Research on Simulating the Volume of Industrial Traffic Control System Using Standard Communication Protocols

Vasile Florin POPESCU, Tiberiu ION
CAROL I National Defence University of Bucharest, Faculty of Security and Defense
popescu.vflorin@unap.ro, ion.tiberiu@unap.ro

Victor GÂNSAC, Marius Emil PÂRVU, Sorin PISTOL, Olivia COMȘA
SAFETECH Innovation
victor.gansac@safetech.ro, marius.parvu@safetech.ro,
pistolsorin@icloud.com, olivia.comsa@safetech.ro

Abstract: This paper aims to analyze, simulate and test the control of industrial traffic by using existing standard communication protocols in order to be able to respond to cyber security incidents and to implement new services and innovative processes. This study with practical results is part of the research carried out within the project "Center of Excellence for Cyber Security and Critical Infrastructure Resilience - SafePIC, funded under the Operational Program Competitiveness 2014-2020.

Keywords: Industrial, Cyber, Applications, Interface, Virtual Machines, Uplink, Sniffers

INTRODUCTION

In Europe and, implicitly, in Romania, the responsibility regarding industrial cyber security is not very clearly delimited conceptually and practically. But what is very clear, is the need to prepare and certify an entire chain of actors that must add value to the concept of industrial cyber security. (Popescu & Comsa, 2021).

Industrial traffic simulation can be done in several ways. Firstly, by resubmitting previously captured and recorded packets. These packages can come from either a real source or a simulation. Secondly, by generating packages using specialized applications. In the case of the present paper, as a result of the research carried out within the SAFEPic 19 project, previously registered Ethernet packets (also called "frames") were used. These packages, which simulate a data transaction between industrial equipment, were generated using the Ixia Breaking Point application. The role of the application is to simulate the traffic of a network of computers and / or industrial equipment. The „tcpreplay" utility was used for resubmission. Security Onion server has been used on the network to receive a copy of the packets passing through the network for analysis.

http://doi.org/10.54851/v4i1y202205

Network sniffers or analyzers can also be used on a LAN or Wi-Fi network. The main difference is that if this is used in a LAN, we will have access to the packages of any connected equipment. You can also set a limitation based on the network device, when used in a wireless network, situation in which the network analyzer can only scan one channel at a time for the network limiter, in case of using multiple wireless interfaces. When we track packets using a Sniffer or a network analyzer, we can access details such as:

- Information about the sites visited;
- Content and recipient of e-mails sent and received;
- View downloaded files and many other details.

The main objective of a Sniffer is to analyze all packets in the network, especially incoming traffic, to look for any object whose content integrates malicious code and thus increase security in the organization by preventing any installation of a malware on any computer of a client. Knowing a little about how the network analyzer works, we'll get to know some of the best network analyzers or Sniffers available for Windows and Linux.

NECESSARY STEPS TO CONFIGURE THE VIRTUAL NETWORK TO CAPTURE SIMULATED TRAFFIC

The network should be configured promiscuously to route traffic to the analysis server (Security Onion) as well. In this way, packets destined for a certain address / port will also be sent to the other ports of the virtual switch.

In the ESXi interface (Seaton, 2021) click the networking menu, then the Virtual switches tab, and click the Add standard virtual switch button. Disable the uplink section and check that the security options are passed from Reject to Accept. Security settings allow packets to be routed to all ports as well as resend packets with MAC addresses other than those marked in the address table.

Under the same menu, the Port groups tab, click the Add Port Group button. It is called the new port group, a dedicated VLAN ID and the virtual switch. Security settings can be inherited from the switch.

In the Virtual Machines menu, select the source server, click the Edit Settings button in the context menu where a new network card connected to the port group configured above is added.

SIMULATION AND TESTING

Simulations and tests using the tcpreplay utility

Tcpreplay utility resends a set of previously captured packets from a communication medium. This utility can change the source or destination addresses, it can vary the time between two sent packets, it can send the source-destination traffic on a different network card than the destination-source traffic. The flexibility of the utility is especially helpful for testing IDS systems. The source used by tcpreplay is a packet capture in pcap format. This format is generated by the Pcap library - Packet Capture Library (Keary, 2021). Data contained in the pcap file can be viewed with a variety of applications, for example tcpdump and Wireshark.

If at any time you have tried to perform certain network scans no doubt you have seen or been recommended WireShark as one of the best solutions. The reason is simple, WireShark has positioned itself as one of the most used network protocol analyzers for millions of people around the world not only because of its ease of use, but also because of its integrated features. Among its features we highlight the following:

- It can run smoothly on systems such as Windows, Linux, macOS, Solaris, FreeBSD, NetBSD and others;
- It integrates powerful analysis for VoIP.
- You can perform an in-depth inspection of more than 100 protocols;
- You can perform live capture and offline analysis of network packets;
- It is compatible with read and write

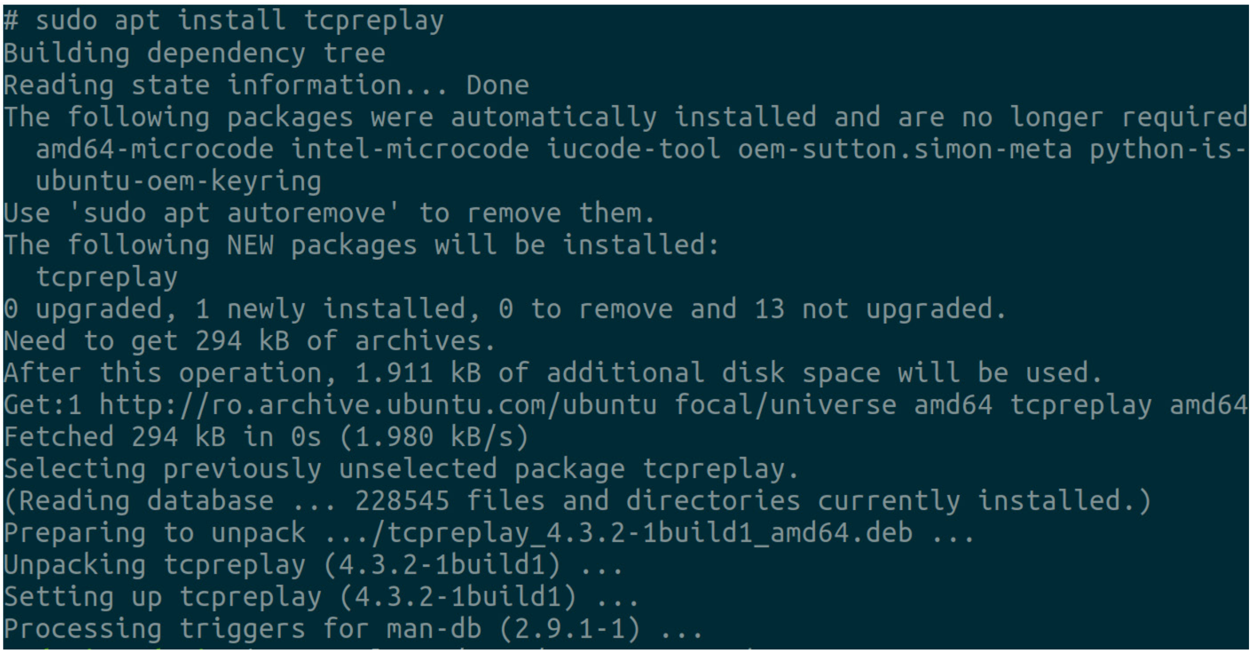
formats such as tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN / LAN Analyzer, Shomiti / Finisar Surveyor, Tektronix K12xx, Visual Networks Time Up Visual, WildPackets EtherPeek / TokenPeek / AiroPeek and many more.;

- Data that is captured live can be read from platforms such as Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, which give us a wide range of access possibilities;
- Network data that is captured can be explored using a graphical interface (GUI) or TShark in TTY mode;
- It supports to decrypt multiple protocols such as IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP and WPA / WPA2;
- We can implement color rules for better management of the obtained data;
- Results can be exported to XML, PostScript®, CSV or plain text (CSV).

Example of viewing the pcap file in the Wireshark application (https://www.wireshark.org)

Step 1: Install the tcpreplay utility from the default application registry (if it doesn't exist it can be compiled from the source code)

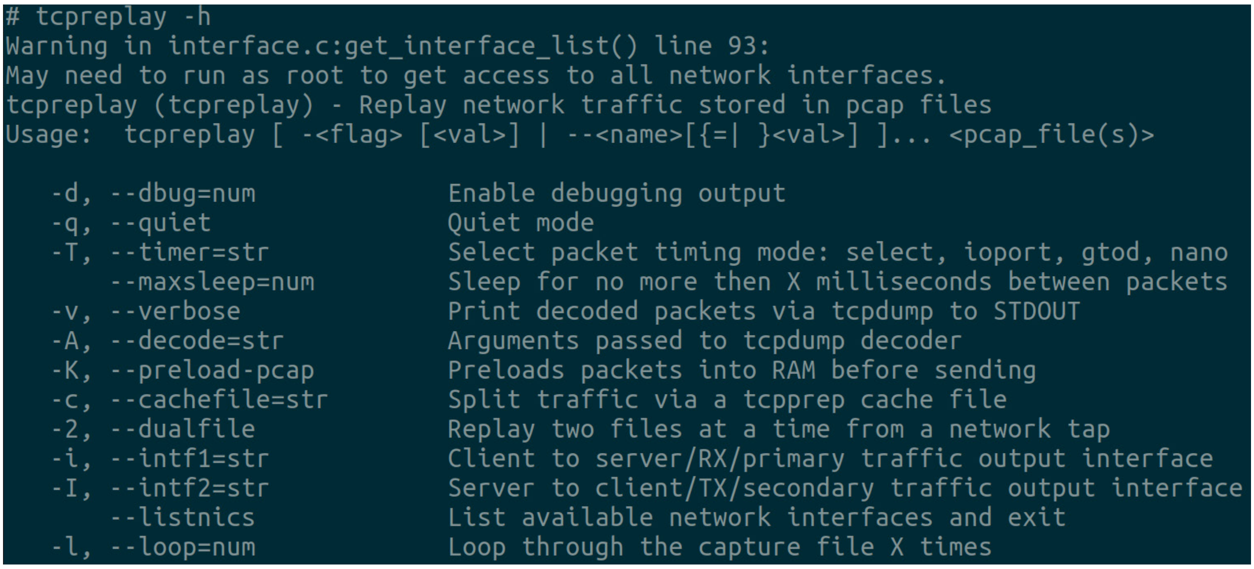
# apt install tcpreplay



```
# sudo apt install tcpreplay
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required
  amd64-microcode intel-microcode iucode-tool oem-sutton.simon-meta python-is-
  ubuntu-oem-keyring
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  tcpreplay
0 upgraded, 1 newly installed, 0 to remove and 13 not upgraded.
Need to get 294 kB of archives.
After this operation, 1.911 kB of additional disk space will be used.
Get:1 http://ro.archive.ubuntu.com/ubuntu focal/universe amd64 tcpreplay amd64
Fetched 294 kB in 0s (1.980 kB/s)
Selecting previously unselected package tcpreplay.
(Reading database ... 228545 files and directories currently installed.)
Preparing to unpack .../tcpreplay_4.3.2-1build1_amd64.deb ...
Unpacking tcpreplay (4.3.2-1build1) ...
Setting up tcpreplay (4.3.2-1build1) ...
Processing triggers for man-db (2.9.1-1) ...
```

***Fig.1**: Printscreen apt install tcpreplay*

Step 2: Running the utility with the -h argument for visibility into options



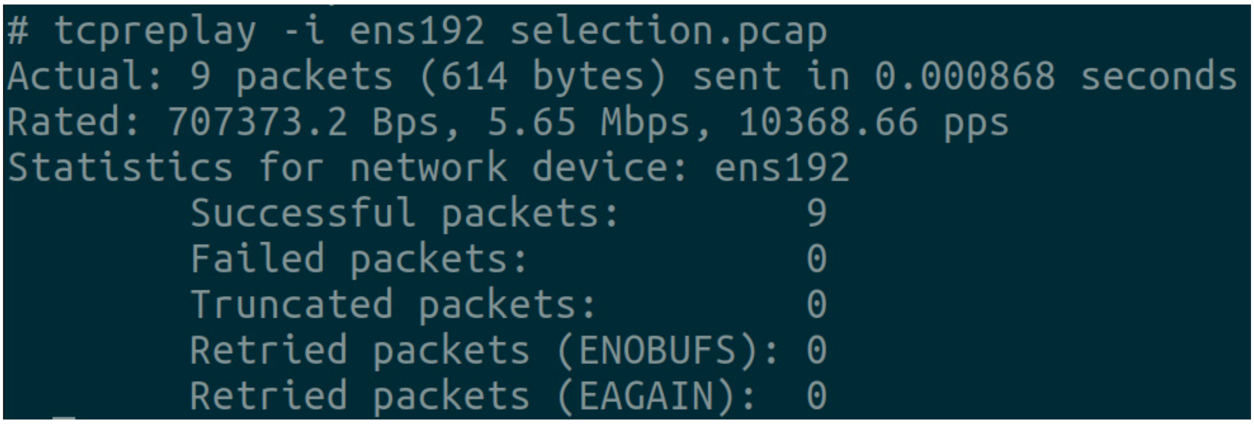
```
# tcpreplay -h
Warning in interface.c:get_interface_list() line 93:
May need to run as root to get access to all network interfaces.
tcpreplay (tcpreplay) - Replay network traffic stored in pcap files
Usage:  tcpreplay [ -<flag> [<val>] | --<name>[{=| }<val>] ]... <pcap_file(s)>

   -d, --dbug=num              Enable debugging output
   -q, --quiet                 Quiet mode
   -T, --timer=str             Select packet timing mode: select, ioport, gtod, nano
       --maxsleep=num          Sleep for no more then X milliseconds between packets
   -v, --verbose               Print decoded packets via tcpdump to STDOUT
   -A, --decode=str            Arguments passed to tcpdump decoder
   -K, --preload-pcap          Preloads packets into RAM before sending
   -c, --cachefile=str         Split traffic via a tcpprep cache file
   -2, --dualfile              Replay two files at a time from a network tap
   -i, --intf1=str             Client to server/RX/primary traffic output interface
   -I, --intf2=str             Server to client/TX/secondary traffic output interface
       --listnics              List available network interfaces and exit
   -l, --loop=num              Loop through the capture file X times
```

***Fig.2**: Running the utility with the -h argument for visibility into options*

Step 3: The utility is running specifying the file with the saved packages

# tcpreplay -i ens192 selection.pcap



```
# tcpreplay -i ens192 selection.pcap
Actual: 9 packets (614 bytes) sent in 0.000868 seconds
Rated: 707373.2 Bps, 5.65 Mbps, 10368.66 pps
Statistics for network device: ens192
        Successful packets:        9
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

***Fig.3**: Printscreen - saved packages*

Testing traffic capture on the Security Onion server <https://securityonionsolutions.com/software/>

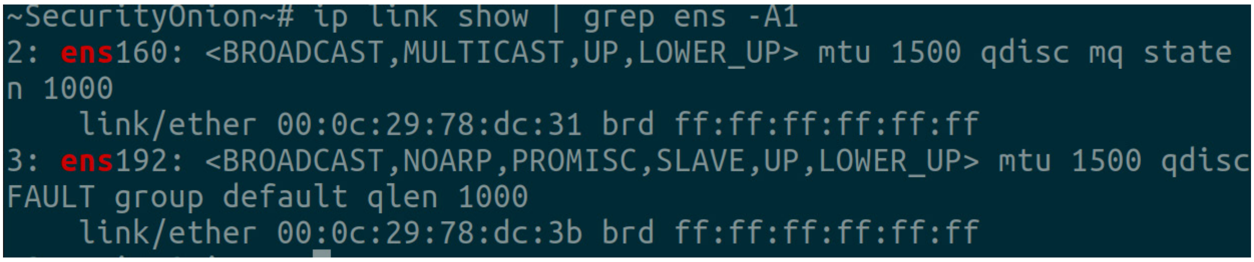
The Security Onion monitoring platform interprets the captured traffic and assimilates it in a form that can be easily interpreted by a security researcher. Security Onion is installed and configured stand-alone. All components are on a single virtual machine, with the possibility of a distributed installation depending on the level of traffic to be analyzed.

The Security Onion solution is built on a distributed client-server model. In the past, Security Onion relied solely on the use of a „sensor" (client) and a „server" such as the Security Onion server. Recently, with the inclusion of Elastic Stack (the suite of Elastic Search, Logstash and Kibana), the distributed architecture has changed and now includes the use of Elastic components and separate nodes for processing and storing data from the Elastic Stack. From an architectural point of view, for complex infrastructures and with very large volumes of data, Security Onion recommends multiple nodes for data collection and storage.

Tcpdump, a traffic capture and visualization utility, can be used to verify the successful routing of packets to the Security Onion monitoring platform.

Verification of interfaces on the Security Onion monitoring platform:

# ip link show | grep ens -A1

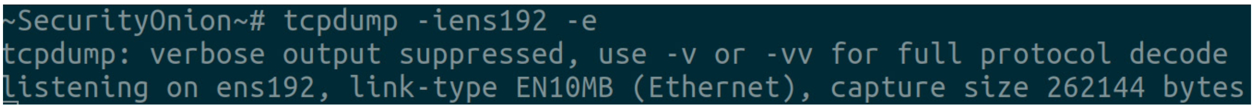


```
~SecurityOnion~# ip link show | grep ens -A1
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state
n 1000
    link/ether 00:0c:29:78:dc:31 brd ff:ff:ff:ff:ff:ff
3: ens192: <BROADCAST,NOARP,PROMISC,SLAVE,UP,LOWER_UP> mtu 1500 qdisc
FAULT group default qlen 1000
    link/ether 00:0c:29:78:dc:3b brd ff:ff:ff:ff:ff:ff
```

***Fig.4**: Printscreen - interfaces verification*

Launch the tcpdump utility on the Security Onion monitoring platform to view the received traffic. The arguments used are: -i - specifies the listening interface, -e - specifies the display of frame headers.

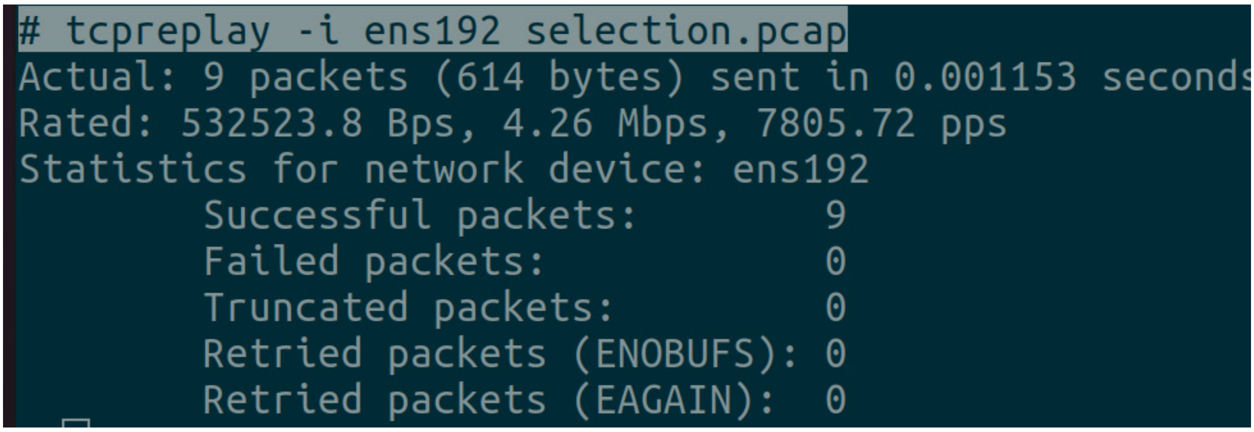
# tcpdump -iens192 -e



```
~SecurityOnion~# tcpdump -iens192 -e
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens192, link-type EN10MB (Ethernet), capture size 262144 bytes
```

***Fig.5**: Printscreen - sending packets with the tcpreplay utility from the source server*

# tcpreplay -i ens192 selection.pcap



```
# tcpreplay -i ens192 selection.pcap
Actual: 9 packets (614 bytes) sent in 0.001153 seconds
Rated: 532523.8 Bps, 4.26 Mbps, 7805.72 pps
Statistics for network device: ens192
        Successful packets:        9
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

***Fig.6**: Printscreen - confirm receipt of packets on the monitoring server*

CONCLUSIONS

Industrial traffic represents indeed a huge web network of protocols, services and infrastructure that allows the network connection to be taken everywhere and more than 90% of us have heard of TCP / IP, HTTP, SMTP, etc. These are all protocols that play a key role in how the network reaches your computer or device, but behind it are routers and other components that, if they fail, two things can happe: you lose access to the network, or you are susceptible to an attack. That's why network and network product developers have worked hard to create applications known as Sniffers and Network Analyzers, and while they are generally very technical, the truth is that they are valuable tools for determining if a communication sniffer or a network analyzer is a hardware or software utility that has been developed for the purpose of generating constant monitoring of local or external network traffic. This tracking is practically responsible for analyzing the packet data flows that are sent and received between the network equipment, either internally or externally. It uses a tracking mode called „promiscuous mode" which allows us to examine all packets regardless of their destination. This can take time, but it is essential to know for sure that it passes through our network.

ACKNOWLEDGMENTS

This paper was published as part of the project „Center of Excellence for Cyber Security and Critical Infrastructure Resilience (SafePIC)", Contract No. 270 / 23.06.2020, ID 120436, funded under the Operational Program Competitiveness 2014-2020, Priority Axis: 1. Research, Technological Development and Innovation (RDI) to support economic competitiveness and business development.

REFERENCE LIST

Keary, T. (2021). PCAP: Packet Capture, what it is & what you need to know. Available at <https://www.comparitech.com/net-admin/pcap-guide/>.

Popescu, Fl. & Comșa, Ol. (2021).

Seaton, J. (2021). What Does VMware ESXi Server Mean?. Available at <https://www.techopedia.com/definition/25979/vmware-esxi-server>.

<https://www.wireshark.org>

<https://securityonionsolutions.com/software/:>