Configuration Manual

MSc Research Project
MSc in Cybersecurity

Alessandro Gentili
Student ID: x19176546

School of Computing
National College of Ireland

Supervisor: Ross Spelman

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Alessandro Gentili

Student ID: x19176546

Programme: MSc in Cybersecurity **Year:** 2021/2022

Module: Internship

Lecturer: Ross Spelman

Submission Due Date: 15/08/2022

Project Title: The Impact of Conti Ransomware on a Modern Virtualized Environment

Word Count: 1500 **Page Count:** 13

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Alessandro Gentili ……………………………………………………………………………

Date: 15/08/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Alessandro Gentili
Student ID:x19176546

1 Overview

This document presents all the necessary steps to create a secure and anonymous malware virtual lab, ad-hoc tailored for studying the Conti ransomware and its interaction (impact) with a modern virtual environment.

2 Requirements

2.1 Functional Requirements

The main requirement is to establish a secure tunnel that will protect the researcher during their study in two different cases. The first is during dynamic analysis (when the Conti ransomware is running), and the second is in the worst-case scenario if the malware finds a way to communicate with its C&C server. The Conti Group is a large criminal organization, and it is vital to use all possible precautions to avoid revealing personal information. The idea is to enforce a secure tunnel with the internet respecting all the C.I.A. (Confidentiality, Integrity, Availability) principles. The tunnel will be made secure using an encrypted channel through a VPN connection to encrypt all the packets. The T.O.R. Network will hide the actual I.P. address. The Malware Analyst workstation will automatically get a local I.P. address, transparently routed in the background to the internet through a Linux Gateway.

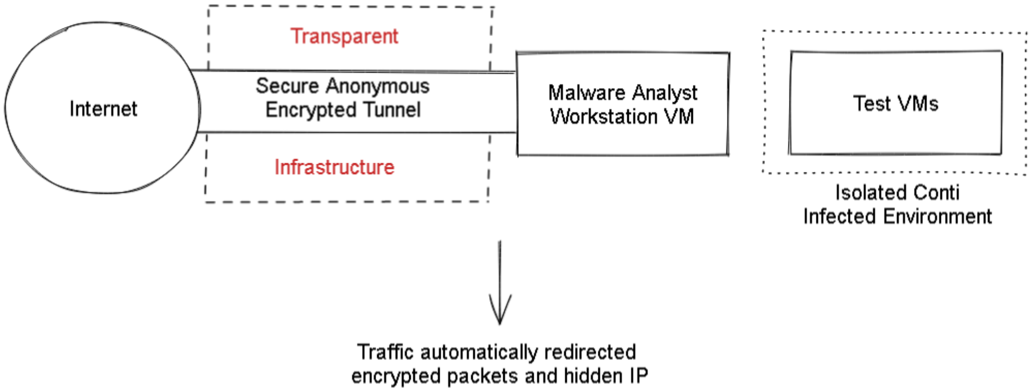
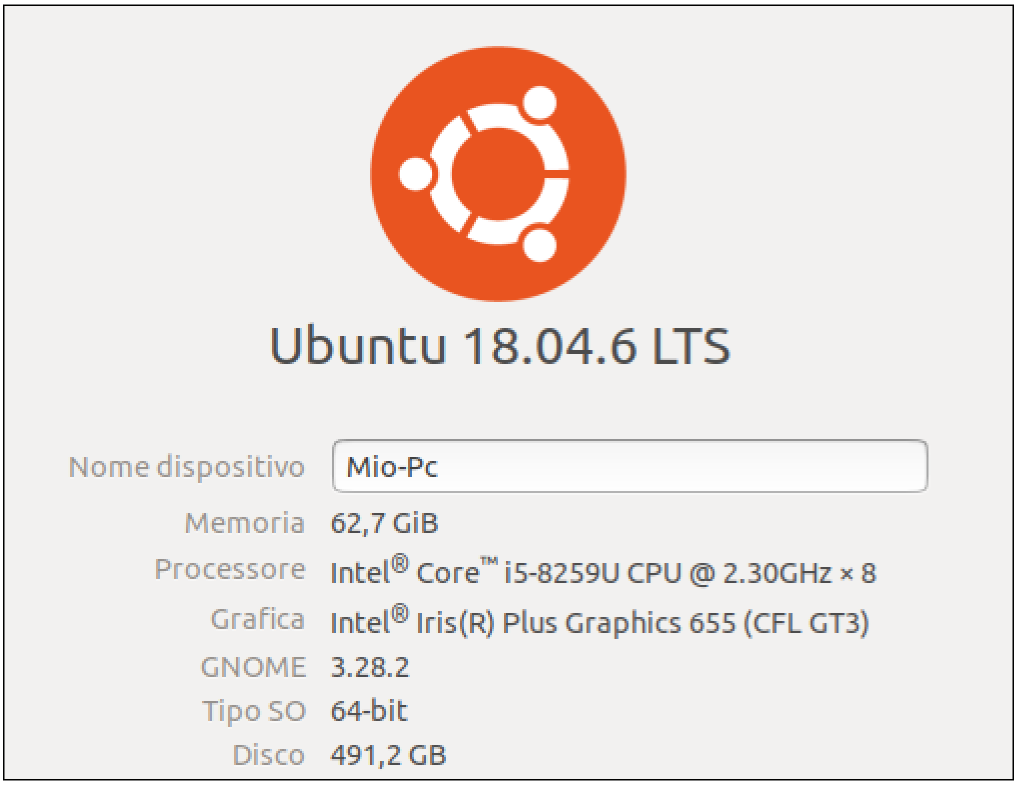


Figure 1 Conceptual Diagram

2.2 Workstation Operating System

Linux Distribution Ubuntu 18.04.6 LTS

- Stability
- Open Source/Free
- Long Term Support
- Immune from Windows-based Malware



Ubuntu 18.04.6 LTS

Nome dispositivo: Mio-Pc

Memoria: 62,7 GiB

Processore: Intel® Core™ i5-8259U CPU @ 2.30GHz × 8

Grafica: Intel® Iris(R) Plus Graphics 655 (CFL GT3)

GNOME: 3.28.2

Tipo SO: 64-bit

Disco: 491,2 GB

Figure 2 Workstation O.S.

2.3 Software

Hypervisor (type 2)	VMware Workstation 16 Pro (Linux vers.)

Table 1 - Hypervisor Software

2.4 Hardware

Platform	Intel NUC
CPU	i5 (8 threads)
RAM	64 G.B.

Drives	500 NVME SSD + 1TB SATA SSD
Network	1Gbit ethernet adapter
Mobile Device	Samsung Note 10 Lite
Network Adapter	USB-C Ethernet Adapter

Table 2 – Hardware

3 Environment Setup

This section highlights the installation process of each part composing the virtual lab specifically designed to analyze the Conti ransomware. The description starts from the most external device (the mobile connection) to the most internal (Test Virtual Machines).

3.1 Overview

The conceptual diagram below illustrates an overall picture of the project architecture and how anonymous-encrypted connectivity has been achieved.

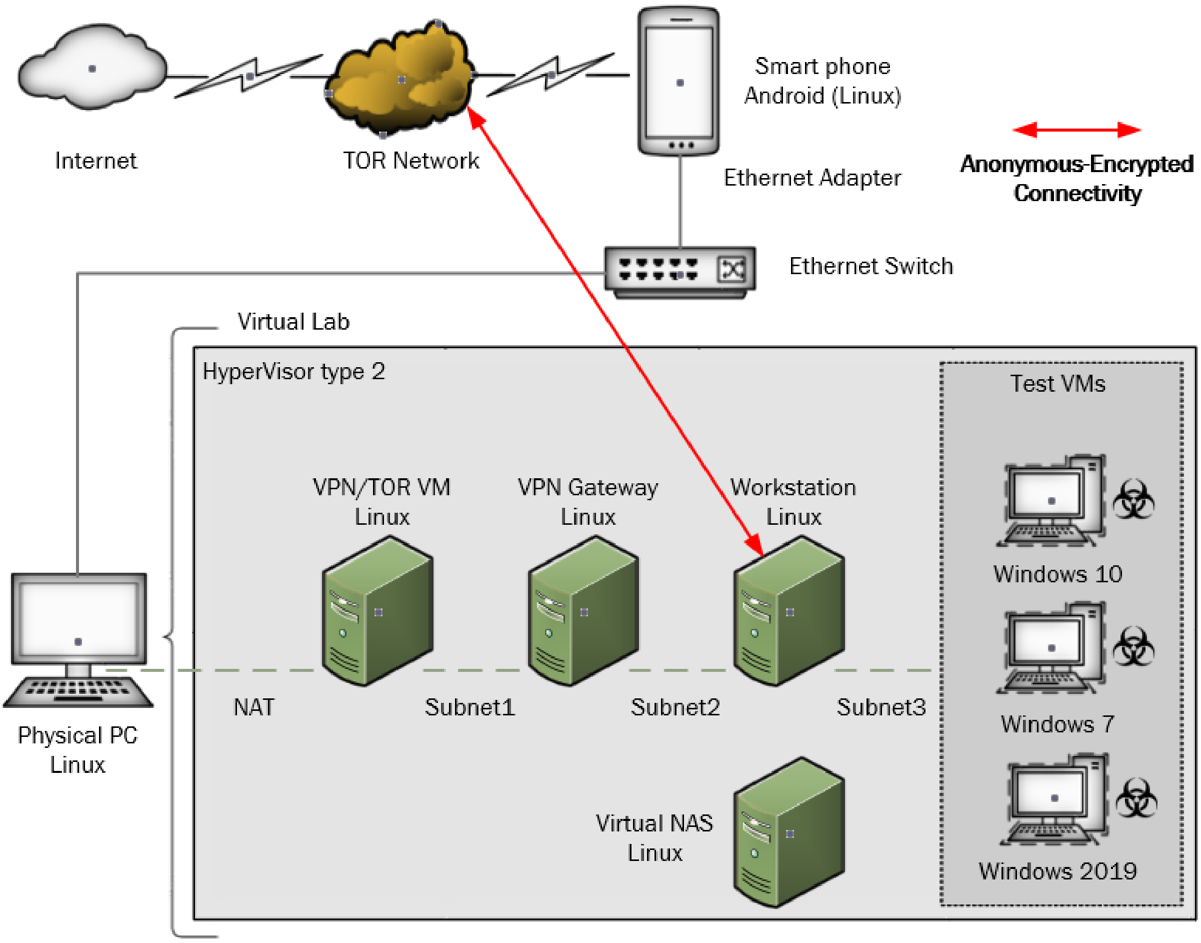


Figure 3 Conceptual Diagram

3.2 Installation

3.2.1 Mobile Device

The use of a mobile phone for dedicated internet connectivity ensures two things:

- The network is not part of a home/organization (enforcing even more isolation)
- The mobile connection is less oriented to be geolocated and traced

The android mobile device (Samsung Note 10 Lite) relates to a USB-C ethernet adapter to share through DHCP the internet connection to the physical machine that will share with N.A.T. to the virtual environment.

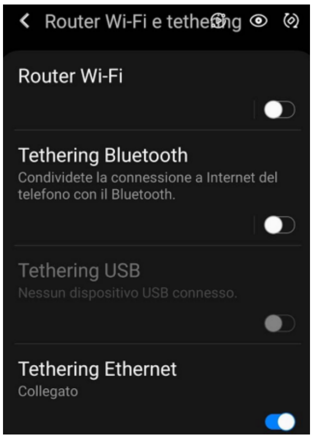
 Router Wi-Fi e tethering Router Wi-Fi ○ Tethering Bluetooth Condividete la connessione a Internet del telefono con il Bluetooth. ○ Tethering USB Nessun dispositivo USB connesso. ○ Tethering Ethernet Collegato ●		

Table 3 – Tethering, Note 10 Lite, Ethernet USB-C Adapter

3.2.2 Physical Machine

VMware Workstation Pro 16 can run several V.M.s thanks to the massive amount of RAM (64 G.B.) and up to 20 different virtual networks crucial for this project.

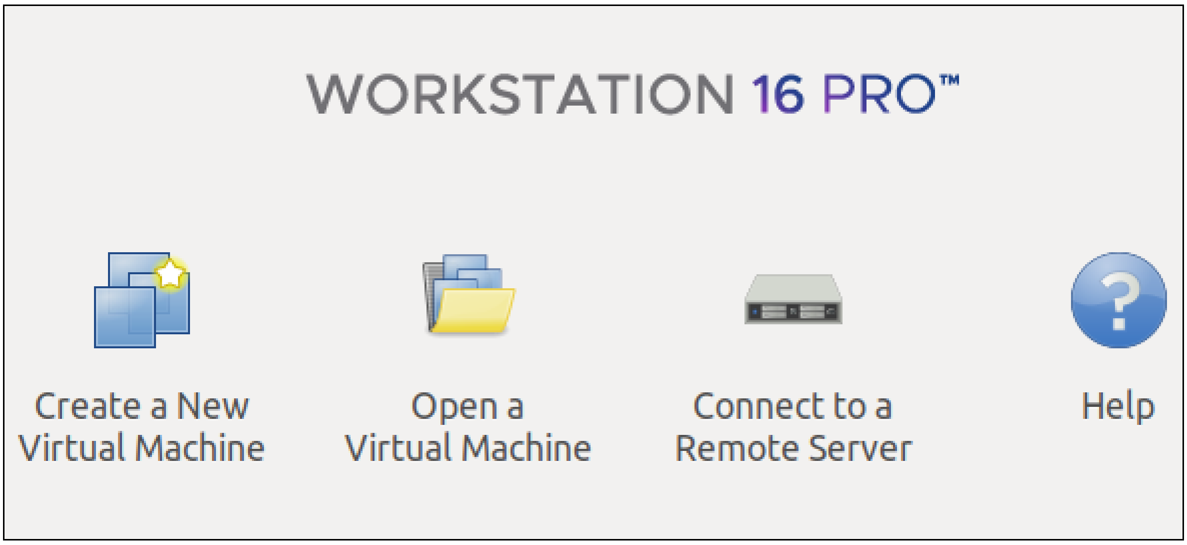
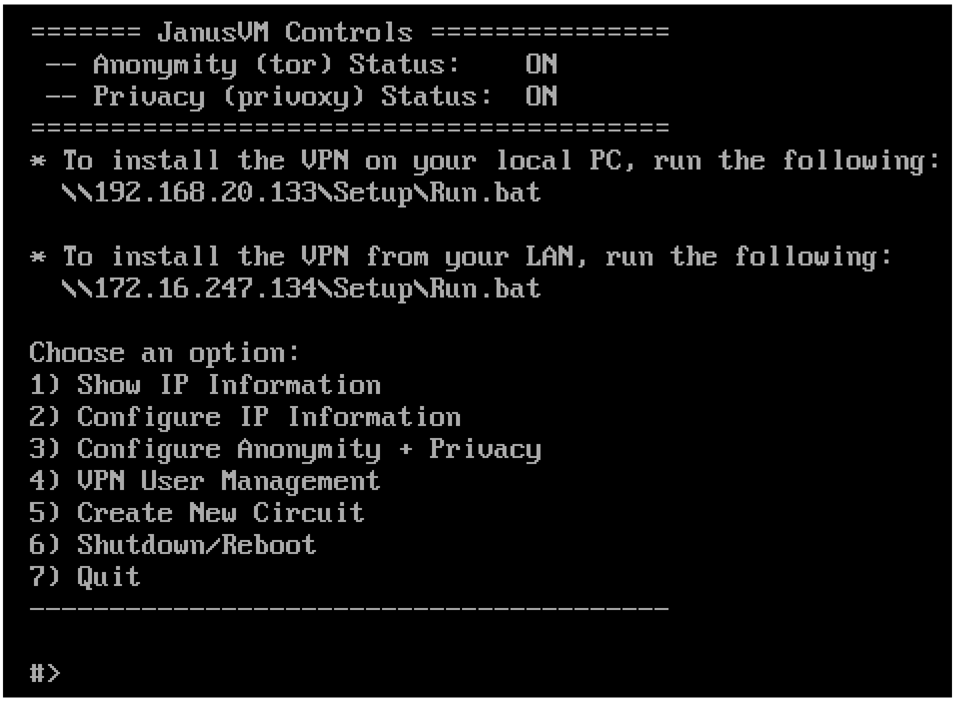


Figure 4 Hypervisor type 2

3.2.3 VPN-TOR Server



```
======= JanusVM Controls ===============
 -- Anonymity (tor) Status:    ON
 -- Privacy (privoxy) Status:  ON
========================================
* To install the VPN on your local PC, run the following:
  \\192.168.20.133\Setup\Run.bat

* To install the VPN from your LAN, run the following:
  \\172.16.247.134\Setup\Run.bat

Choose an option:
1) Show IP Information
2) Configure IP Information
3) Configure Anonymity + Privacy
4) VPN User Management
5) Create New Circuit
6) Shutdown/Reboot
7) Quit
----------------------------------------

#>
```

Figure 5 VPN-TOR Server (Janus VM)

The VPN server needs to be set up with a valid user and password for the client.

3.2.4 Gateway Linux

The Linux gateway (Ubuntu 16 L.T.S.) acts as an intermediary between the external VPN-TOR server and the malware analysis workstation Virtual Machine. The gateway will be a client for the VPN-TOR server and a server that will route all the packets for the malware analysis workstation and all the potential Virtua Machines in that subnet.

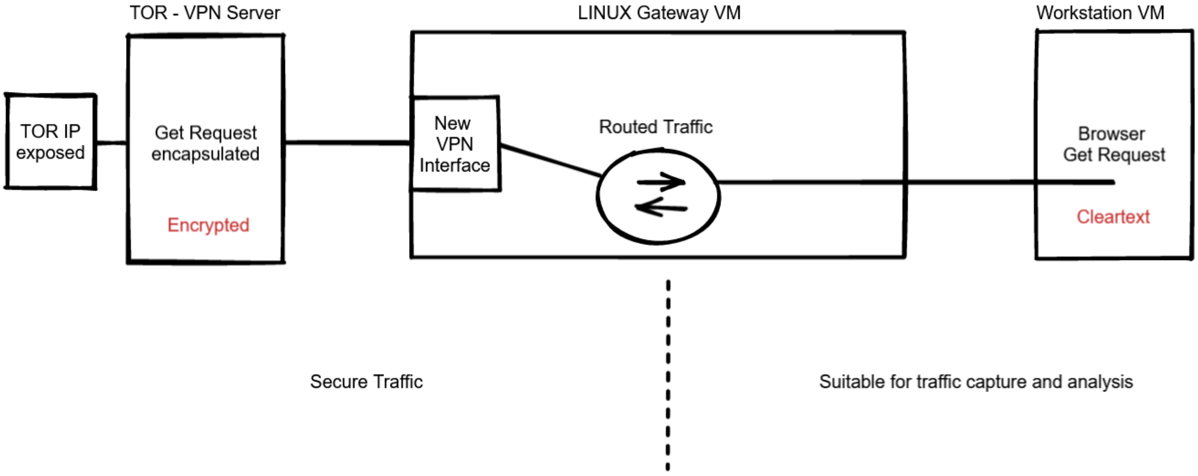
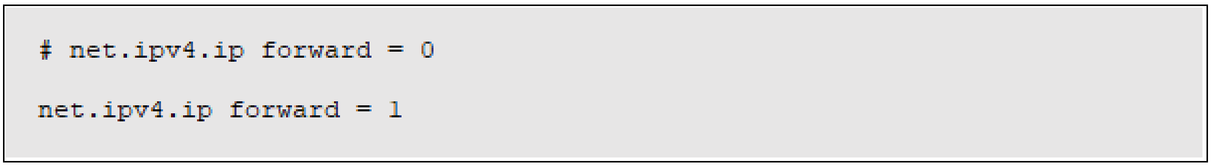


Figure 6 Gateway Linux V.M.

To enable the routing in the Linux Gateway V.M. is necessary to change the value from 0 to 1 as shown in the below file /etc/sysctl.conf. (for ipv4 requests to be forwarded from the internal vmnet3 to the newly created VPN interface).

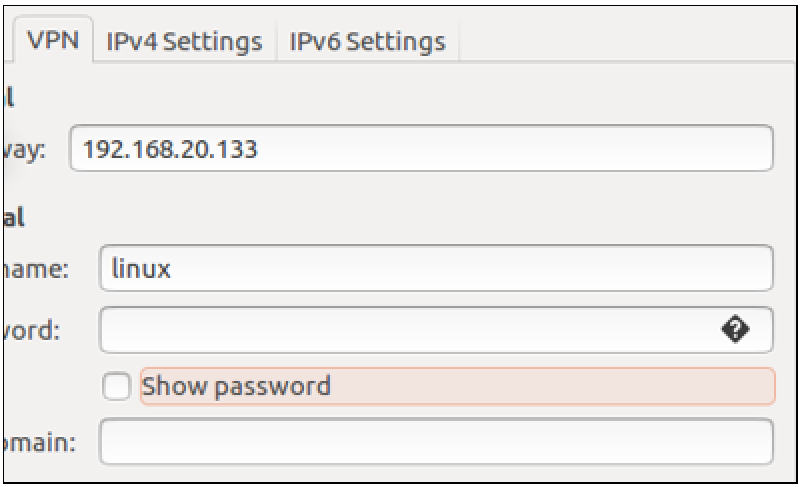


```
# net.ipv4.ip forward = 0

net.ipv4.ip forward = 1
```

Figure 7 Code snippet to enable routing

Enabling the VPN connection can be done via G.U.I.:



vay: 192.168.20.133

ame: linux

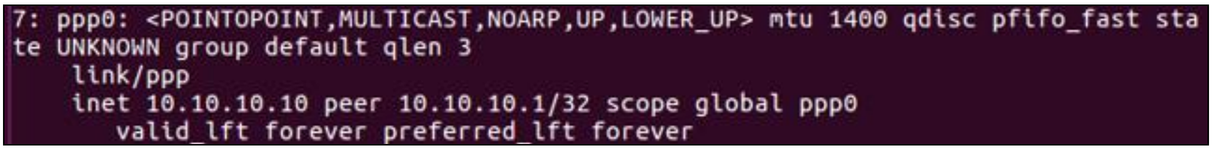
ord:

□ Show password

main:

Figure 8 VPN GUI setting

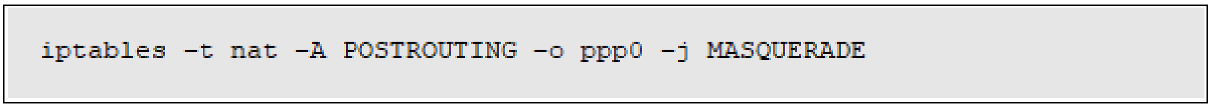
The previous step will create the new VPN interface where the packets will be routed.



```
7: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1400 qdisc pfifo_fast sta
te UNKNOWN group default qlen 3
    link/ppp
    inet 10.10.10.10 peer 10.10.10.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

Figure 9 Newly created VPN interface

To redirect all the traffic to the new interface is necessary to use N.A.T.:



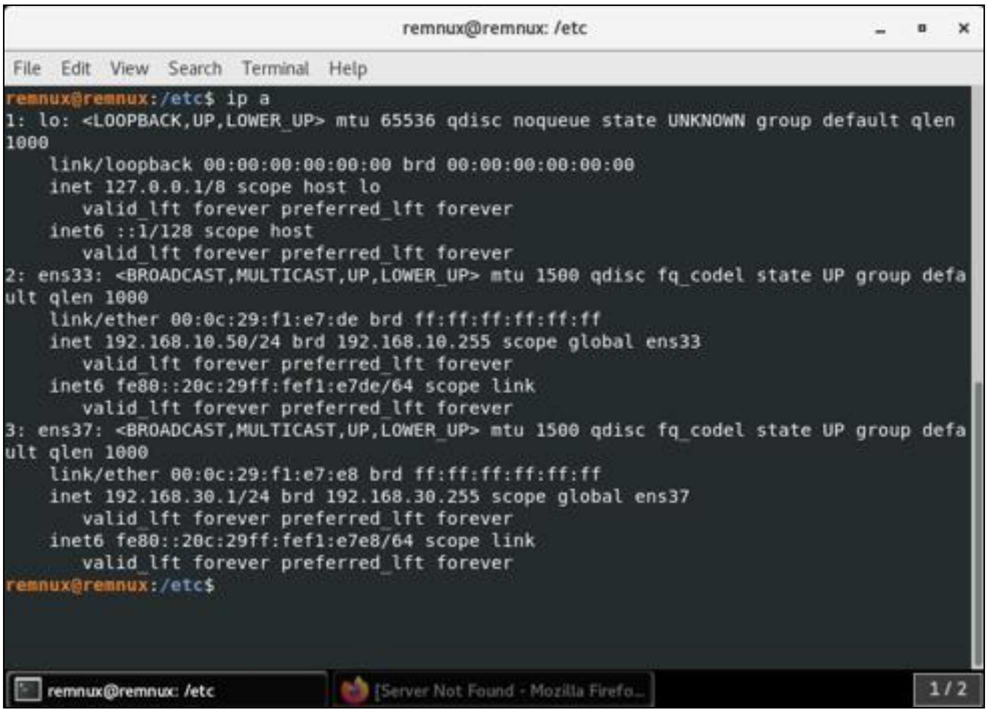
```
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Figure 10 Code snippet – How to redirect traffic to VPN interface

Note: To verify that the change has been applied successfully (command: iptables –t nat -list-rules).

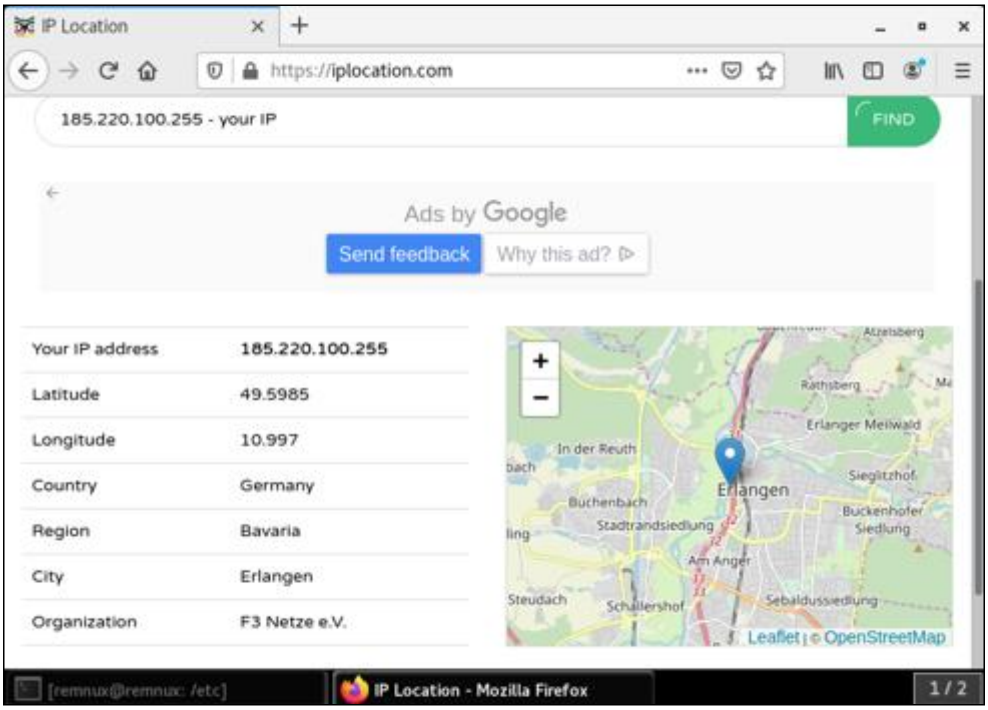
3.2.5 Remnux

Remnux is a tailored Linux Ubuntu 18 based distribution with embedded malware analysis tools.


remnux@remnux: /etc
File Edit View Search Terminal Help
remnux@remnux: /etc
[Server Not Found - Mozilla Firefo...
1 / 2

```
remnux@remnux:/etc$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defa
ult qlen 1000
    link/ether 00:0c:29:f1:e7:de brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.50/24 brd 192.168.10.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef1:e7de/64 scope link
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defa
ult qlen 1000
    link/ether 00:0c:29:f1:e7:e8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.30.1/24 brd 192.168.30.255 scope global ens37
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef1:e7e8/64 scope link
       valid_lft forever preferred_lft forever
remnux@remnux:/etc$
```

Figure 11 Remnux network interfaces



185.220.100.255 - your IP

Your IP address	185.220.100.255
Latitude	49.5985
Longitude	10.997
Country	Germany
Region	Bavaria
City	Erlangen
Organization	F3 Netze e.V.

Figure 12 Remnux T.O.R. IP

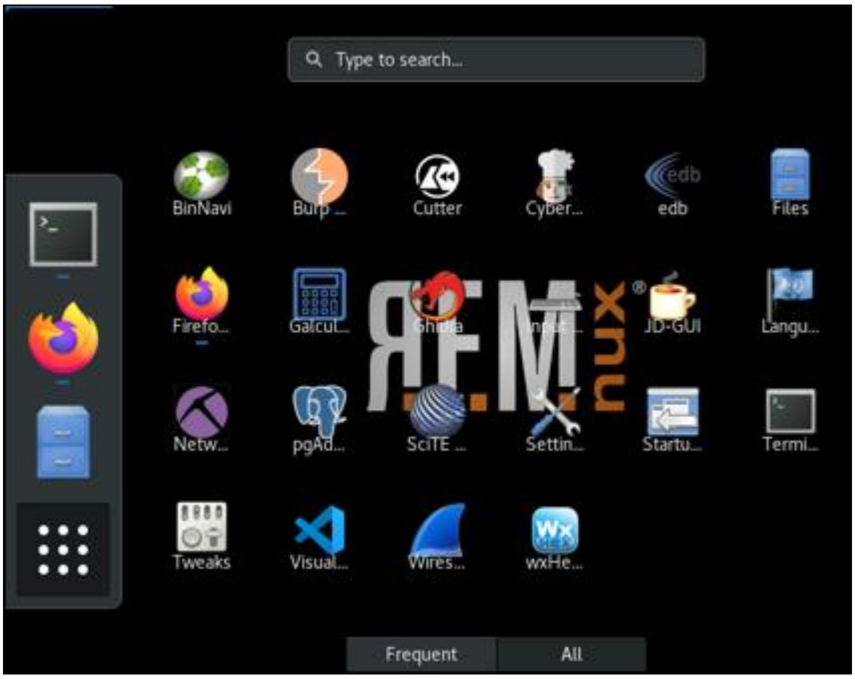


Figure 13 Malware analysis tools

It has one network interface connected to the Linux Gateway and another to the same subnet of the Test V.M.s and the N.A.S. The previous step makes the network capture easier because here, the traffic is isolated, and there is no VPN encryption, so the packets are exchanged in clear text. It is possible to see how the Linux gateway provides internet connectivity, but the T.O.R. network automatically hides the I.P.

3.2.6 Test V.M.s

These are the Windows virtual machines chosen to be infected by the Conti ransomware because they are the most used at the time of writing and will produce more reliable data to be analyzed.

Test V.M.	Network Address	Description
Windows Server 2019	192.168.30.5	Windows Server release
Windows 10 Pro	192.168.30.3	Most common client version
Windows 7 64bit	192.168.30.4	Old client version still in use

Table 3 – Test V.M.s

The main V.M. used for the test is the one with Windows 10 Pro. This operating system is the most commonly used among all virtual infrastructures as a client or workstation to manage servers. The Flare V.M[1]. has been installed in the Windows 10 PRO V.M.

Flare V.M. integrates all the tools that a Malware Analyst requires both for static and dynamic analysis.

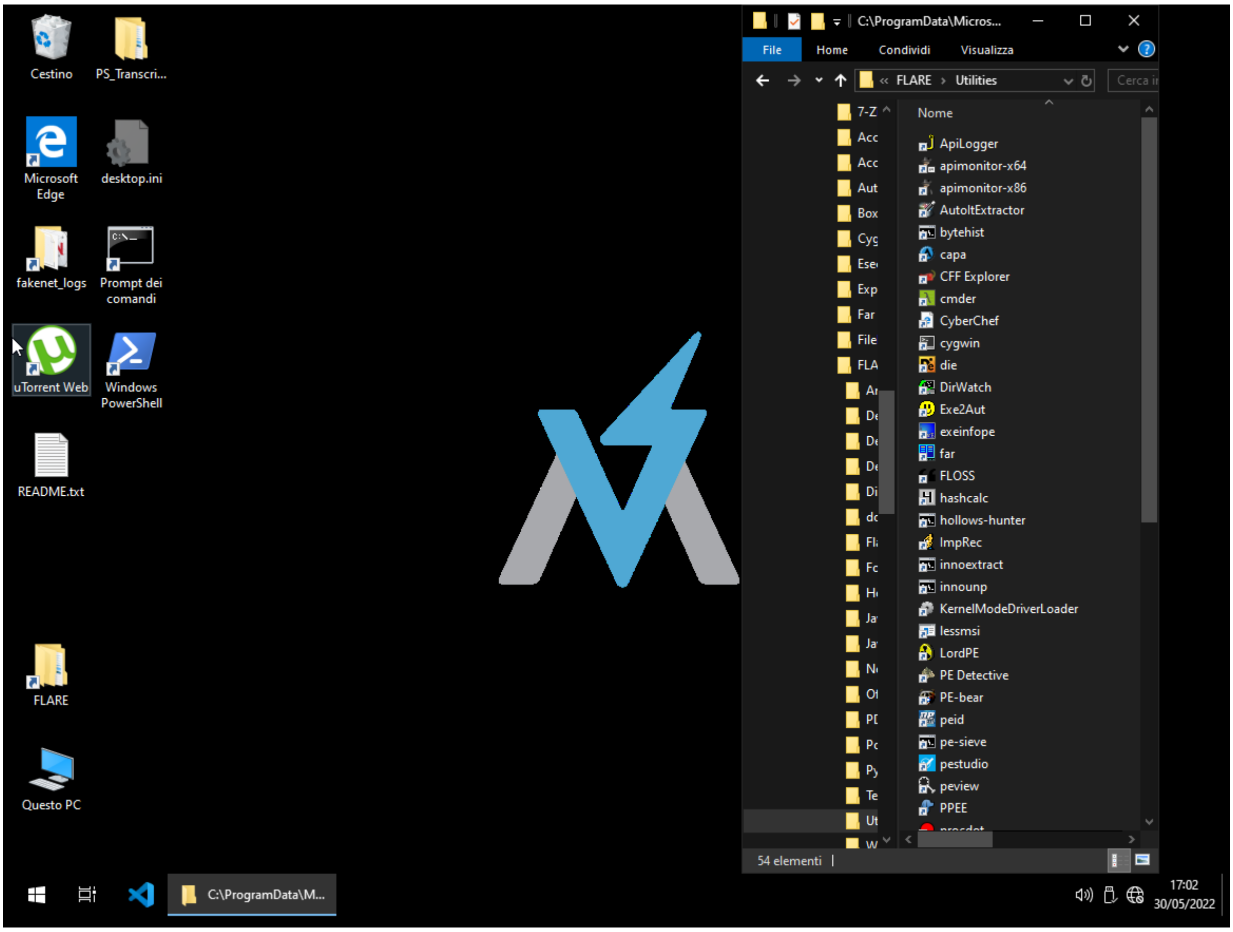


Figure 14 Flare V.M. and tools

The installation is performed using a Powershell installer that requires admin privileges and will automatically install and reboot the operating system a few times. In addition, there are hundreds of tools and utilities for reverse engineering the code and network captures, such as Fakenet, Wireshark, and PeStudio.

3.2.7 Virtual N.A.S.

OpenMediaVault is a Linux distribution developed to provide a reliable N.A.S. (Network Attached Storage) for sharing files in a network. It is an excellent solution to store files from the test V.M.s because it is immune to Windows malware like Conti.

[1] https://github.com/mandiant/flare-vm

3.3 Networking Configuration

The network configuration has been designed to maintain all the C.I.A. principles, especially confidentiality. It is of vital importance that the researcher's identity is not compromised and remains not known to the members of the Conti group.

The network is composed of four subnets. The most external subnet gets internet access with N.A.T. (Network Access Translation), chosen over bridging because this ensures that the internal network is not browsable from the outside, augmenting the overall security.

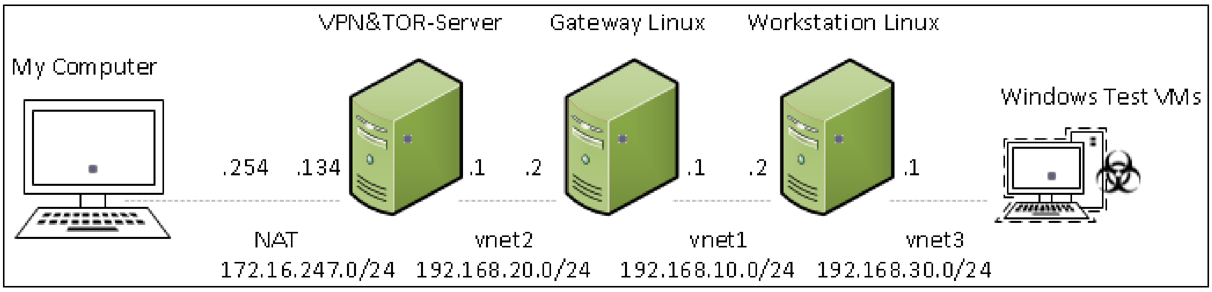
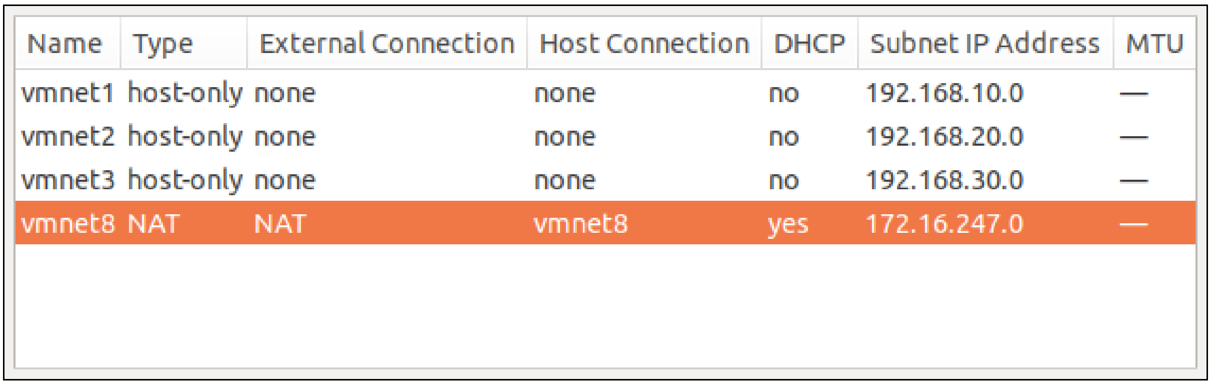


Figure 15 Virtual Lab subnets



Name	Type	External Connection	Host Connection	DHCP	Subnet IP Address	MTU
vmnet1	host-only	none	none	no	192.168.10.0	—
vmnet2	host-only	none	none	no	192.168.20.0	—
vmnet3	host-only	none	none	no	192.168.30.0	—
vmnet8	NAT	NAT	vmnet8	yes	172.16.247.0	—

Figure 16 Virtual Lab subnets

The design enhances the network isolation; it is possible to shut down a node to block the connectivity to the external. The Linux gateway is a different virtual machine than the malware workstation; therefore, a researcher can continue working and doing tests with the most external nodes powered off. The encryption ensures that cryptography is used in the packet. This action protects the information from being leaked if the traffic is intercepted. On the other hand, in the most internal subnet (192.168.30.0/24), the VPN encryption has not been applied yet. Thus the researchers will conduct experiments with plain text packets efficiently. Anonymity is achieved using the T.O.R. network by hiding the real internet I.P. so that the Conti group can not trace the geographical location of the virtual lab. In addition, the internet connection is established using a mobile operator to exclude infection in the local area network of the house/company.

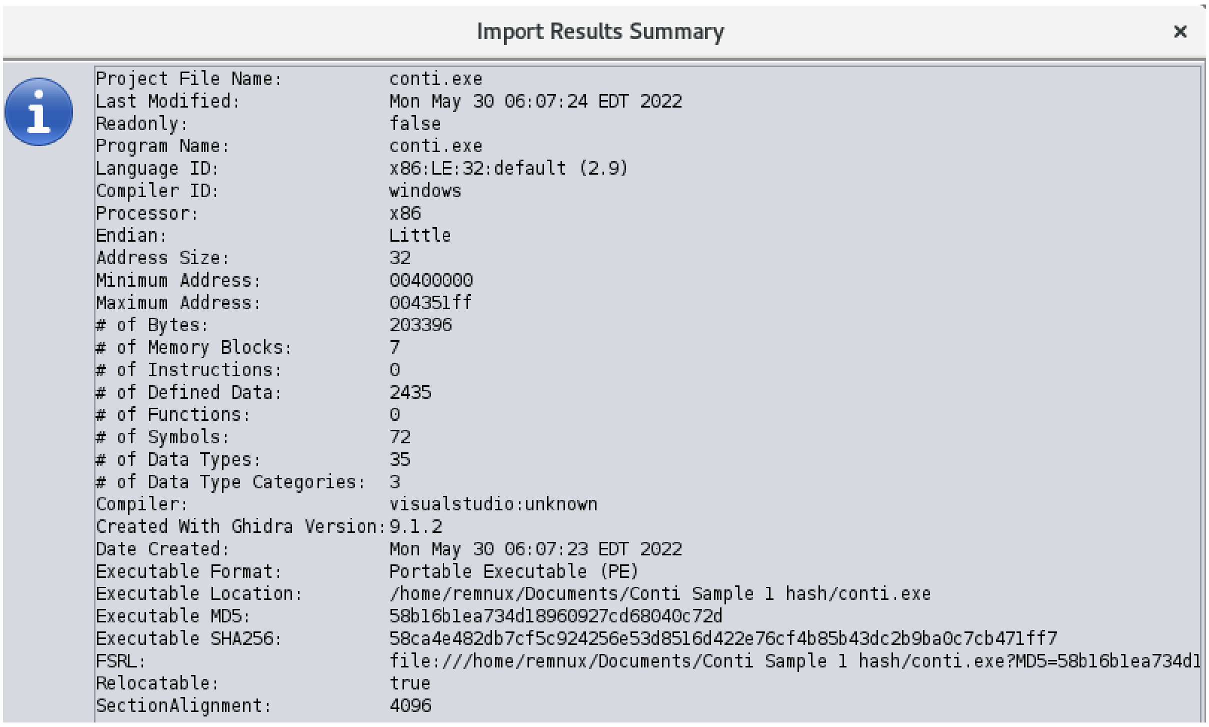
4 Using the System

4.1 Conti Sample

In order to experiment, the Conti sample must be downloaded from a trusted website and executed safely.

Even though the website has a good reputation, it is always best practice to verify the sample's integrity by comparing the two hash values. First, the one advertised on the website, and second, the one gathered from the sample downloaded.

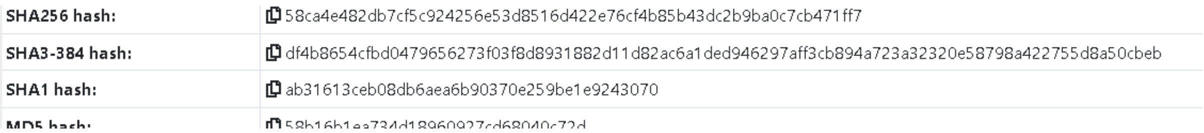
Details collected with PeStudio:



```
Project File Name:            conti.exe
Last Modified:                Mon May 30 06:07:24 EDT 2022
Readonly:                     false
Program Name:                 conti.exe
Language ID:                  x86:LE:32:default (2.9)
Compiler ID:                  windows
Processor:                    x86
Endian:                       Little
Address Size:                 32
Minimum Address:              00400000
Maximum Address:              004351ff
# of Bytes:                   203396
# of Memory Blocks:           7
# of Instructions:            0
# of Defined Data:            2435
# of Functions:               0
# of Symbols:                 72
# of Data Types:              35
# of Data Type Categories:    3
Compiler:                     visualstudio:unknown
Created With Ghidra Version:9.1.2
Date Created:                 Mon May 30 06:07:23 EDT 2022
Executable Format:            Portable Executable (PE)
Executable Location:          /home/remnux/Documents/Conti Sample 1 hash/conti.exe
Executable MD5:               58b16b1ea734d18960927cd68040c72d
Executable SHA256:            58ca4e482db7cf5c924256e53d8516d422e76cf4b85b43dc2b9ba0c7cb471ff7
FSRL:                         file:///home/remnux/Documents/Conti Sample 1 hash/conti.exe?MD5=58b16b1ea734d1
Relocatable:                  true
SectionAlignment:             4096
```

Figure 17 – Conti Sample Hash Value

SHA256 hash from MalwareBazaar by Abuse.ch

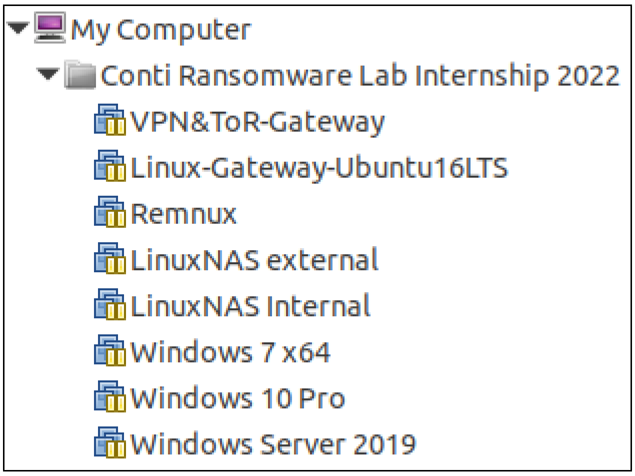


SHA256 hash:	58ca4e482db7cf5c924256e53d8516d422e76cf4b85b43dc2b9ba0c7cb471ff7
SHA3-384 hash:	df4b8654cfbd0479656273f03f8d8931882d11d82ac6a1ded946297aff3cb894a723a32320e58798a422755d8a50cbeb
SHA1 hash:	ab31613ceb08db6aea6b90370e259be1e9243070
MD5 hash:	58b16b1ea734d18960927cd68040c72d

As it is possible to see above, the hash values match.

4.2 Virtual Lab Utilization

Before experimenting, taking a snapshot of each virtual machine and backups to an external storage is good practice. Then, in case of mistakes or hardware failures, it will be possible to revert quickly to a valid previous state.



My Computer
Conti Ransomware Lab Internship 2022
VPN&ToR-Gateway
Linux-Gateway-Ubuntu16LTS
Remnux
LinuxNAS external
LinuxNAS Internal
Windows 7 x64
Windows 10 Pro
Windows Server 2019

Figure 18 Virtual Lab V.M.s

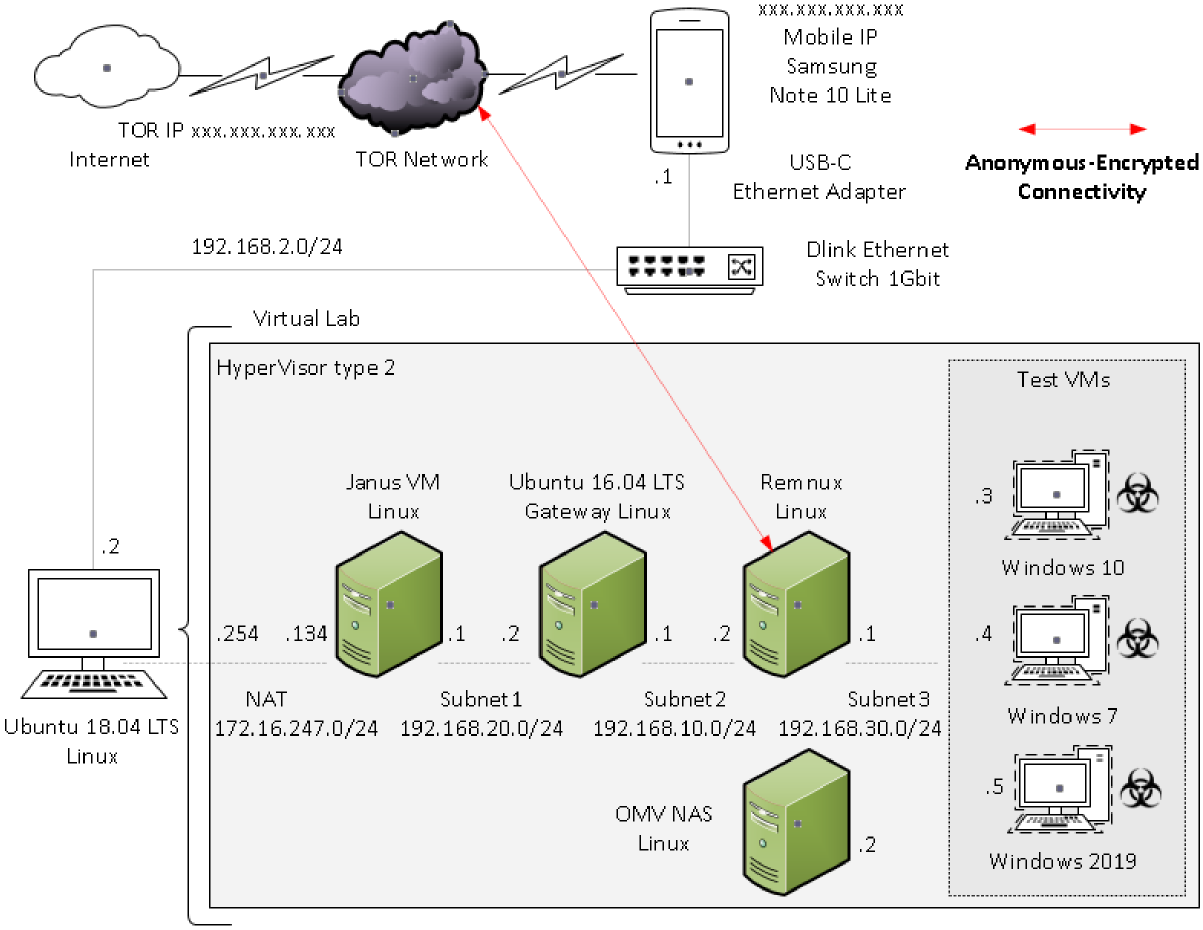


Figure 19 Virtual Lab in use

5 Data Sets

5.1 Experiment 1

5.1.1 Virtual Machines configuration files

Each VMware virtual machine has a .vmx in its folder with the specific configuration. Therefore, it is essential to use these files to reproduce the virtual lab configuration.

An example of the file below structure specifies the V.M. name, the hardware version and other important features:

```
#!/usr/bin/vmware
.encoding = "windows-1252"
displayName = "Infected_ Windows 10 Pro"
config.version = "8"
virtualHW.version = "16"
```

5.1.2 Encrypted Connection network capture pcap file

This file contains the capture of the network traffic from the gateway Linux machine to the external, showing that the connection is encrypted with the VPN and the packets are not readable.

5.2 Experiment 2

5.2.1 Kill Switches check output file

This file contains the output of the pestr command launched against the conti.exe, showing all the strings found.

5.2.2 I.D.A. Pro Disassembler files

The folder contains the files gathered with I.D.A. Pro when reverse engineering the conti.exe sample.

5.3 Experiment 3

5.3.1 Openshares vs. Protectedshares network capture pcap file

The pcap file contains the capture of the network traffic showing the attempts made by the conti.exe sample when encrypting the open share on the OMV NAS and the failure in encrypting the Windows Server share protected by authentication.