**🧪 RITA Labs – Beginner Notes (Hacking Identification & Analysis)**

**🛠️ What is RITA?**

**RITA** (Real Intelligence Threat Analytics) is an open-source tool by **Black Hills Information Security** used to analyze network traffic and detect **suspicious or malicious behavior**.

It works with **Zeek logs** (formerly Bro) to analyze:

| **🔍 Detection Type** | **💡 Description** |
| --- | --- |
| Beaconing | Regular "phone home" behavior by malware |
| Long Connections | Suspicious long-lived connections |
| DNS Tunneling | Hiding data in DNS queries |
| Threat Intel | Checking traffic against known bad IPs/domains |

**✅ Why Learn RITA?**

* To simulate **real-world threat detection** techniques.
* To **analyze traffic patterns** of malware like dnscat and vsagent.
* To understand **how to hunt** for hidden attackers in a network.

**⚙️ How to Use RITA (General Workflow)**

Here’s a simplified step-by-step process to use RITA in a lab:

**🔹 1. Install Zeek & RITA (in lab environment)**

Use Kali Linux or a clean Ubuntu server.

# Install Zeek

sudo apt install zeek -y

# Install RITA

curl https://raw.githubusercontent.com/activecm/rita/master/install.sh | sudo bash

**🔹 2. Collect Network Logs Using Zeek**

Capture PCAP traffic using tcpdump or a lab tool like Security Onion. Then convert it into logs using Zeek:

zeek -r traffic.pcap

This creates log files like conn.log, dns.log, etc.

**🔹 3. Import Zeek Logs into RITA**

rita import /path/to/zeek/logs my-lab-data

my-lab-data is the name of the dataset (you can name it anything)

**🔹 4. Analyze the Data**

Run analysis:

rita analyze my-lab-data

Then generate a report:

rita show-beacons my-lab-data

rita show-long-connections my-lab-data

rita show-dns my-lab-data

rita show-threats my-lab-data

Each command shows specific activity:

**🕵️ RITA Detection Types Explained**

**📡 1. Beaconing Detection**

* Malware often “phones home” at regular intervals.
* RITA detects **repeating patterns** in network traffic.

rita show-beacons my-lab-data

Useful for detecting tools like vsagent.

**🕓 2. Long Connection Detection**

* Attackers may keep long-lasting sessions to avoid reconnecting.

rita show-long-connections my-lab-data

Suspicious if you see long sessions with unknown IPs.

**🌐 3. DNS Tunneling Detection**

* Malware like dnscat hides data inside DNS requests.

rita show-dns my-lab-data

Look for strange or overly long DNS requests.

**🚨 4. Threat Intel Feed Checking**

* Checks IPs/domains against known **blacklists** (bad actors).

rita show-threats my-lab-data

Great for spotting **blacklisted IPs** or malware hosts.

**🧠 Summary Table**

| **🔍 Feature** | **🔑 Purpose** | **🧪 Detects** |
| --- | --- | --- |
| show-beacons | Repeating traffic | Malware callbacks |
| show-long-connections | Ongoing connections | Hidden tunnels |
| show-dns | Weird DNS usage | DNS Tunneling |
| show-threats | Matches bad IPs/domains | Known threats |

**🎯 Real Lab Use-Cases**

* Use PCAPs from labs that simulate **dnscat**, **vsagent**, or C2 communication.
* Analyze using Zeek + RITA to detect activity.
* Practice threat hunting and writing basic reports.