NSF Award 1829698

CyberTraining CIP: Cyberinfrastructure Expertise on High-throughput Networks for Big Science Data Transfers

Hands-on Zeek (Bro) Labs

UTSA.

The University of Texas at San Antonio[™] The Cyber Center For Security and Analytics

Elias Bou-Harb, Ph.D., CISSP

Elias Bou-Harb

Associate Director Associate Professor



Expertise

Operational Cyber Security Cyber Forensics Critical Infrastructure Security Data Science Digital Investigation Internet Measurements

Research Grants

NSF OAC Core: Small: Devising Data-driven Methodologies by Employing Large-scale Empirical Data to Fingerprint, Attribute, Remediate and Analyze Internet-scale IoT Maliciousness

NSF CyberTraining CIP: Cyberinfrastructure Expertise on High-throughput Networks for Big Science Data Transfers

Recent Publications

Miranda, C., Kaddoum, G., **Bou-Harb, E**., Garg, S. and Kaur, K., 2020. A Collaborative Security Framework for Software-Defined Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security.

Pour, M.S., Mangino, A., Friday, K., Rathbun, M., **Bou-Harb, E.**, Iqbal, F., Samtani, S., Crichigno, J. and Ghani, N., 2019. On Data-driven Curation, Learning, and Analysis for Inferring Evolving Internet-of-Things (IoT) Botnets in the Wild. Computers & Security, p.101707.

Kaur, K., Garg, S., Kaddoum, G., **Bou-Harb, E**. and Choo, K.K.R., 2019. A Big Data-Enabled Consolidated Framework for Energy Efficient Software Defined Data Centers in IoT Setups. IEEE Transactions on Industrial Informatics.

Neshenko, N., **Bou-Harb, E.,** Crichigno, J., Kaddoum, G. and Ghani, N., 2019. Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3), pp.2702-2733.

Oliveira, D., Ghani, N., Hayat, M., Crichigno, J. and **Bou-Harb, E**., 2018. SDN testbed for evaluation of large exo-atmospheric EMP attacks. IEEE Communications Magazine, 57(1), pp.88-97.

Intro to Zeek (Bro)

Network Intrusion Detection Systems

- Software/hardware systems that actively monitor live networks for malicious traffic, policy violations and unidentified anomalies
- Deployed to protect operational networks without disturbing normal/benign packet traffic flows
- In contrast to firewalls, NIDS are most often passive, looking for signatures or anomalies, although they can operate as NIPS as well

UTSA. The Cyber Center For Security and Analytics The University of Texas at San Antonio[™]

- Zeek's Development began in 1995 by Vern Paxon (as Bro)
- Zeek's scripting language creates a versatile environment for fine-grained anomaly-related detection and processing
- Versatile formatting of output data for preprocessing and advanced analytics



Network Traffic Signatures: A Snort Signature

Follows a rule-based format



Network Traffic Signatures: A Zeek Signature

Follows a variable/data object-based format Variables support strings, integers and floats

```
signature sid-1371 {
    ip-proto == tcp
    dst-ip == a.b.0.0/16,c.d.e.0/24
    dst-port == 80
payload /.*conf/\httpd\.conf/
tcp-state established, originator
event "WEB-ATTACKS conf/http.conf attempt"
}
```

Zeek Log Files

- After processing network traffic, Zeek will output statistical log files
- By default, log files will be separated by the transport protocol and related characteristics
- At a basic level, these log files can be used to determine the presence of an anomaly
- Zeek log files can be formatted and exported to external processing software

Connection	Protocol-Specific	Detection	Observations
conn.log	http.log	notice.log	known_certs.log
files.log	ftp.log	signatures.log	known_services.log
x509.log	dns.log	traceroute.log	weird.log

Zeek Policy Scripts and Filters

- The Zeek scripting language is used to develop and implement filters and policies for the event-based engine
- Scripts can be implemented to permanently update Zeek's event handling or used as a non-permanent filter
- Script events include (but are not limited to):
 - Protocol-specific events
 - Application-level headers
 - Unknown/broken connection handling
- Packet data is accessible within the filters to be used for calculations or to be exported into separate log files

Zeek Policy Scripts and Filters

Protocol-oriented Zeek Filter

export { const addr_scan_interval = 5min &redef; const addr_scan_threshold = 20 &redef;

Custom-based detectors

function horizontal_scanning(c: connection):bool {
 if (num_requests(c\$id\$orig_h) > addr_scan_threshold &&
 time_alive(c\$connection) < addr_scan_interval) {
 print fmt("Horizontal Scanner Detected!");
 return c\$id\$orig_h;
 }
</pre>

```
}//end function
```

Zeek Inferring IoT-generating Scanning



The Insecurity of the IoT Paradigm

Zeek Inferring IoT-generating Scanning

Internet Address Space

Darknet

Scans

Attacker



- 2 TB of Darknet Data (Daily)
- 840K global IoT exploitations (25K in the US)
- Exploitations in health services, manufacturing plants, gov. entitles





Zeek Inferring IoT-generating Scanning

Internet Address Space

Darknet

Scans

Attacker

- Malicious scans from compromised IoT devices
 - 2 TB of Darknet Data (Daily)
 - 840K global IoT exploitations (25K in the US)
 - Exploitations in health services, manufacturing plants, gov. entitles



Date	2019-10-08	2019-11-25	2020-03-11	2020-04-26
# all infected hosts	754,169	836,255	806,326	839,082 (752,348)
# Compromised IoT	274,699	229,488	224,964	480,049 (405,184)
# all infected hosts (in USA)	16,614	15,957	23,779	25,468 (16,981)
# Compromised IoT (in USA)	6,569	5,489	8,541	12,909 (4,920)
# infected hosts in Medical	131	6	160	323 (311)
# Compromised IoT in Medical	17	0	10	76 (58)
# infected hosts in Medical (US)	26	2	22	58 (54)
# Compromised IoT in Medical (US)	3	0	2	11 (10)

Hands-on Zeek (Bro) Labs

Zeek Hands-on Labs

- Lab 1- Introduction to the Capabilities of Zeek
- Lab 2 An Overview of Zeek Logs
- Lab 3 Parsing, Reading and Organizing Zeek Files
- Lab 4 Generating, Capturing and Analyzing Network Scanner Traffic
- Lab 5 Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic
- Lab 6 Introduction to Zeek Scripting
- Lab 7 Introduction to Zeek Signatures
- Lab 8 Advanced Zeek Scripting for Anomaly and Malicious Event Detection
- Lab 9 Profiling and Performance Metrics of Zeek
- Lab 10 Application of the Zeek IDS for Real-Time Network Protection
- Lab 11 Preprocessing of Zeek Output Logs for Machine Learning
- Lab 12 Developing Machine Learning Classifiers for Anomaly Inference and Classification

Lab 4 - Generating, Capturing and Analyzing Network Scanner Traffic



Device	Account	Password	
Client	admin	password	

Lab 4 - Generating, Capturing and Analyzing Network Scanner Traffic

admin@bro1: ~ 💿 🗐 😣
File Edit View Search Terminal Help
admin@bro1:~\$ sudo nmap -sS 192.168.2.2 [sudo] password for admin:
Starting Nmap 7.60 (https://nmap.org) at 2019-06-26 18:27 EDT Nmap scan report for 192.168.2.2 Host is up (0.0012s latency). All 1000 scanned ports on 192.168.2.2 are closed
admin@bro2: ~/Zeek-Labs-Workspace/TCP-Traffic 🛛 🔵 回 😣
File Edit View Search Terminal Help
<pre>admin@bro2:~/Zeek-Labs-Workspace/TCP-Traffic\$ sudo tcpdump -i ens33 -s 0 -w scan traffic.pcap [sudo] password for admin: tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 by tes ^C8045 packets captured 8045 packets received by filter 0 packets dropped by kernel admin@bro2:~/Zeek-Labs-Workspace/TCP-Traffic5</pre>
admin@bro2: ~/Zeek-Labs-Workspace/TCP-Traffic 💿 🗐 😣
<pre>File Edit View Search Terminal Help admin@bro2:~/Zeek-Labs-Workspace/TCP-Traffic\$ zeek-cut id.resp_p < conn.log so rt uniq -c sort -rn head -n 10 62 53 8 80 8 443 5 995 5 6667 5 3 5 25 4 9999 4 9998 4 999 admin@bro2:~/Zeek-Labs-Workspace/TCP-Traffic\$</pre>

Lab 9 - Developing Machine Learning Classifiers for Anomaly Inference and Classification

Program Visualization Tools Help Applications Explorer Experimenter KnowledgeFlow Waikato Environment for Knowledge Analysis Version 3.8.3 (c) 1999-2018 The University of Waikato Hamilton, New Zealand			w	eka GUI (hooser			008	
Applications Explorer Experimenter KnowledgeFlow Waikato Environment for Knowledge Analysis Version 3.8.3 (c) 1999 - 2018 The University of Waikato Hamilton, New Zealand	Program Vis	ualization	Tools H	elp					P
Waikato Environment for Knowledge Analysis Weikato Environment for Knowledge Analysis Version 3.8.3 (c) 1999 - 2018 The University of Waikato Hamilton, New Zealand						Ap	plicatio	ns	Choose None
Waikato Environment for Knowledge Analysis Experimenter Waikato Environment for Knowledge Analysis KnowledgeFlow Workbench I ime Instances: 1401 None No. Name Image: Nonversity of Waikato Simple CLI Simple CLI 3 destip 4 sourceport						ſ	Expl	orer	Current relation
of Waikato KnowledgeFlow Waikato Environment for Knowledge Analysis Workbench Workbench No. No. Name 1 time 2 sourceip 3 destip 4 sourceport		A	N Th		l.		Experin	nenter	Relation: networktrafficAttributes: 8Instances: 1401Sum of weights: 1401
Waikato Environment for Knowledge Analysis Version 3.8.3 (c) 1999 - 2018 The University of Waikato Hamilton, New Zealand Workbench No. Name 1 time 2 sourceip 3 destip 4 sourceport	· ·	t	of	Waikato			Knowled	IgeFlow	Attributes All None Invert Pattern
Waikato Environment for Knowledge Analysis 1 time Version 3.8.3 2 sourceip (c) 1999 - 2018 3 destip The University of Waikato 4 sourceport							Workb	pench	No. Name
5 destport	Waikato Enviro Version 3.8.3 (c) 1999 - 2018 The University Hamilton, New	nment for Ki of Waikato Zealand	nowledge A	inalysis			Simpl	e CLI	1 time 2 sourceip 3 destip 4 sourceport 5 destport 6 protocol
Detailed Accuracy By Class 8 Class	Detailed A	ccuracy By	Class ===						7 duration 8 class
TP Rate FP Rate Precision Recall F-Measure MCC ROC Area 1.000 0.000 1.000 1.000 1.000 1.000 1.000 1.000 0.000 1.000 1.000 1.000 1.000 1.000 Weighted Avg. 1.000 0.000 1.000 1.000 1.000 1.000	Weighted Avg.	TP Rate 1.000 1.000 1.000	FP Rate 0.000 0.000 0.000	Precision 1.000 1.000 1.000	Recall 1.000 1.000 1.000	F-Measur 1.000 1.000 1.000	e MCC 1.000 1.000 1.000	ROC Area 1.000 1.000 1.000	
=== Confusion Matrix === a b < classified as 831 0 a = 1 0 570 b = 0	Confusion a b < 831 0 a 0 570 b	Matrix === classified = 1 = 0	l as						

NSF Award 1829698

CyberTraining CIP: Cyberinfrastructure Expertise on High-throughput Networks for Big Science Data Transfers

Hands-on Zeek (Bro) Labs

Enjoy the Labs [©] Thanks for the support!



The University of Texas at San Antonio[™] The Cyber Center For Security and Analytics

Elias Bou-Harb, Ph.D., CISSP elias.bouharb@utsa.edu