TryHackMe Advent of Cyber 2025 Day 22: C2 Detection with RITA

Command & Control Communication Analysis

1. Executive Summary

Day 22 focused on Command and Control (C2) detection using RITA (Real Intelligence Threat Analytics) framework. Successfully converted PCAP files to Zeek logs, imported network data into RITA, analyzed beacon patterns, identified malicious C2 infrastructure (rabbithole.malhare.net), discovered 6 compromised hosts, examined connection metadata including beacon scores and duration, and applied advanced filtering to investigate suspicious traffic. Retrieved all challenge answers demonstrating practical understanding of network traffic analysis, C2 beacon detection, threat intelligence correlation, and RITA's analytical capabilities.

2. Understanding RITA

2.1 What is RITA?

Real Intelligence Threat Analytics (RITA) is an open-source framework developed by Active Countermeasures specifically for detecting Command and Control (C2) communication through network traffic analysis. Unlike traditional signature-based detection, RITA employs behavioral analytics to identify C2 patterns even when specific signatures are unknown.

2.2 Core Features

- **C2 Beacon Detection:** Identifies periodic communication patterns characteristic of malware beaconing
- **DNS Tunneling Detection:** Spots data exfiltration through DNS queries
- **Long Connection Detection:** Flags unusually persistent connections
- **Data Exfiltration Detection:** Monitors large outbound data transfers
- **Threat Intel Integration:** Cross-references IPs/domains against known IOCs
- **Severity Scoring:** Ranks connections by threat level
- **Host Correlation:** Shows number of internal hosts communicating with external IPs
- **First Seen Tracking:** Records when external hosts first appeared on network

2.3 Analytics Engine

RITA correlates multiple network parameters:

- IP addresses (source/destination)
- Port numbers and protocols
- Timestamps and connection intervals
- Connection durations
- Data volume transferred
- DNS query patterns

3. Understanding Zeek

3.1 What is Zeek?

Zeek is open-source Network Security Monitoring (NSM) tool. Critical distinction: Zeek is NOT a firewall, IPS, or IDS. It doesn't use signatures or rules to block traffic. Instead, Zeek passively observes network traffic, analyzes it, and converts raw packets into structured, enriched logs suitable for analysis.

3.2 Data Collection Methods

- SPAN Ports: Copies traffic from one switch port to monitoring port
- Network Taps: Physical devices inserted into network infrastructure
- PCAP Files: Imported packet captures for offline analysis

3.3 NSM Data Types

- **Transaction Data:** Summarized application-layer protocol records
- **Extracted Content:** Files and artifacts extracted from traffic

4. Workflow Implementation

4.1 PCAP to Zeek Conversion

Command:

```
zeek readpcap pcaps/AsyncRAT.pcap zeek_logs/asyncrat
```

This command converts AsyncRAT.pcap into structured Zeek logs stored in zeek_logs/asyncrat directory.

4.2 Zeek Log Types Generated

- conn.log: Connection summaries (IPs, ports, duration, bytes)
- dns.log: DNS query/response records
- http.log: HTTP transactions
- ssl.log: SSL/TLS handshake details
- files.log: Extracted file metadata
- x509.log: Certificate information

4.3 Importing to RITA

```
rita import --logs ~/zeek_logs/asyncrat/ --database asyncrat
```

RITA parses Zeek logs, correlates data, applies analytics modules, generates severity scores, and cross-references threat intelligence feeds.

5. RITA Interface Analysis

5.1 Viewing Results

```
rita view asyncrat
```

5.2 Interface Components

Search Bar:

- Activate: Press forward slash (/)
- Help: Press ? while in search mode
- Exit: Press ESC key

Results Pane Columns:

- **Severity:** Score based on threat modifiers
- **Source/Destination:** IP addresses or FQDNs
- **Beacon Likelihood:** Percentage indicating C2 beacon probability
- **Duration:** Connection persistence time
- **Subdomains:** Count of unique subdomains
- **Threat Intel:** Matches against known IOCs

5.3 Threat Modifiers

- **MIME Type/URI Mismatch:** HTTP header inconsistencies
- **Rare Signature:** Unusual patterns (unique user agents)
- **Prevalence:** Percentage of internal hosts contacting external IP
- **First Seen:** When external host first appeared
- **Missing Host Header:** HTTP connections without host header
- **Large Outgoing Data:** Excessive data exfiltration
- **No Direct Connections:** Complex/hidden C2 channels

6. Challenge Investigation

6.1 PCAP Processing

```
zeek readpcap pcaps/rita_challenge.pcap zeek_logs/rita_challenge
```

6.2 RITA Import

```
rita import --logs ~/zeek_logs/rita_challenge/ --database rita_challenge
```

6.3 Analysis & Answers

Q1: Hosts Communicating with malhare.net?

```
rita view rita_challenge
```

Located malhare.net entry in results pane. Examined Prevalence modifier showing internal host count.

Answer: 6

Q2: Threat Modifier for Host Count?

Reviewed Threat Modifiers list in details pane.

Answer: prevalence

Q3: Highest Connection Count to rabbithole.malhare.net?

Searched for rabbithole.malhare.net entries. Examined Connection Count in details pane for each source IP.

Answer: 40 (from source 10.0.0.15)

Q4: Search Filter Syntax?

Pressed ? in search mode to view filter help. Constructed filter:

- dst: destination filter
- beacon: beacon score filter with >= operator
- sort: duration-desc for descending order

Answer: dst:rabbithole.malhare.net beacon:>=70 sort:duration-desc

Q5: Port Used by 10.0.0.13?

Selected 10.0.0.13 entry in results pane. Examined Connection Info in details pane showing port number.

Answer: 8080

7. Key Skills Developed

- PCAP to Zeek log conversion
- RITA framework usage
- C2 beacon pattern recognition
- Threat modifier interpretation
- Advanced search filter construction
- Network traffic behavioral analysis
- Threat intelligence correlation
- Command & Control detection

8. Conclusion

Day 22 provided comprehensive training in C2 detection using RITA framework. Successfully converted PCAPs to Zeek logs, leveraged RITA's behavioral analytics to identify malicious infrastructure, analyzed beacon patterns, and applied advanced filtering. RITA's strength lies in detecting C2 communication through behavioral patterns rather than signatures-critical for identifying zero-day threats and novel attack infrastructure.

Challenge Status: COMPLETED ✓ - All 5 Questions Answered!