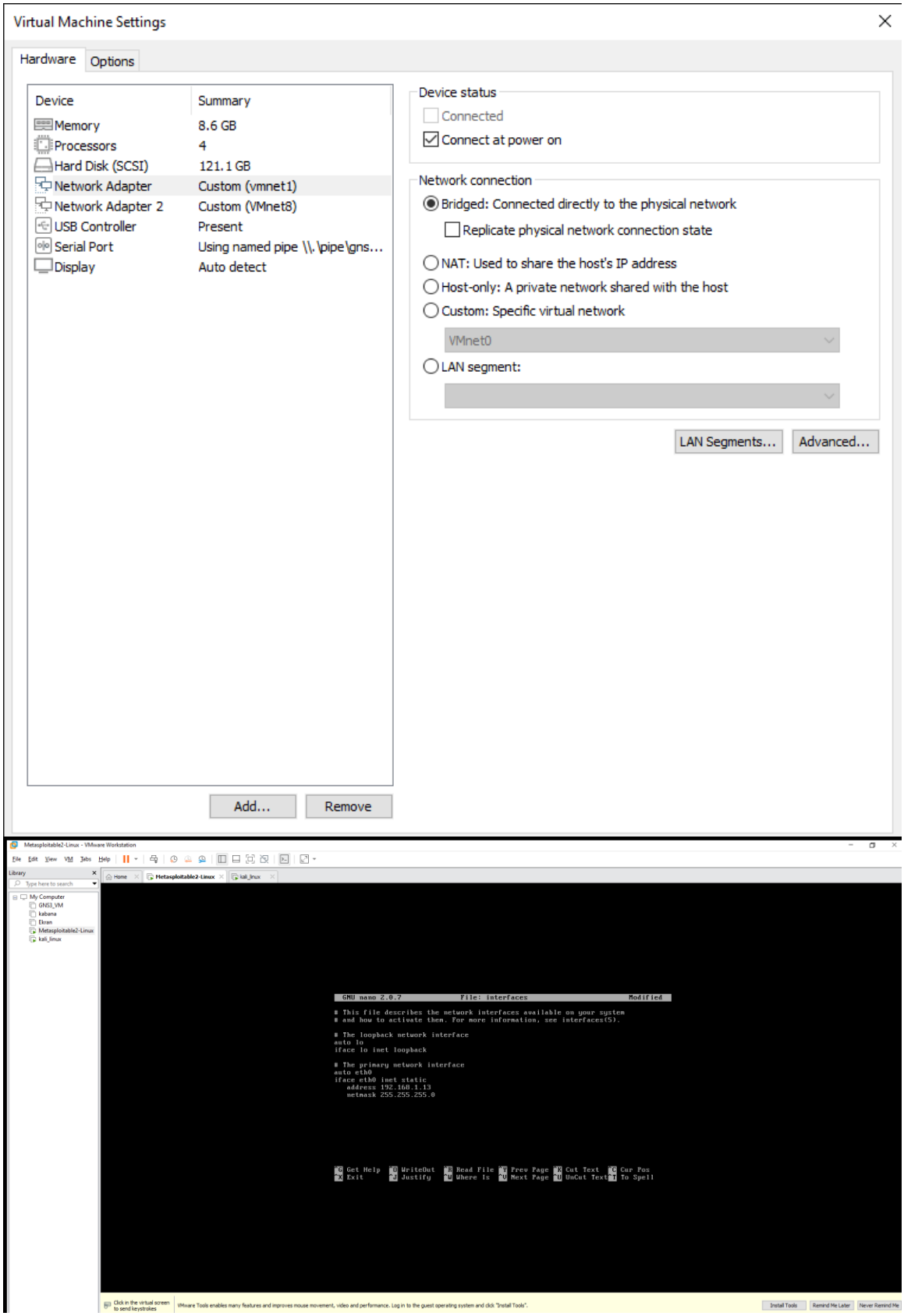


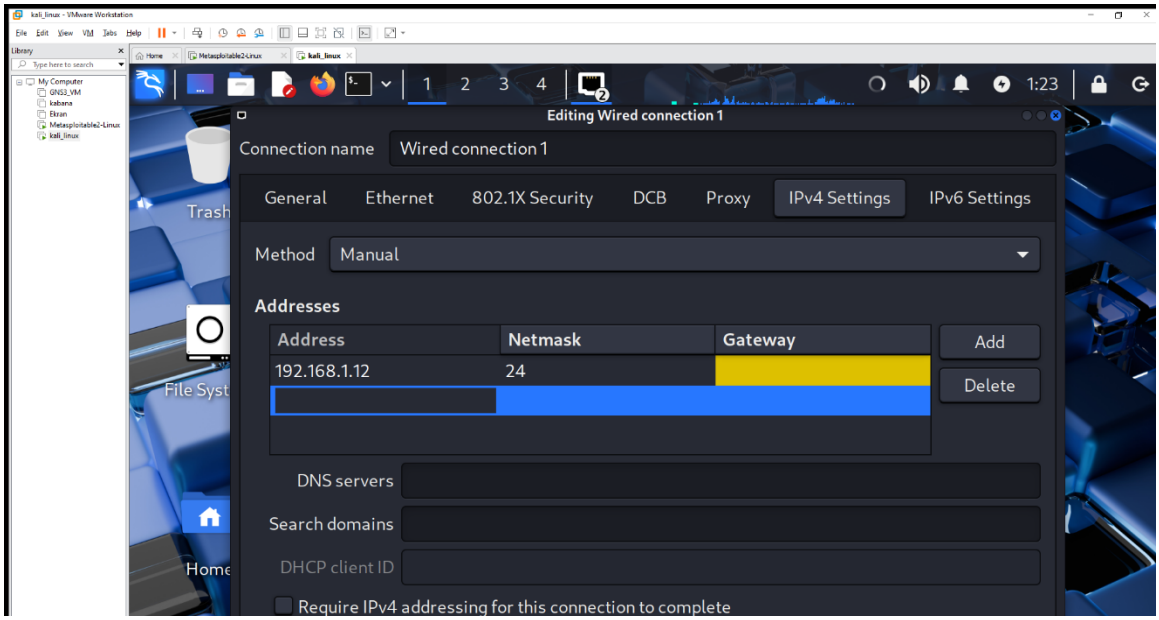




after that we connect each os such as kali and Metasploitable to each network in lab by doing this steps




Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
8.6 GB
Processors
4
Hard Disk (SCSI)
121.1 GB
Network Adapter
Custom (vmnet1)
Network Adapter 2
Custom (VMnet8)
USB Controller
Present
Serial Port
Using named pipe \\.\pipe\gns...
Display
Auto detect
Add...
Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN Segments...
Advanced...
GNU nano 2.0.7
File: interfaces
Modified
This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).
The loopback network interface
auto lo
iface lo inet loopback
The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.13
netmask 255.255.255.0
Get Help
WriteOut
Read File
Prev Page
Cut Text
Cur Pos
Exit
Justify
Where Is
Next Page
UnCut Text
To Spell


Editing Wired connection 1
Connection name
Wired connection 1
General
Ethernet
802.1X Security
DCB
Proxy
IPv4 Settings
IPv6 Settings
Method
Manual
Addresses
Address
Netmask
Gateway
192.168.1.12
24
Add
Delete
DNS servers
Search domains
DHCP client ID
Require IPv4 addressing for this connection to complete
Trash
Home
1:23