Introduction to network forensics

Analysis of an airport third-party VPN connection compromise

Toolset, Document for students

1.0

JANUARY 2019

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use:

csirt-relations@enisa.europa.eu

PGP Key ID:	31E777EC 66B6052A
PGP Key Fingerprint:	AAE2 1577 19C4 B3BE EDF7 0669 31E7 77EC 66B6 052A

For media enquiries about this paper, please use:

press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-288-2, DOI: 10.2824/995110

Table of Contents

1. What Will You Learn? 6
1.1 Analysis of an airport third-party VPN connection compromise 6
2. Introduction 7
3. Exercise Tasks 9
3.1 Task 1: Evidence 9
3.2 Task 2: Examine the network setup 11
3.3 Task 3: Examine the router log files 13
3.4 Task 4: Examine the attack 13
3.5 Tools used in this use-case 14
4. Glossary 15

PARAMETER	DESCRIPTION	DURATION
Main Objective	The purpose of this exercise is to show the students that encrypted Virtual Private Network (VPN) connections make the work of network forensics more difficult. The students will learn the danger of compromised VPN connections. The students will learn that research can be done on different log files with graphical tools or with command-line programs.	
Targeted Audience	This exercise is intended for (new) CERT personnel who are involved in network forensics, and is also valuable for (all) CERT employees who are involved in the daily response to incidents.	
Total Duration	4.0 hours	
Time Schedule	Introduction to the exercise and tools overview	0.75 hour
	Task 1: Evidence files	0.5 hour
	Task 2: Examine the network setup	0.5 hour
	Task 3: Examine the router log files	1.0 hour
	Task 4: Examine the attack	1.0 hour
	Summary of the exercise	0.5 hour
Frequency	It is advised to organise this exercise when new team members join a CERT/CSIRT.	

1. What Will You Learn?

1.1 Analysis of an airport third-party VPN connection compromise

Familiarize students with the concept of giving third parties access to business systems via a VPN connection and the associated risks:

- How VPN connections can be compromised
- How to use Wireshark to analyse network packet captures.
- How encrypted Virtual Private Network (VPN) connections make the work of network forensics more difficult.
- How to use command line tools to get the right information from log files.

2. Introduction

Background information of the case

A large (European) airport uses third parties to maintain applications in their core network. The airport uses VPN connections for remote access. With these VPN connections, external companies have access to the core network of the airport. "IT System Administrators Europe" (ITSAEU) is a fictional company that performs maintenance on one of the airports database servers and on applications. Bob, an ITSAEU employee, uses a VPN connection for maintenance. The VPN connection gives access to the complete core network of the airport.

The case

A hacker wants to break into one of the airport's applications. Because it is difficult to get into the core network of the airport from the outside, the attacker has to penetrate via a VPN connection from one of the maintenance parties.

It is Thursday and Bob is doing maintenance on the application of the airport. During the maintenance Bob uses the VPN connection from the airport. Bob finish at 17:00, locks his computer and leaves the ITSAEU office.

Just after 18:00, a hacker compromises the computer of Bob, enables Remote Desktop (RDP) and creates a new (hidden) account. The hacker logs into the computer of Bob in trough the Remote Desktop with the newly created account. There is an OpenVPN icon on the Desktop with an inactive status. The hacker looks at the current configuration of the computer's *route table* to see if the computer still has an active VPN connection initiated by an administrator. The computer has an active VPN connection and has access to private networks of the airport.

A command line port scan tool called "Nmap" is uploaded to the computer. The hacker starts the scan (over the VPN connection) to search for devices. In order not to be noticed, he sets up the scanner to scan slowly. Four IP addresses where found on the airport's network and are being investigated further.

Three IP addresses have open ports that indicate web servers. One of the web servers contains a front end for a database server. This is a web application for maintenance of databases called "phpMyAdmin". The hacker uses frequently used (standard) passwords but cannot log in. The names "Bob" and "ITSAEU" are listed on the main page of the database server's web server. The hacker uses the combination of these names to log in successfully. After logging in, a database-export is made and downloaded to Bob's computer.

The hacker looks at the second web server (timetable). He uses well-known frequently used passwords[1], but they do not work. The airport is monitoring for failed login attempts in the log files. When the threshold value is exceeded, a notification is sent to the airport system administrators.

At 22:50, the airport system administrators are notified that someone is trying to log in to the dashboard of the timetable application with username "admin" but with a wrong password. The administrators look

[1] admin/admin and similar

at the web server logs of server AirtPortSys1 and the VPN server log. They find out that the incorrect login attempts are coming from the VPN connection of Bob.

Because of the late and rather unusual time for the ITSAEU administrators to log in, the administrators of the airport have been triggered that something strange is going on. Bob is trusted, but the suspected traffic goes through his VPN connection. They think his VPN connection might be compromised. The airport secures the current network log, the VPN log and the web server log for research. They also contact ITSAEU and receive relevant network logs of the ITSAEU router. ITSAEU does not find any traces on Bob's computer.

The following log files are collected:

a. routerairport_20180726_enp0s8.pcap
b. routeritsaeu_20180726_enp0s8.pcap
c. openvpn.log (VPN server of the Airport)
d. access_log (Webserver AirPortSys1 Airport)

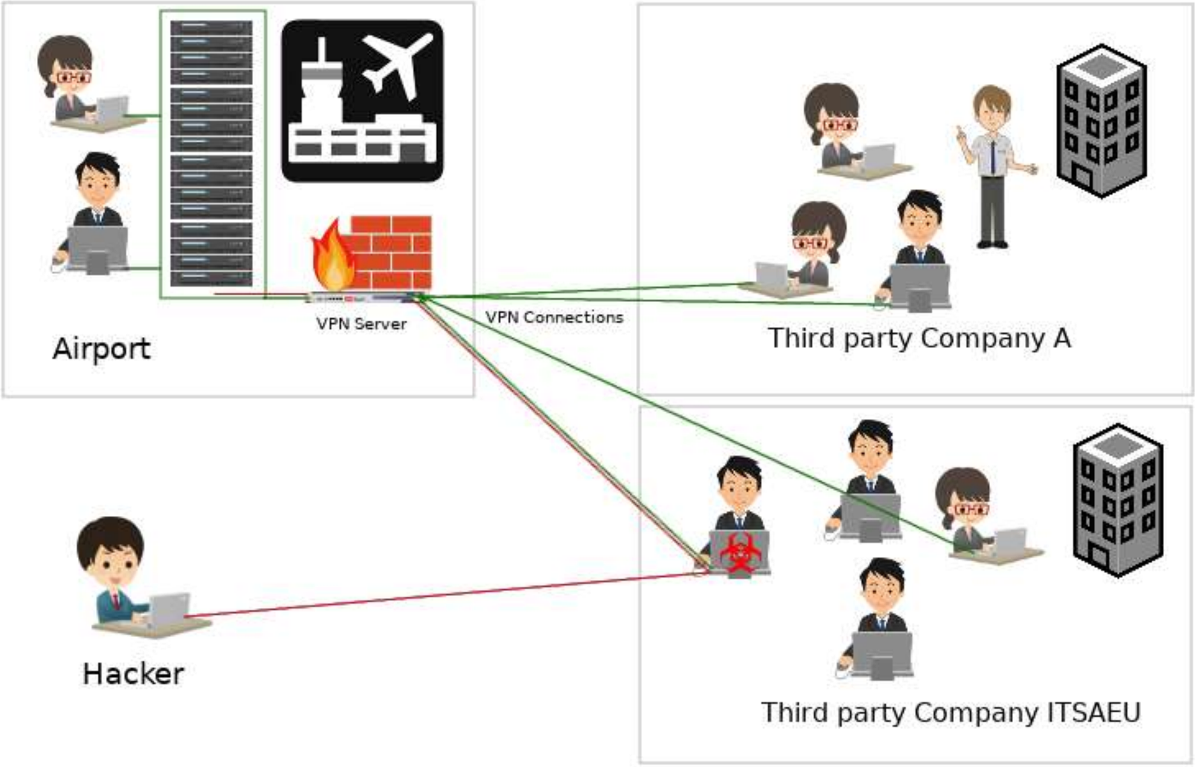


Figure 1. Graphical view of the work situation and the attack (source: images from openclipart.org)

3. Exercise Tasks

Materials

The following digital course materials are needed:

- Network documents
  - Document "5c_graphical.pdf"
  - Document "5c_Internal_network_design_student.pdf"

- Log files
  - routerairport_20180726_enp0s8.pcap
  - routeritsaeu_20180726_enp0s8.pcap
  - openvpn.log (VPN server of the Airport)
  - access_log (Webserver AirPortSys1 Airport)

Tools

The following tools will be discussed in the examination part:

- wireshark
- tcpdump
- sha256sum
- cat
- grep
- wc
- sed
- awk

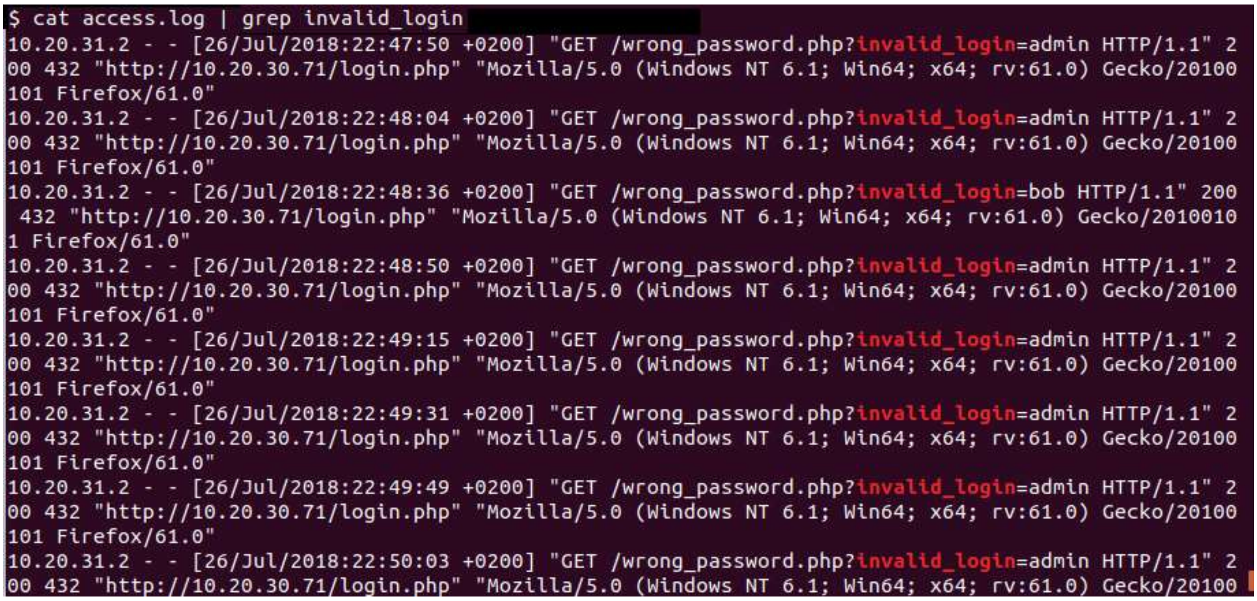
If the files are not provided and/or tools are not available, the following Virtual Image can be downloaded (no credentials needed):

https://www.enisa.europa.eu/ftp/Caine_ENISA__INF _5.3.ova

3.1 Task 1: Evidence

Webserver log

The airport administrators have been informed about the invalid login attempts of the application running on the AirPortSys1 web server. When the administrators look at the web server log, the failed login attempts are confirmed.



```
$ cat access.log | grep invalid_login [redacted]
10.20.31.2 - - [26/Jul/2018:22:47:50 +0200] "GET /wrong_password.php?invalid_login=admin HTTP/1.1" 2
00 432 "http://10.20.30.71/login.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100
101 Firefox/61.0"
10.20.31.2 - - [26/Jul/2018:22:48:04 +0200] "GET /wrong_password.php?invalid_login=admin HTTP/1.1" 2
00 432 "http://10.20.30.71/login.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100
101 Firefox/61.0"
10.20.31.2 - - [26/Jul/2018:22:48:36 +0200] "GET /wrong_password.php?invalid_login=bob HTTP/1.1" 200
 432 "http://10.20.30.71/login.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/2010010
1 Firefox/61.0"
10.20.31.2 - - [26/Jul/2018:22:48:50 +0200] "GET /wrong_password.php?invalid_login=admin HTTP/1.1" 2
00 432 "http://10.20.30.71/login.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100
101 Firefox/61.0"
10.20.31.2 - - [26/Jul/2018:22:49:15 +0200] "GET /wrong_password.php?invalid_login=admin HTTP/1.1" 2
00 432 "http://10.20.30.71/login.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100
101 Firefox/61.0"
10.20.31.2 - - [26/Jul/2018:22:49:31 +0200] "GET /wrong_password.php?invalid_login=admin HTTP/1.1" 2
00 432 "http://10.20.30.71/login.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100
101 Firefox/61.0"
10.20.31.2 - - [26/Jul/2018:22:49:49 +0200] "GET /wrong_password.php?invalid_login=admin HTTP/1.1" 2
00 432 "http://10.20.30.71/login.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100
101 Firefox/61.0"
10.20.31.2 - - [26/Jul/2018:22:50:03 +0200] "GET /wrong_password.php?invalid_login=admin HTTP/1.1" 2
00 432 "http://10.20.30.71/login.php" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100
```

Figure 2. Screenshot the invalid logins from the webserver log of AirportSys1 (source: screenshot created by ENISA)

Hash values of the log files reported in the Chain of Custody form

The researchers at the airport also keep a Chain of Custody form. The calculated hash values of the log files are *noted* as the following values:

```
6f33beb68e3641b0c9b1866c7b5821c8142634f2ba7ede0fc73c45504ecef5a9  access.log
e65cd8c0d80da7dadc4c17f80d20cc8d51c064b2ed3e064b9edbc4ec688f7eea  openvpn.log
4b80c6ebc3b229eabe6617cbf5662da83a7fbcfe0dc35a2c415cf467ab291706  routerairport_20180726_enp0s8.pcap
3c8b8d5c68dbb9fe7ba196fccc11ee82e693646620183cfb4639bd11447ef836  routeritsaeu_20180726_enp0s8.pcap
```

Table: hash values form the Chain of Custody form

Logfiles openvpn.log and access_log

In TASK 1, the students will use the openvpn.log log file from the VPN server and log access_log from the AirportSys1 Apache web server. To give the students a visual impression of the location of the log files in the network, a piece of network drawing has been added.

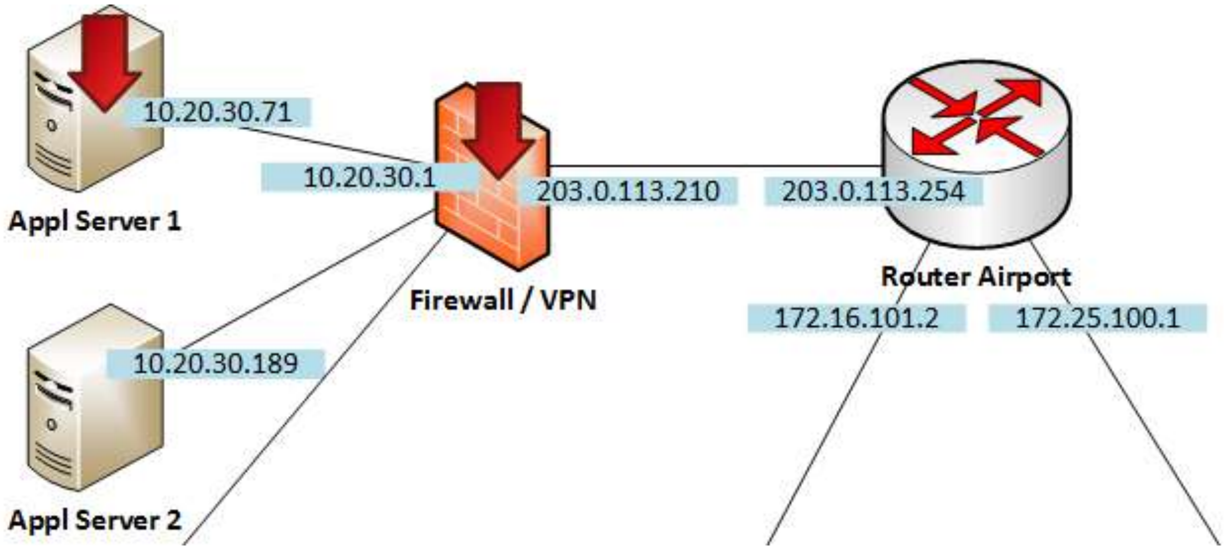


Figure 3. Location of log files openvpn.log and access_log in the network setup (source: image created by ENISA)

Student

Examine the *openvpn.log* and *access_log* file in relation to above piece of network drawing.

a) Use command line tools, based on the access_log, how many times was tried to login with the username "admin"?
b) What can be said about the integrity of the log files?
c) Based on the openvpn.log, what is the IP address of Bob's computer?

3.2 Task 2: Examine the network setup

Getting stared

The students need the file 5c_Internal_network_design_student.pdf. The image of the document is shown below and shows the IP addresses known by the airport administrators.

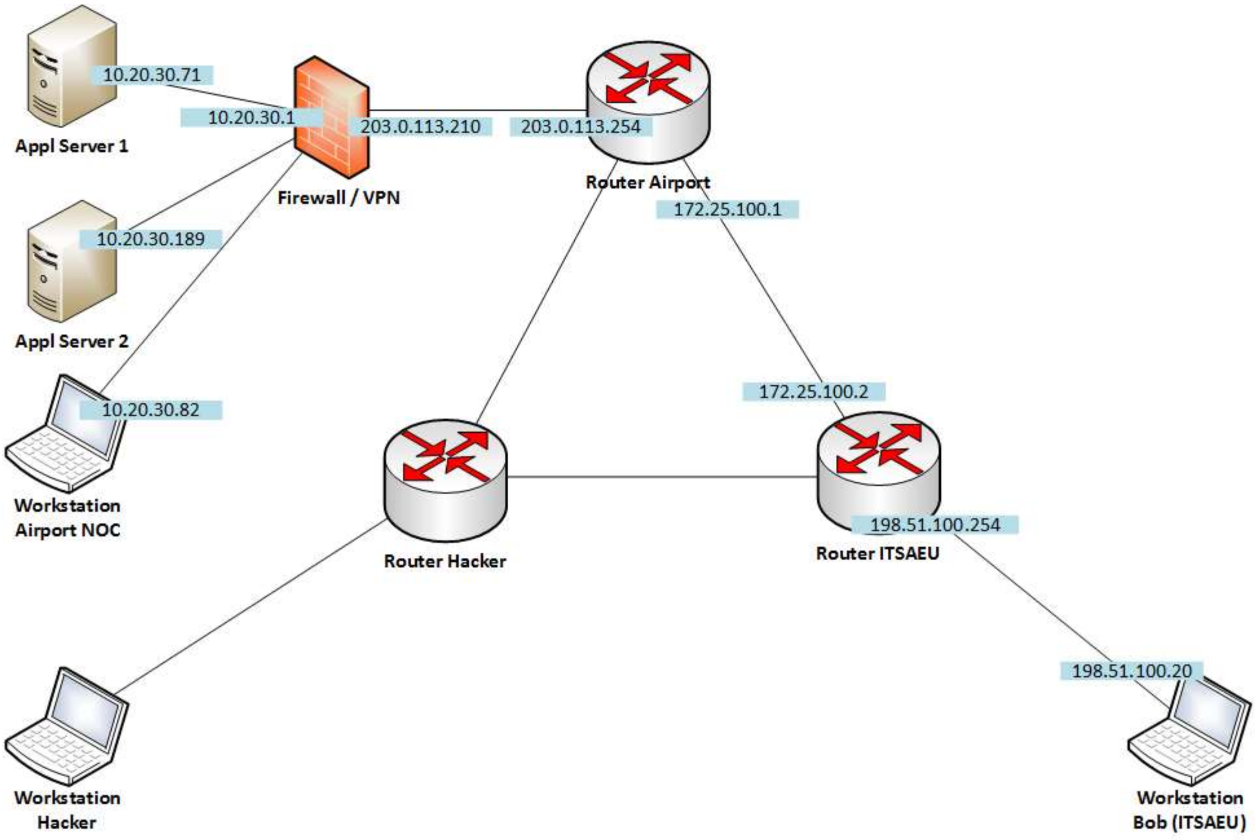


Figure 4. The setup of the internal network (source: image created by ENISA)

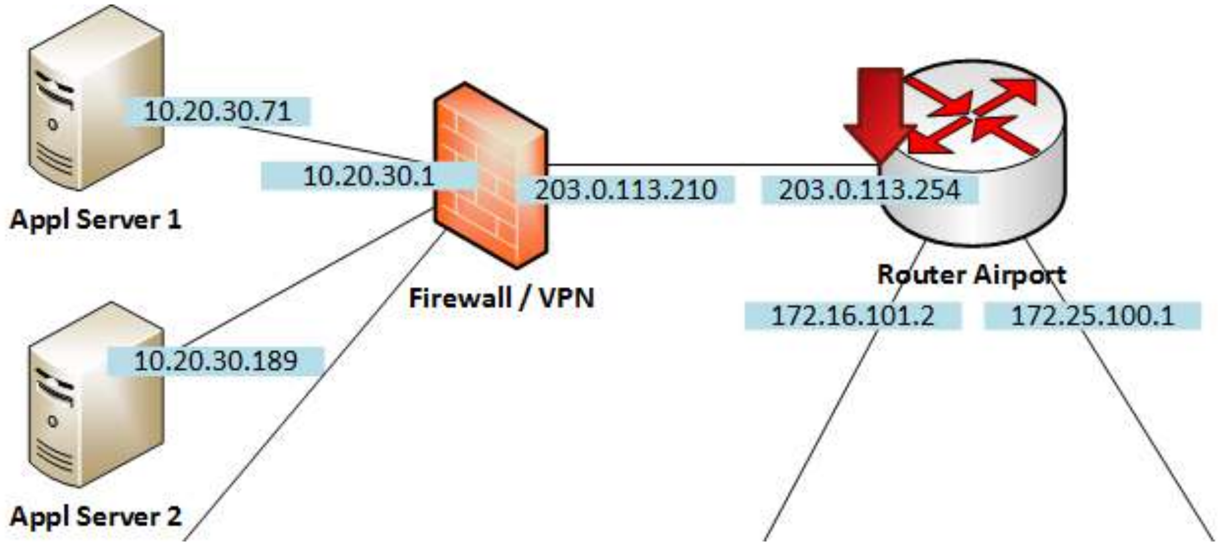


Figure 5. Network Location of log file routerairport_20180726_enp0s8.pcap in the network setup (source: image created by ENISA)

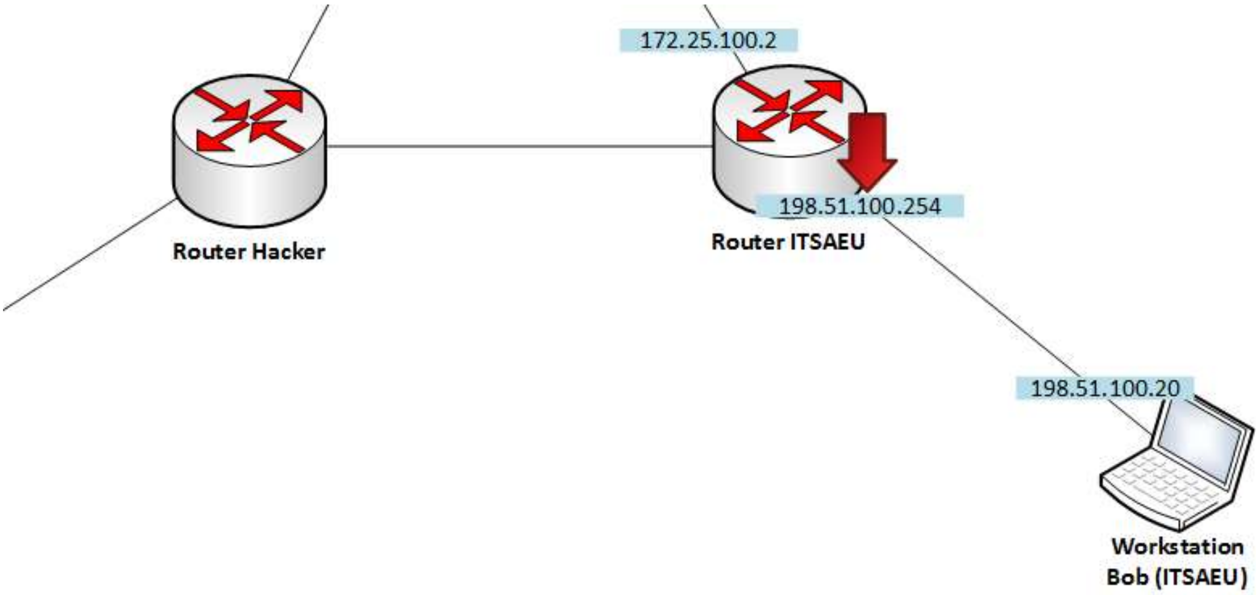


Figure 6. Location of the capture log file routeritsaeu_20180726_enp0s8.pcap in the network setup (source: image created by ENISA)

Student

Examine the two network documents in combination with the history of the attack.

a) What can you say about the following IP addresses that are used in this example? Are they public? Are they routable?
   a. 10.20.30.71
   b. 172.25.100.2
   c. 198.51.100.20
   d. 203.0.113.210

3.3 Task 3: Examine the router log files

In this task, the students will investigate the router logs.

Getting stared
The student needs the following network dump files for this task:

- routerairport_20180726_enp0s8.pcap
- routeritsaeu_20180726_enp0s8.pcap

Student
Use only the log files routerairport_20180726_enp0s8.pcap and routeritsaeu_20180726_enp0s8.pcap

a) When was the VPN connection started?
b) Which IP addresses have many connections with Bob's machine?
c) Assume Bob's computer is compromised, what is most likely the IP address of the hacker?
d) Examine the traffic of the hacker's IP address in relation to the IP address of Bob's computer and locate the attack
e) Follow the TCP stream of the attack in Wireshark
f) What can be said about the readability of the network activity during the VPN connection?
g) Convert the routeritsaeu_20180726_enp0s8.pcap to ASCII
h) Create a timeline of the incident based on the available log files

Bonus question (time-dependent):

i) Select output form ASCII output routeritsaeu_20180726_enp0s8.pcap
While using the output of the ASCII conversion of routeritsaeu_20180726_enp0s8.pcap.
Use cat/grep/sed/awk to generate a list of

- All lines that belong to the Openvpn connection based on port number or replacement service
- <time [hh:mm:ss]> <src-ip.src-port> <direction> <dst-ip.dst-port>
- Remove last colon after dst-port

e.g.

```
16:36:18 198.51.100.20.1048 > 203.0.113.210.openvpn
16:36:18 203.0.113.210.openvpn > 198.51.100.20.1048
```

3.4 Task 4: Examine the attack

Getting stared
The student needs the following network dump files for this task:

- routerairport_20180726_enp0s8.pcap
- routeritsaeu_20180726_enp0s8.pcap

Student

a. Based on the information in the log files, which attack is probably used?

b. What technique is used by the hacker to bypass firewall restrictions on open ports?

3.5 Tools used in this use-case

- http://www.tcpdump.org/ (last accessed on July 31th 2018)
- https://www.wireshark.org/ (last accessed on July 31th 2018)
- https://www.kali.org (last accessed on July 31th 2018)
- https://www.pfsense.org/ (last accessed on July 31th 2018)
- https://openvpn.net/ (last accessed on July 31th 2018)

4. Glossary

ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
C&C	Command and Control (Server)
CLI	Command Line Interfaces
COTP	Connection Oriented Transport Protocol
GUI	Graphical User Interface
ICS	Industrial Control Systems
IGMP	Internet Group Management Protocol
ISO 27001	International Organization for Standardization
LLDP	Link Local Discovery Protocol
LLMNR	Link Local Multicast Name Resolution
PCAP	Packet CAPture
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SMB	Server Message Block
SSDP	Simple Service Discovery Protocol
TCP	Transmission Control Protocol
TPKT	Packet format used to transport OSI TPDUs over TCP
TPDU	(OSI) Transport Protocol Data Uni
UDP	User Datagram Protocol
VNC	Virtual Network Computing

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-288-2
DOI: 10.2824/995110