ARL-TN-1193 ● FEB 2024

Themis Deep Packet Inspection (DPI) Evasion Detection

by Jaime Acosta, Michael De Lucia, and Kelly Toppin

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 it is no longer needed. Do not return it to the originator.

ARL-TN-1193 ● FEB 2024

Themis Deep Packet Inspection (DPI) Evasion Detection

Jaime Acosta and Michael De Lucia
DEVCOM Army Research Laboratory

Kelly Toppin
ICF

REPORT DOCUMENTATION PAGE

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
February 2024	Technical Note	October 2023	September 2023

4. TITLE AND SUBTITLE
Themis Deep Packet Inspection (DPI) Evasion Detection

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**

6. AUTHOR(S)
Jaime Acosta, Michael De Lucia, and Kelly Toppin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
DEVCOM Army Research Laboratory ATTN: FCDD-RLA-ND El Paso, TX 79968-8900	ARL-TN-1193

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
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
ORCID ID: Jaime Acosta, 0000-0003-2555-9989

14. ABSTRACT
Open-source network intrusion detection systems (NIDS) such as Snort, Suricata, and Zeek rely primarily on signature- and anomaly-based detection techniques. These systems also deploy deep packet inspection (DPI) to analyze the data as it would be used by its final application layer. Malicious actors often use evasion techniques to avoid these NIDS. This study analyzed several DPI methods versus Themis DPI and Zeek detection capabilities.

15. SUBJECT TERMS
networks, docker, intrusion detection systems, IDS evasion, Zeek, Themis, Network, Cyber and Computational Sciences

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	C. THIS PAGE		
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UU	14

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*
Jaime Acosta	(915) 747-8012

STANDARD FORM 298 (REV. 5/2020)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures

List of Tables

1. Introduction

Open-source network intrusion detection systems (NIDS) such as Snort, Suricata, and Zeek rely primarily on signature- and anomaly-based detection techniques. These systems also deploy deep packet inspection (DPI) to analyze the data as it would be used by its final application layer. Malicious actors often use evasion techniques to avoid these NIDS. This study analyzed several DPI methods versus Themis DPI and Zeek detection capabilities. The current implementation of Transmission Control Protocol (TCP) is defined by RFC 9293.[1] TCP provides a reliable, in-order, byte-stream service to applications through the use of sequence numbers and per-segment checksums. The TCP connections are used to ensure point-to-point connection between two endpoints in an IP network. An important character, a TCP connection is its state and the connection progresses from one state to another in response to events. TCP states include LISTEN, SYN-SENT, SYN-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, TIME-WAIT and ClOSED. Attackers often abuse TCP statefulness to evade the NIDS to abuse application layer protocols. The DPI evasion techniques we tested are presented in Table 1.

Table 1 DPI evasion techniques

Experiment	DPI technique	Description
Experiment 0	Non-DPI	Attack without DPI evasion
Experiment 1	Bad ACK Num Data	In ESTABLISHED state, send junk data with out-of-window ACK number, and then send the request
Experiment 2	Bad ACK Num R STACK	In ESTABLISHED state, send partial request, then send an RST/ACK packet with out-of-window ACK number, and then send the remaining request
Experiment 3	MD5 Data	In ESTABLISHED state, send junk data with TCP MD5 option, and then send the request
Experiment 4	MD5 RST	In ESTABLISHED state, send partial request, then send an RST packet with TCP MD5 option, and then send the remaining request
Experiment 5	No ACK Flag Data	In ESTABLISHED state, send junk data without ACK flag, and then send the request
Experiment 6	No ACK Flag Fin	In ESTABLISHED state, send partial request, then send a FIN packet without ACK flag, and then send the remaining request

2. Methods

As shown in Figs. 1 and 2, individual Docker containers for the attacker, victim: ShellShock vulnerable, Zeek v4 and Zeek v5 were created on a Linux virtual machine. This Linux virtual machine was placed on a laptop connected to a tactical network environment. The team conducted the six localhost experiments using the custom DPI tools and collected the packet capture (PCAP) data. Then the experiment conditions were modified to allow external access by the Red Team. Next, the Red Team laptops were connected to the tactical network. The Red Team performed various DPI methods and we collected the PCAP data. The Team analyzed the PCAPs and results are presented in Tables 2 and 3.

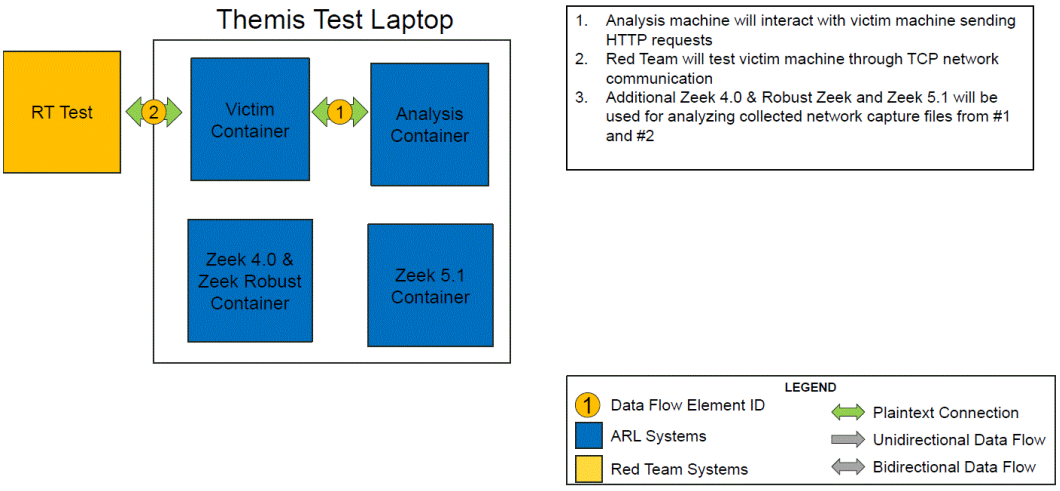

Fig. 1 Data flow 1

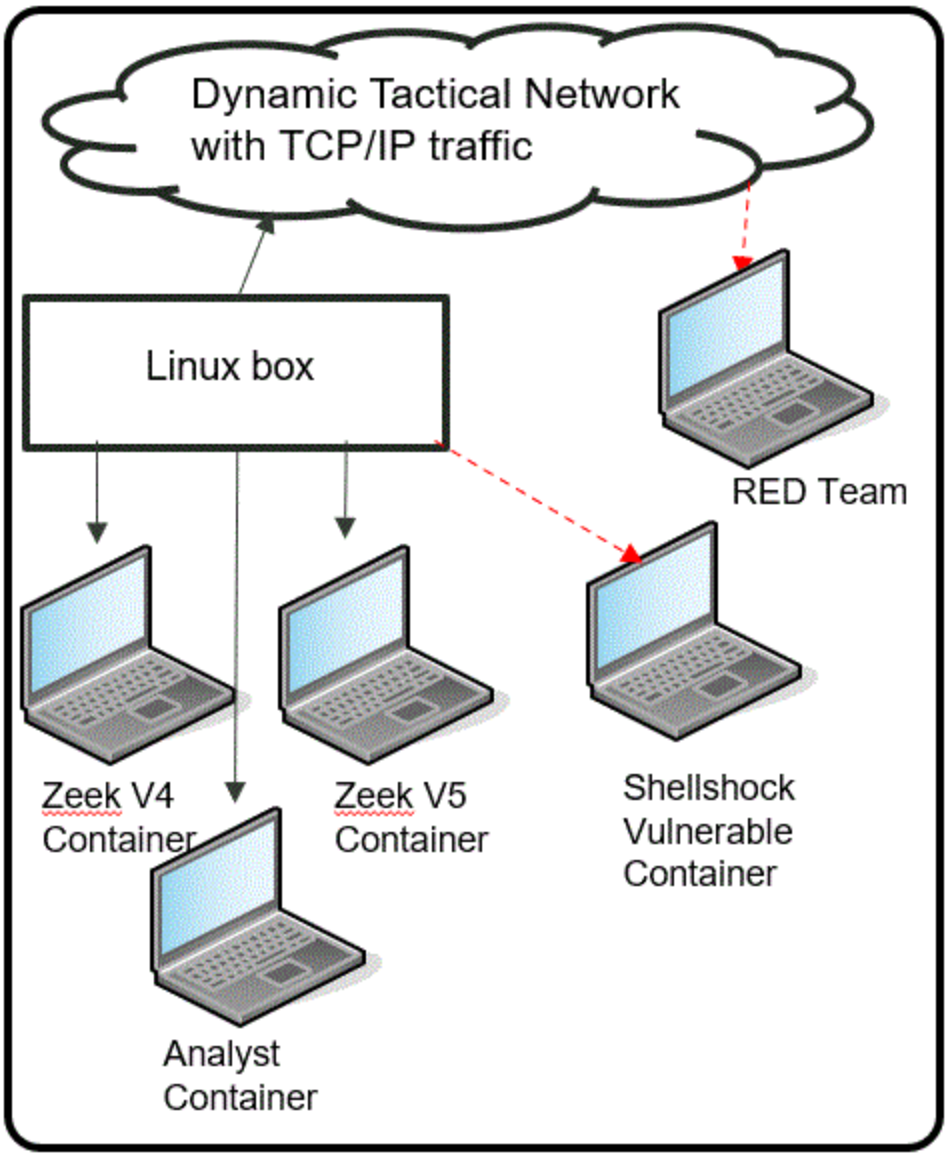

Fig. 2 Data flow across tactical network 1

3. Results

3.1 Localhost Experiments Using Custom DPI Tools

Table 2 shows the results of the localhost experiments using the various intrusion detection system technologies.

Table 2 Experiment success results

Experiment	Description	Zeek v4	Themis	Zeek v5
Experiment 0	Attack without DPI Evasion	Yes	Yes	Yes
Experiment 1	Bad ACK Num Data	No	Yes	No
Experiment 2	Bad ACK Num R STACK	No	Yes	No
Experiment 3	MD5 Data	No	Yes	No
Experiment 4	MD5 RST	No	Yes	No
Experiment 5	No ACK Flag Data	No	Yes	No
Experiment 6	No ACK Flag FIN	No	Yes	No

3.2 Red Team Experiments Using Commercial Off-the-Shelf DPI Evasion Tools

Table 3 shows the results from the red team interacting with the various intrusion detection system technologies.

Table 3 Red Team success results

Red Team	Zeek V4	Themis	Zeek V5
Red Team member 1	No	No	Yes
Red Team member 2	No	No	Yes
Red Team member 3	No	No	Yes
Red Team member 4	Yes	Yes	Yes

Note: Red Team member 4 used the custom DPI evasion scripts provided by the US Army Combat Capabilities Development Command Army Research Laboratory team.

4. Discussion

Themis was successful in detecting all the DPI techniques discussed in the *Themis Ambiguity-Aware Network Intrusion Detection Based on Symbolic Model Comparison*,[2] but was unsuccessful in detecting DPI used by the Red Team. The opposite is true for Zeek v5. This suggests the need for robust rules in Zeek v5 to reduce this gap in coverage.

5. Conclusions

The open-source nature of Zeek NIDS has allowed it to be a successful tool in the fight against malicious actors. However, this experiment shows the need for the community to remain committed to building robust detection rules.

6. References

1. Eddy W, editor. RFC 9293. Transmission control protocol (TCP), STD 7. MTI Systems; 2022 Aug. doi:10.17487/RFC9293

2. Wang Z, Zhu S, Man K, Zhu P, Hao Y, Qian Z, Krishnamurthy SV, La Porta T, De Lucia MJ. Themis: ambiguity-aware network intrusion detection based on symbolic model comparison. CCS '21: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security; 2021 Nov 15–19; Republic of Korea. p. 3384–3399. doi.org/10.1145/3460120.3484762

List of Symbols, Abbreviations, and Acronyms

ACK	an acknowledgment message employed to declare the receipt of a particular message
ARL	Army Research Laboratory
DEVCOM	US Army Combat Capabilities Development Command
DPI	deep packet inspection
FIN	a message that triggers a graceful connection termination between a client and a server
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
MD5	message-digest algorithm
NIDS	network intrusion detection systems
PCAP	packet capture
SYN	a synchronization message typically used to request a connection between a client and a server
RST	a message that aborts the connection (forceful termination) between a client and a server
TCP	Transmission Control Protocol

1 (PDF)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
1 (PDF)	DEVCOM ARL FCDD RLB CI TECH LIB
3 (PDF)	DEVCOM ARL FCDD RLA ND J ACOSTA M DE LUCIA K TOPPIN