ARL-TR-8884 ● JAN 2020

Hands-on Cybersecurity Studies: Network Routing Analysis

by Jaime C Acosta

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when no longer needed. Do not return to the originator.

ARL-TR-8884 ● JAN 2020

Hands-on Cybersecurity Studies: Network Routing Analysis

Jaime C Acosta
Computational and Information Sciences Directorate,
CCDC Army Research Laboratory

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
January 2020	Technical Report	June–December 2019

4. TITLE AND SUBTITLE
Hands-on Cybersecurity Studies: Network Routing Analysis

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Jaime C Acosta

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
CCDC Army Research Laboratory
ATTN: FCDD-RLC-ND
Adelphi, MD 20783-1138

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-8884

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Devices communicate across networks seemingly instantaneously across the world, and underlying this communication are complex software and hardware infrastructures that attempt to optimize the digital pathways. Network routers, switches, and firewalls make up the hardware, and software such as the Routing Information Protocol (RIP), Open Shortest Path First, and Border Gateway Protocol implement the necessary logic required to compute optimal paths. This report is part of a hands-on cybersecurity studies series. Provided is a hands-on exercise that starts by demonstrating RIP and describing some of the dangers that may arise when the service is misconfigured. Then a listing of mitigations are discussed.

15. SUBJECT TERMS
network, Routing Information Protocol, RIP, hands-on cybersecurity, CyberRIG, tactical communication

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Jaime C Acosta
Unclassified	Unclassified	Unclassified	UU	19	19b. TELEPHONE NUMBER (Include area code) (575) 993-2375

Contents

List of Figures

1. Introduction

Devices communicate across networks seemingly instantaneously across the world, and underlying this communication are complex software and hardware infrastructures that attempt to optimize the digital pathways. Network routers, switches, and firewalls make up the hardware and software, such as the Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP), which implement the necessary logic required to compute optimal paths.

These routing protocols, however, are not without weaknesses. In many cases, human error and misconfigurations can lead to devastating impacts on the security and privacy of the information carried across a network. These types of weaknesses can lead to route leaks or route hijacks in which traffic is sent through unintended channels, possibly endangering the confidentiality, integrity, and availability of information. Even more devastating is the fact that these weaknesses are difficult to detect, many lasting several week, and they affect a large pool. Recent high-profile incidents ranged from thousands to hundreds of thousands of device addresses, and they are intercontinental, crossing over many countries that have their own set of rules, regulations, and policies.

Several of these types of incidents have occurred since the inception of the Internet. The following incidents are just a few of many that have been identified and reported by analysts across the globe. In 1997, a major disruption in connectivity was observed due to the Florida Internet Exchange accidentally misdirecting roughly 50,000 device addresses, resulting in several hours of nonaccess for Internet Service Providers.[1] In 2010, route leaks led to roughly 37,000 unique network prefixes being mistakenly routed through China.[2] In 2014, leaks led to prefixes including those belonging to the US Department of Defense, YouTube, Time Warner, among others, being sent accidentally through Syria and Indonesia.[3] More recently, in December 2017, 80 prefixes including those used by Google, Facebook, and Apple were unintentionally routed through Russia.[4]

From the end-user's perspective (e.g., someone navigating the Internet using a browser), these misconfigurations are, for the most part, undetectable. For this reason and for the reasons already mentioned, it is critical that users understand ways to protect themselves and their data.

These incidents may also occur in similar ways on smaller networks, including local- and wide-area networks. A common theme is that these incidents occur from of a lack of awareness and training for both network engineers and end-users alike.

The rest of this report describes the setup of the exercise, including the public resources and tools that were used to configure it. Next the main learning objectives and annotated exercise steps are provided. The report concludes with a summary of the activities that make up the exercise as well as conclusions.

2. Setup and Configuration

The following setup, configuration, and analysis is loosely based on Vamsi Kambhampati and Dr Daniel Massey's computer security assignment.[5] The exercise described in this document runs on the US Army Combat Capabilities Development Command Army Research Laboratory–South's (ARL-South's) Collaborative Innovation Testbed (CIT), which allows remote participants to partake in the activity using a sandbox environment. In this sandbox, every participant is provided an isolated network consisting of nodes, switches, routers, and software services. Additionally, through the Evaluator Centric and Extensible Logger Daemon,[6] analysts are able to collect data associated with the actions completed during the exercise. The sandbox environment for the hands-on exercise consists of the following:

- Ubuntu 16 LTS 64-bit
- VirtualBox 6.0 64-bit
- Common Open Research Emulator (CORE) version 4.7, 64-bit virtual machine
- Kali Linux 2019.2 64-bit virtual machine
- Loki route testing software4
- Apache2 Hypertext Transfer Protocol Server version 2.4.6, 64-bit software
- Python Web client script

As shown in Fig. 1, several servers are running the Ubuntu operating system. The hands-on exercise is composed of two VirtualBox virtual machines: the participant machine, running the Kali Linux, and the network topology machine that runs all of the nodes and services that make up the sandbox network. Participants complete the exercise by interacting directly with only the interface of the participant machine (i.e., they never visually see the network topology machine). Aside from the Loki route testing software, no other software is installed on the Kali Linux virtual machine. The CORE virtual machine comes preinstalled with the Quagga quagga-mr_0.99.21mr2.2 routing software. RIP is used for this exercise.

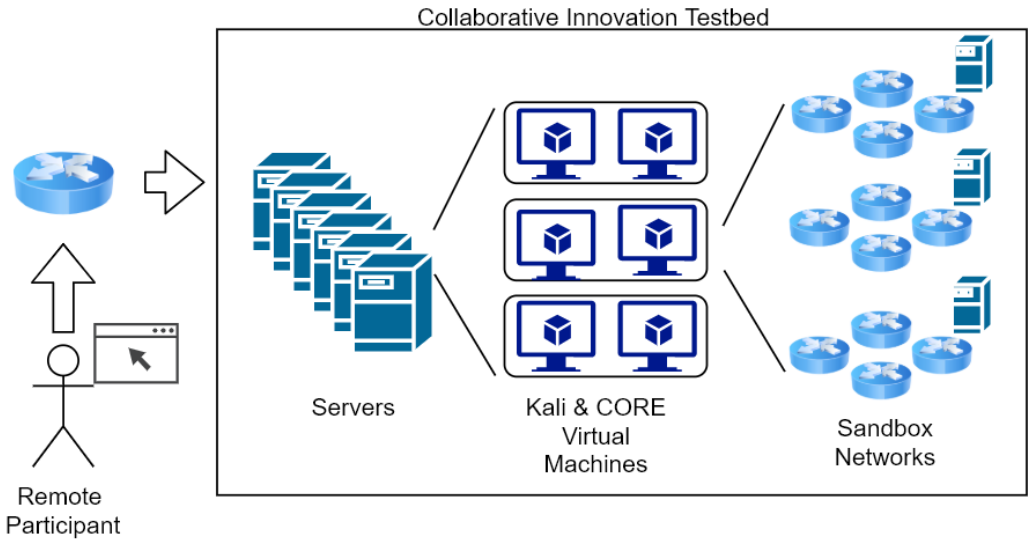

Fig. 1 Accessing the exercise through the CIT

To exhibit Web traffic, the Apache2 Web server software is installed and configured to run within one of the nodes in the network sandbox. In addition, a simple client script that continually requests a Web page runs on a different node within the sandbox. The script checks whether a valid Web page is returned. If so, the script will proceed to send credentials over the network in clear text.

The CORE scenario and all of the services required for the scenario to work correctly are started when the virtual machines boot. At this time, a snapshot of the virtual machines is taken and then the ARL-South CIT generator (CIT-gen) is used to create clones of the virtual machines. The clones are created in such a way to preserve the participant's environments. Last, the CIT-gen is used to create users and allow access from remote locations.

3. Learning Objectives

The exercise described in the next section demonstrates the potential dangers and impacts of misconfigured routing protocols. The exercise was developed with a learning aspect in mind, both for high-level cybersecurity awareness and technical analysis. The following are the targeted cybersecurity awareness learning objectives:

- Do not use old and out-of-date software. This is especially true for services with critical roles in the network or host system. RIPv1 was originally designed without security in place; no authentication is required to become a trusted routing entity. Both RIPv1 and RIPv2 are known to have several other weaknesses.

- Ensure personnel are trained on the technologies and systems used to manage the network. A misconfigured routing protocol could result in route leaks or route hijacks, which in turn could compromise the three security objectives: confidentiality, integrity, and availability.
- Practice defense in depth. Security-weak routing may allow unintended audiences to view data. However, if other security measures are in place (e.g., encrypting multiple layers in the network stack could still protect against unauthorized access), the data may be unreadable.

The following are the targeted technical analysis learning objectives:

- Basic networking in Linux. Learn how to assign an address to a network interface by first studying the subnetwork number on which participants reside.
- Learn how network packets are routed across a wide area network. This is accomplished by generating traffic and then studying the RIP packets as they appear in the Wireshark tool.
- Understand techniques that can be used to mitigate weaknesses that may arise from misconfigured routing.

4. Exercise

The exercise is composed of four separate parts. In the first part, participants are asked to observe the network environment to identify an address that is available and valid. They then proceed to connect to the simulated network. Third, participants use the Loki tool to become a trusted node in the network. Finally, participants analyze the traffic to uncover additional issues in the network. The exercise requires roughly 1–1.5 h to complete.

4.1 Activity 1: Observe the Network Environment

In this exercise, you are positioned in a network, as shown in Fig. 2. To start, login to the Kali system.

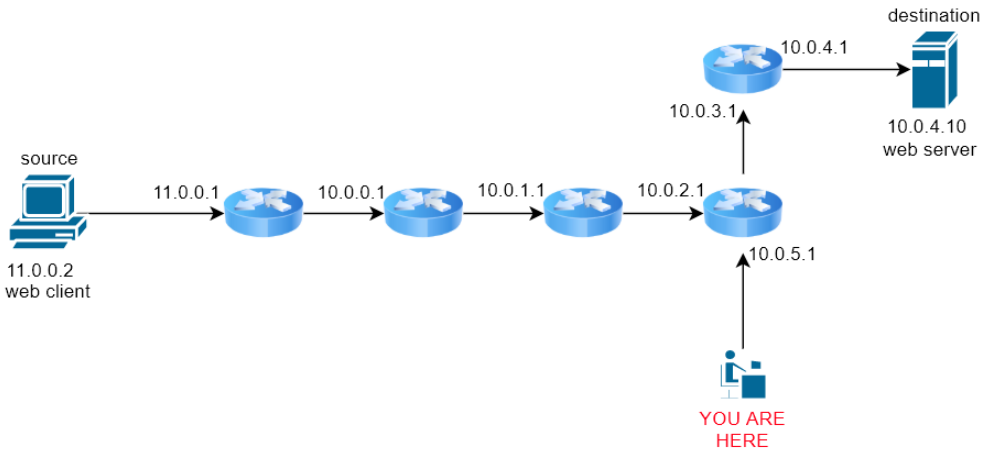

Fig. 2 Network sandbox environment

1. Start a new terminal by clicking on the terminal icon on the left side of the screen  .

2. Bring up the eth0 network interface and start Wireshark (a network sniffer) by typing the following commands in the terminal window:

   ifconfig eth0 up
   wireshark &

3. Click OK on the error window that pops up.

4. In the Wireshark window, double-click the eth0 interface label, as shown in Fig. 3.

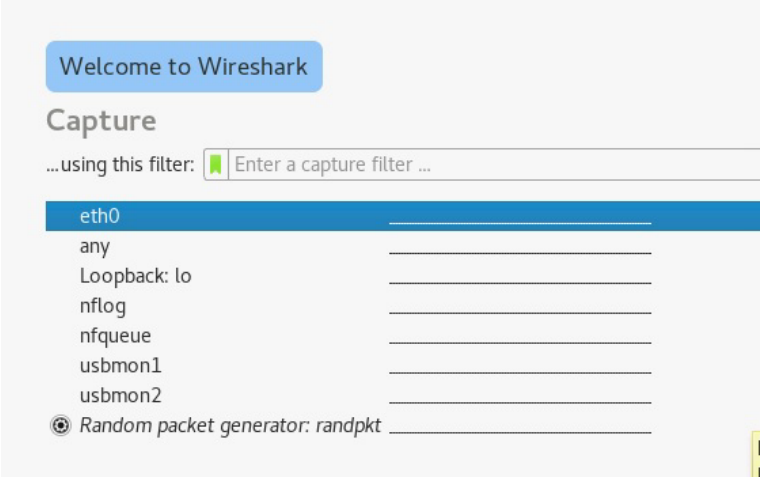

Fig. 3 Wireshark startup interface

5. After the main Wireshark interface pops up, wait a few seconds and you will begin seeing entries appear in the packet list pane, as shown in Fig. 4.

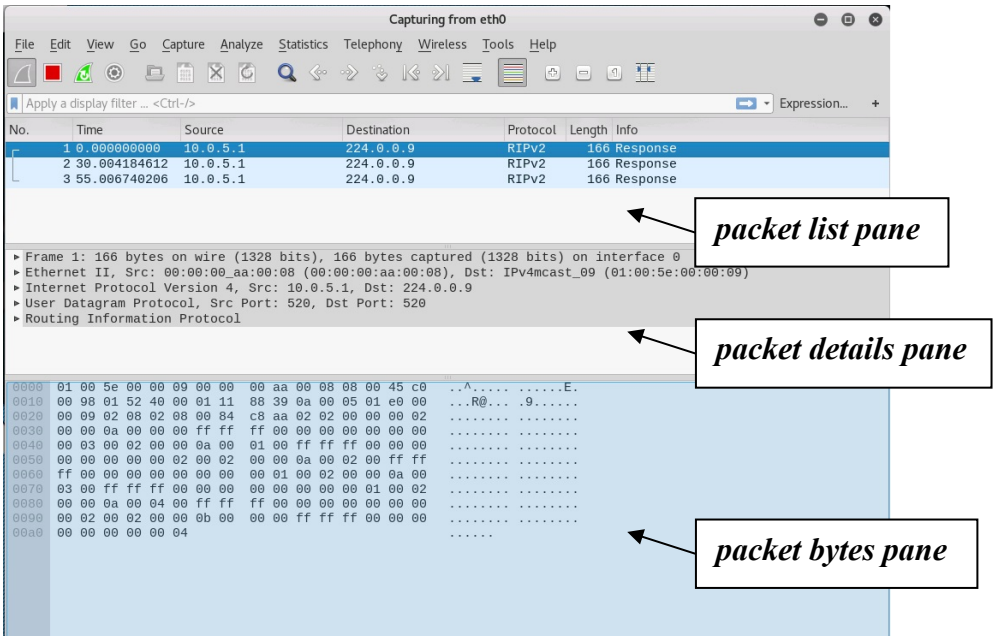

Fig. 4 Wireshark packet capture interface

6. Click on a packet and look in the packet list pane to fill in the following information:

   a. The IP address of the device that sent the packet:

   _____

   b. The IP address of the intended recipient: _____

   c. The type of the packet (protocol): _____

7. Use the packet details pane to find and fill in the following information:

   a. List the reachable networks:

   1. _____
   2. _____
   3. _____
   4. _____
   5. _____
   6. _____

b. What does the value in the metric field represent? (Hint: See Fig. 2)

For the rest of this workshop, do NOT close the Wireshark window.

4.2 Activity 2: Connecting to the Simulated Network

8. Recall the mail analogy from the presentation. What is the IP address of the nearest router (think post office)? (Hint: See Fig. 2).

   _____

9. Add 1 to the last number in your answer to no. 8 and write the new address:

   _____

10. You will now give your computer an IP address on the simulated network. This will allow you to communicate with other devices. Go back to your terminal window and type the following:

    ifconfig eth0 <answer to 9>/24

11. Once you have an assigned IP address, you must set up a default gateway to send your out-of-network packets (think of the mail example in the presentation; you are defining your "local post office"). Open a new terminal window and type the following command:

    route add default gw <answer to 8>

12. Open a browser window by clicking on the Firefox icon on the left side of the screen:  .

13. In your browser, navigate to the simulated University of Texas El Paso (UTEP) Webmail server:

    http://webmail.utep.edu

14. What is the IP address of the machine hosting the http://webmail.utep.edu site?

    _____

4.3 Activity 3: Become a Trusted Entity and View Network Traffic

15. Go to your terminal window. Open the Loki tool by typing the following command:

    loki.py &

16. Click on the Routing tab.

17. Click on the RIP tab.

18. Click on the Gear icon on the top left corner. 

19. Press OK on the popup window shown in Fig. 5.

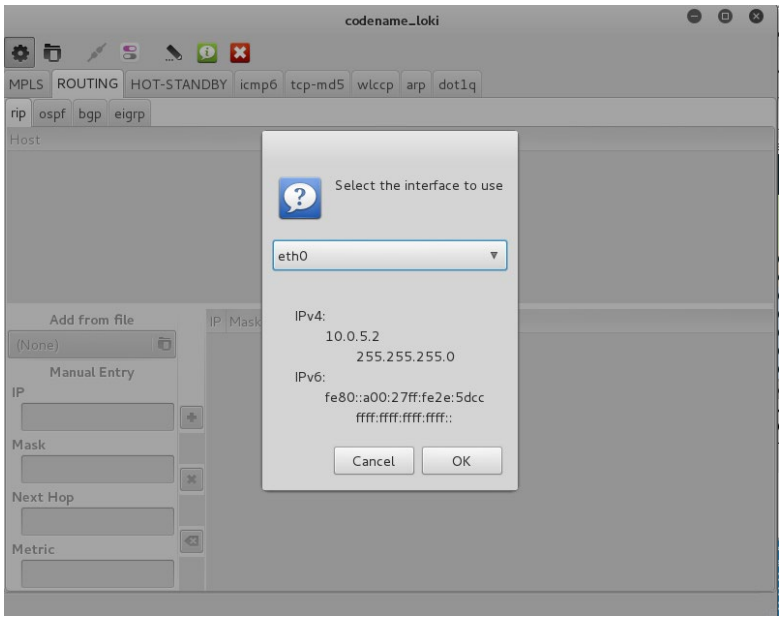

Fig. 5 Loki interface popup

20. In the Manual Entry pane on the left-hand side, enter the following values:

    IP: ***<answer from 14>***

    Mask: 255.255.255.255

    Next Hop: ***<answer from 9>***

    Metric: 1

21. Click on the Plus icon: 

22. In the Wireshark packet list, find a packet with a protocol type of Transmission Control Protocol and a source IP address of 11.0.0.2. Do you think the source of the traffic is still communicating with http://webmail.utep.edu? Why or why not?

4.4 Activity 4: Deeper Data Analysis

23. Open a new terminal window and assign yourself the IP address of the http://webmail.utep.edu machine by typing the following command:

    ifconfig eth0:1 <answer to 14>/24 up

24. Go back to your terminal window. Start a Webserver on your Kali Linux computer by typing the following command (ignore the error messages):

    apache2ctl start

25. Go to your Web browser and navigate to your local webserver that you just started by entering the following Uniform Resource Locator:

    http://localhost

26. To steal credentials, we have to host a Webpage that looks like the real http://webmail.utep.edu. We have stored a copy of the real http://webmail.utep.edu page on your computer. Type the following into your terminal window:

    cp /root/s_site/index.html /var/www/html/index.html

27. Restart the Web server by typing the following in your terminal window:

    apache2ctl restart

28. Go back to your Wireshark window. Type http into the filter textbox at the top of the screen and press the Enter key.

29. You should now see only http traffic that has been captured. Scan through the packet information and identify the user's credentials being passed to the Webserver:

    _____

Congratulations! You have completed the exercise.

5. Conclusions

This report presents a hands-on exercise meant to bring awareness to end-users and network engineers alike. It presents some of the hazards that may result from misconfigured routing protocols or routing protocols that were designed with little or no security. The exercise focuses on the RIP, but the same learning points apply to many other popular routing protocols used today, including OSPF and BGP, which are used to manage the direction of network data across the globe.

6. References

1. Neumann P. Internet routing black hole. 1997 May 1 [accessed 2019 Dec 3]. http://catless.ncl.ac.uk/Risks/19.12.html#subj1.

2. Zmijewski E. Accidentally importing censorship. 2010 Mar 30 [accessed 2019 Dec 3]. https://dyn.com/blog/fouling-the-global-nest/.

3. Jackson C. Auditing layer 3 routing protocols the Loki way. 2010 Aug 14 [accessed 2019 Dec 3]. https://www.networkworld.com/article/2231623/auditing-layer-3-routing-protocols-the-loki-way.html.

4. Mandory D. Recent Russian routing leak was largely preventable. 2017 Dec 22 [accessed 2019 Dec 3]. https://dyn.com/blog/recent-russian-routing-leak-was-largely-preventable/.

5. Kambhampati V, Massey D. BGP prefix hijack attacks [accessed 2019 Dec 3]. https://cs.slu.edu/~espositof/teaching/4650/lab3/.

6. Acosta JC, McKee J, Fielder A, Salamah S. A platform for evaluator-centric cybersecurity training and data acquisition. Proceedings of the Military Communications Conference (MILCOM); 2017 Oct 23; Baltimore, MD. p. 394–399.

List of Symbols, Abbreviations, and Acronyms

ARL	US Army Combat Capabilities Development Command Army Research Laboratory
BGP	Border Gateway Protocol
CIT	Collaborative Innovation Testbed
CIT-gen	Collaborative Innovation Testbed generator
CORE	Common Open Research Emulator
IP	Internet Protocol
RIP	Routing Information Protocol
OSPF	Open Shortest Path First
UTEP	University of Texas El Paso

1 (PDF)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
1 (PDF)	CCDC ARL FCDD RLD CL TECH LIB
2 (PDF)	CCDC ARL FCDD RLC ND J CLARKE FCDD RLC ND J ACOSTA