Naqash Abbas

Cybersecurity analysts | Network Traffic Analyst | Open-Source Advocate

---

🔷 **LinkedIn Profile:** https://www.linkedin.com/in/naqash-abbas-314661282/
🔷 **Location:** Pakistan
🔷 **Lab Environment:** Kali Linux (VM), Zeek Network Security Monitor
🔷 **Tool Focus:** Zeek 8.x (Built from Source)

📘 About This Manual

This hands-on lab manual is the result of my independent exploration and practical implementation of **Zeek**, a powerful open-source network monitoring framework. Every step from installation to traffic analysis, was tested on my Kali Linux machine, and each section includes:

- ✅ Real command outputs
- 🖼️ Annotated screenshots
- 🔍 Log file analysis
- 📄 Custom notes for understanding

This document not only showcases my technical capability, but also my attention to detail, documentation skills, and practical grasp of network-level threat detection.

"Security is not a product, but a process and mastering tools like Zeek puts us in control of that process."
— *Naqash Abbas*

ZEEK PROFESSIONAL MANUAL

INTRODUCTION TO ZEEK

What is Zeek?

Zeek is an open-source network security monitor that passively observes network traffic and generates high-level logs and events. It's used for:

- Detecting intrusions
- Monitoring policy violations
- Analyzing network behavior
- Logging encrypted and unencrypted traffic details

Why Use Zeek?

- Works passively on network taps or SPAN ports
- Highly customizable with its scripting language
- Used in SOCs, threat hunting, and forensic analysis

SYSTEM REQUIREMENTS

- OS: Linux (Ubuntu/Kali/CentOS), FreeBSD, or macOS
- RAM: Minimum 2 GB (8 GB recommended for large traffic)
- Tools: libpcap, cmake, make, gcc/g++, Python 3

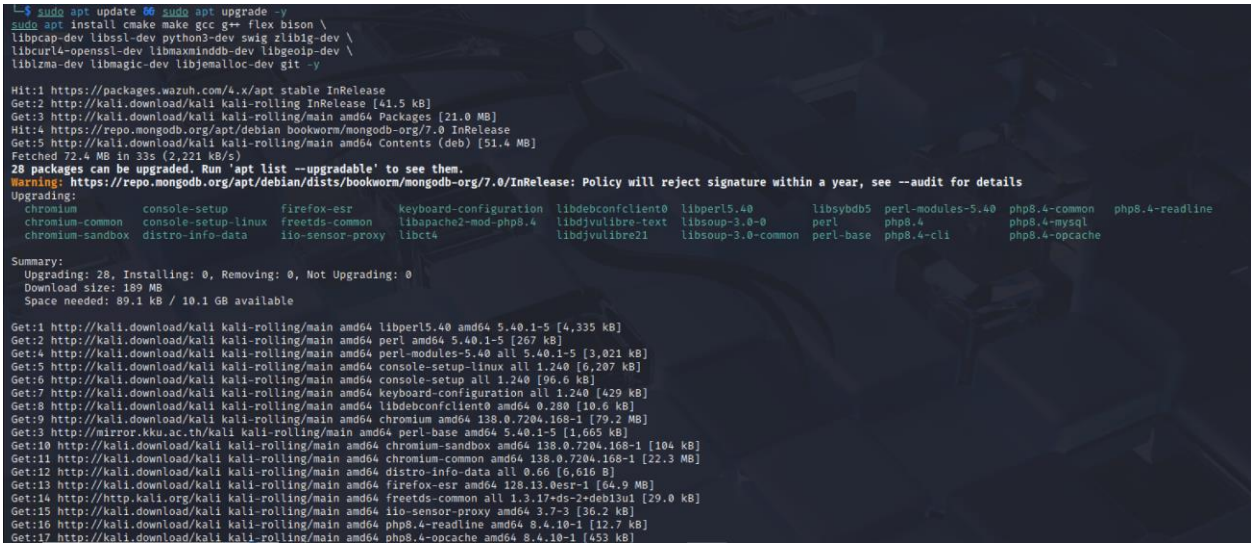
✅ Step-by-Step Installation of Zeek on Kali Linux

🔷 Step 1: Update System & Install Dependencies

Make sure your system is up to date and install required packages:

```
sudo apt update && sudo apt upgrade -y

sudo apt install cmake make gcc g++ flex bison \

libpcap-dev libssl-dev python3-dev swig zlib1g-dev \

libcurl4-openssl-dev libmaxminddb-dev libgeoip-dev \

liblzma-dev libmagic-dev libjemalloc-dev git -y
```

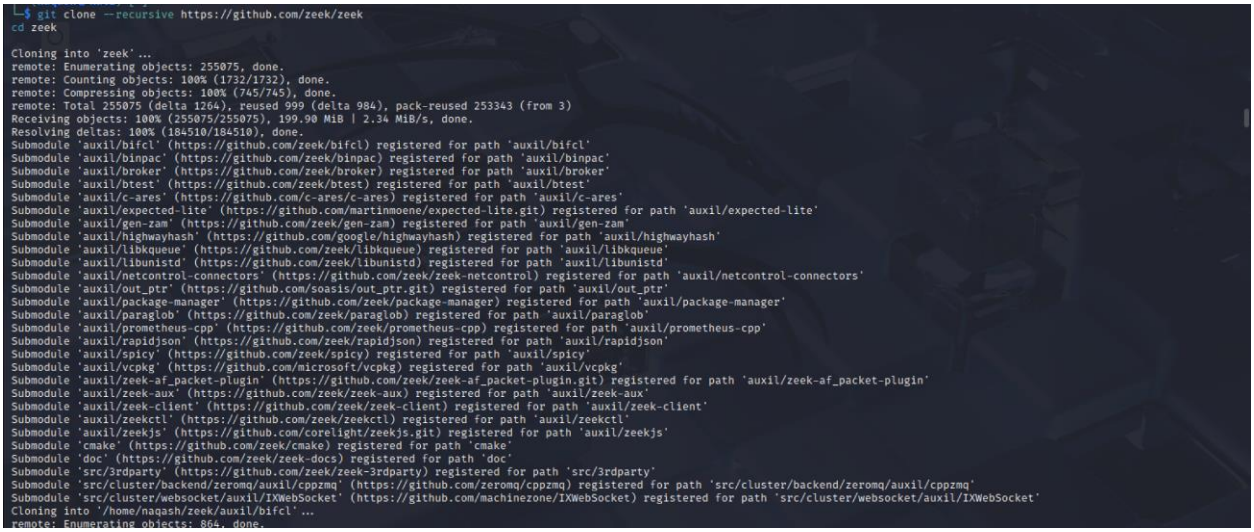
These are essential development libraries needed to build Zeek from source.



🔷 Step 2: Clone the Zeek Source Code

```
git clone --recursive https://github.com/zeek/zeek
cd zeek
```

The --recursive flag ensures all submodules (like zkg, the Zeek Package Manager) are cloned too.



🔷 Step 3: Build Configuration

Create a separate directory for the build process:

```
mkdir build
cd build
../configure
```

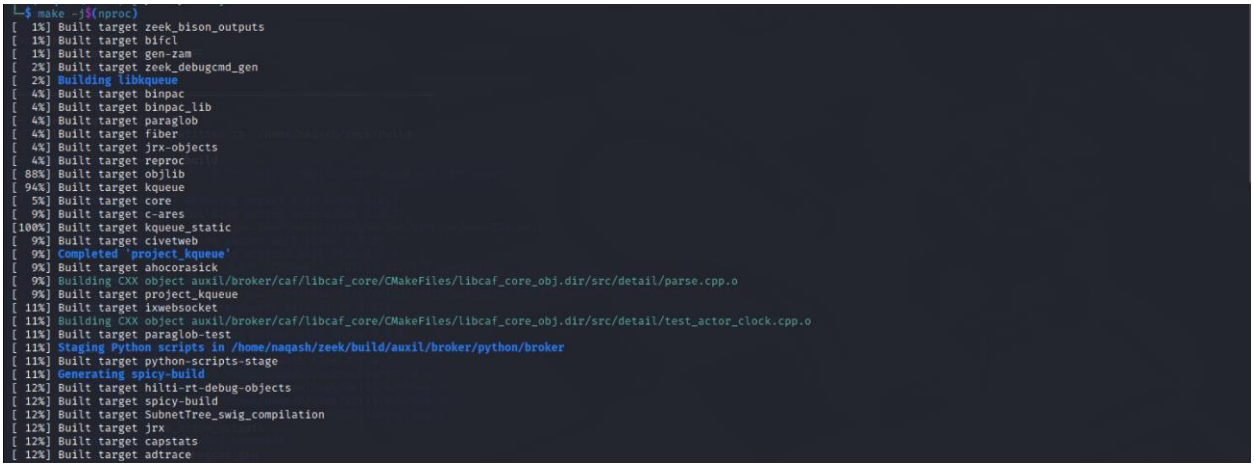
The configure script checks for dependencies and prepares the Makefile.

🔷 Step 4: Compile Zeek

```
make -j$(nproc)
```

The -j$(nproc) option uses all available CPU cores to speed up the build.

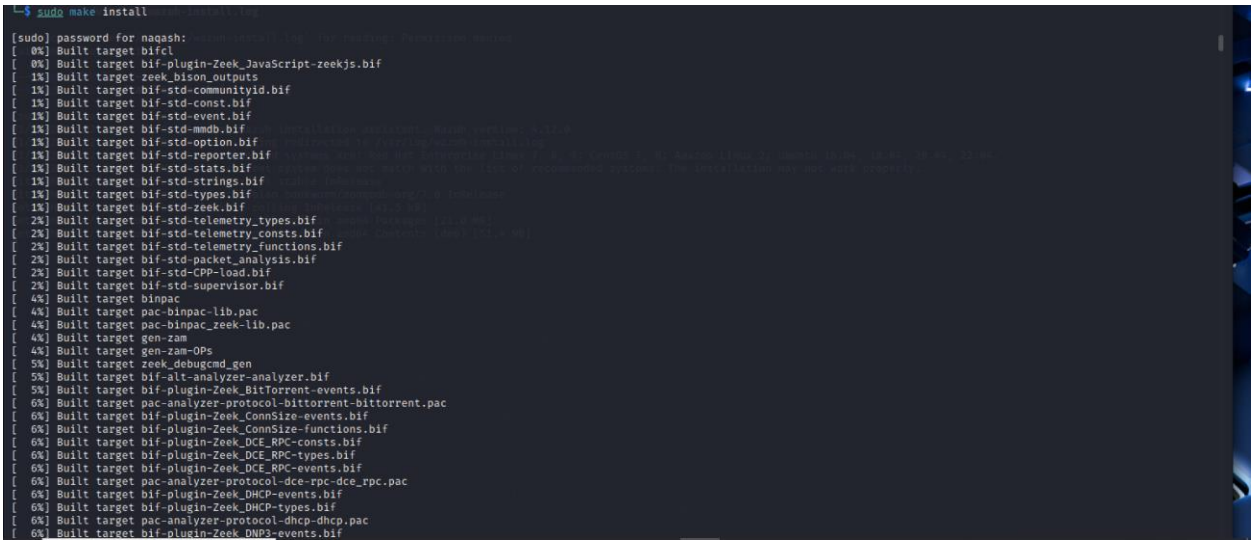
This step can take several minutes depending on your system specs.



🔷 Step 5: Install Zeek

```
sudo make install
```

This will install Zeek binaries to /usr/local/zeek.



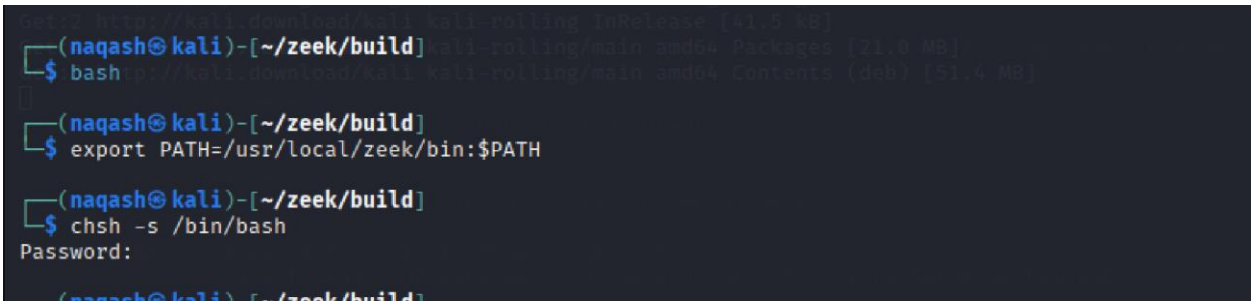
🔷 Step 6: Add Zeek to System PATH

To use Zeek from anywhere in the terminal, add it to your PATH:

```
export PATH=/usr/local/zeek/bin:$PATH
```

You also ensured Bash is your default shell with:

```
chsh -s /bin/bash
```



🧪 Step 7: Verify Installation

zeek --version

You should see an output like:

zeek version 6.0.x

📂 Step 8: Test Zeek with a PCAP File

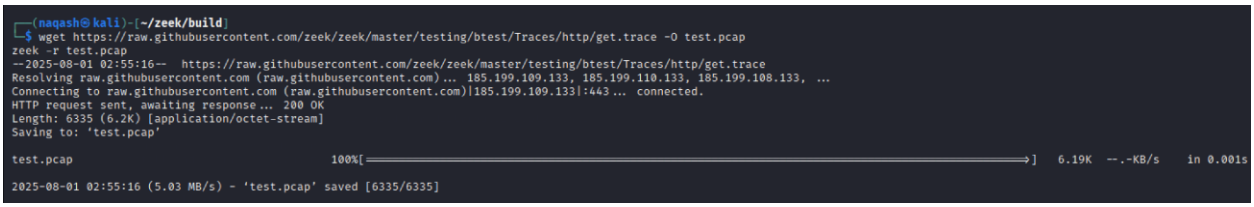
Test Zeek with sample network traffic:

Wget https://raw.githubusercontent.com/zeek/zeek/master/testing/btest/Traces/http/get.trace -O test.pcap

zeek -r test.pcap

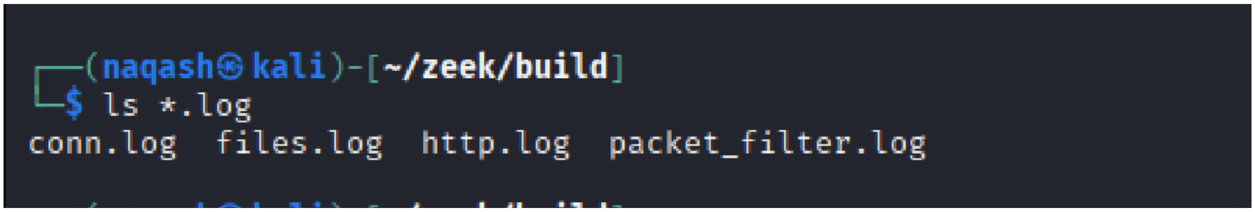
📦 Zeek will process the file and automatically create **log files** in the current folder, such as:

- conn.log → Connection logs
- http.log → HTTP request details
- weird.log → Unexpected protocol behavior
- notice.log → Any triggered alerts (if present)



🔷 2. View the Output Logs

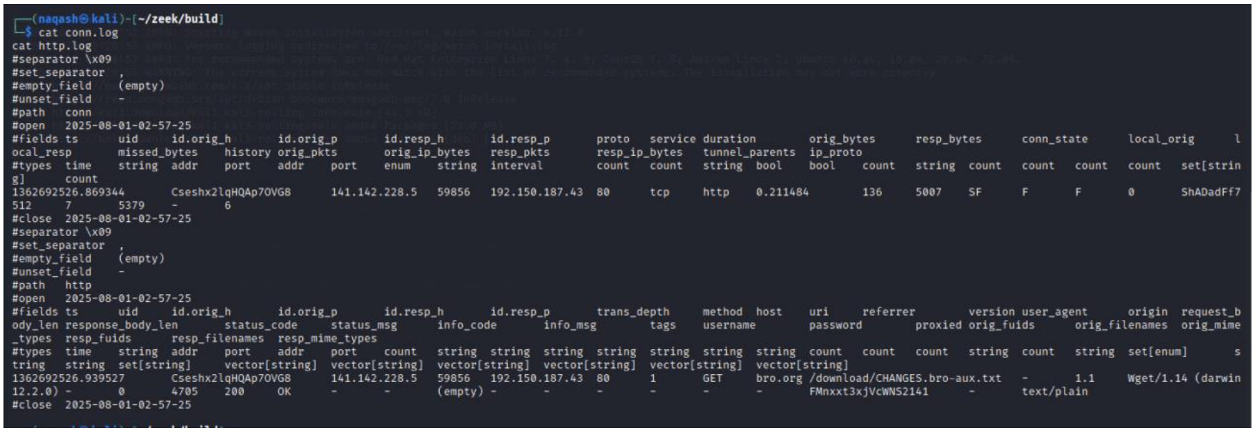
You can now inspect the logs. Try:



Then view individual logs:

cat conn.log

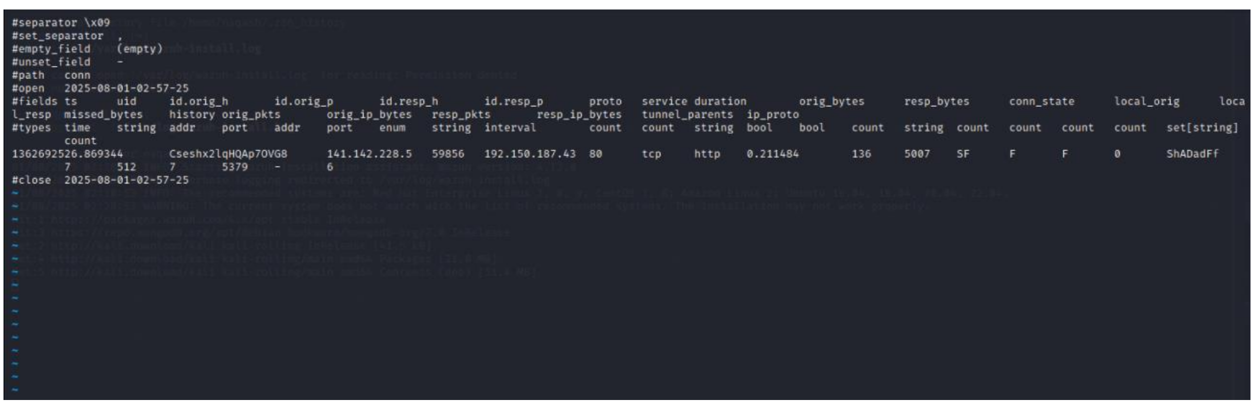
cat http.log



Or more readable:

less conn.log

less http.log

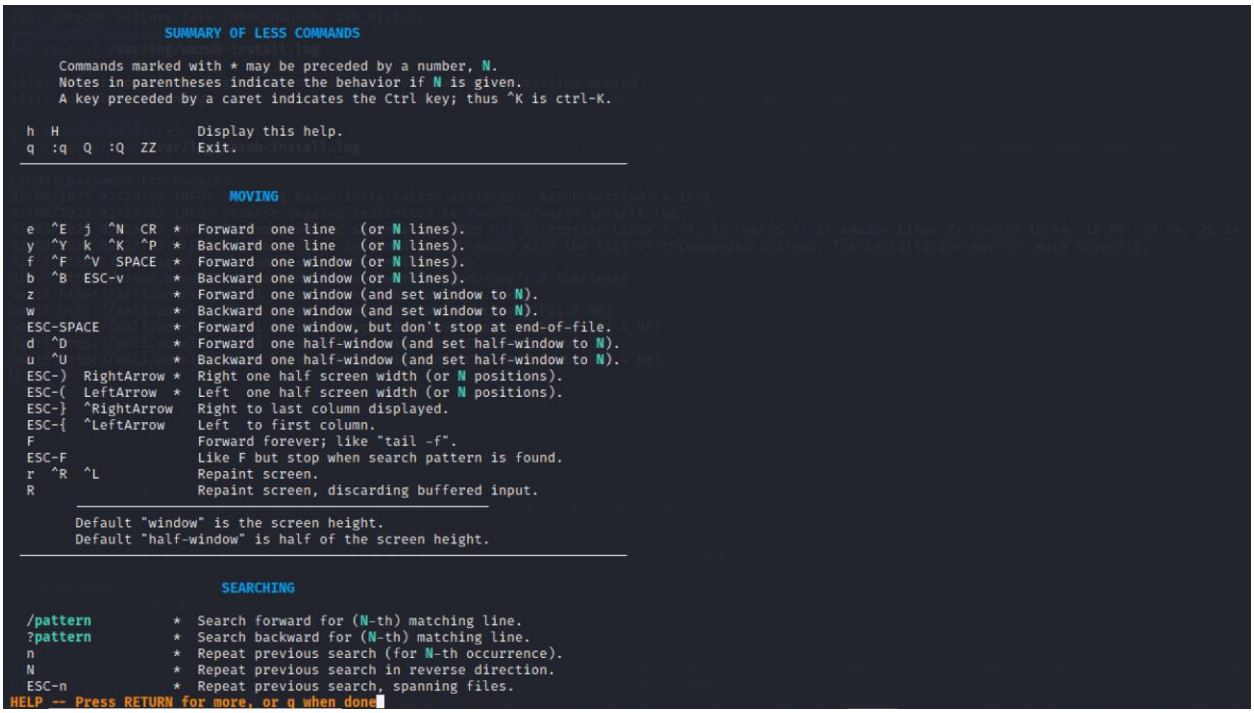


💡 You can also extract specific fields using zeek-cut:

zeek-cut id.orig_h id.resp_h < conn.log

zeek-cut host uri < http.log

press q to exit



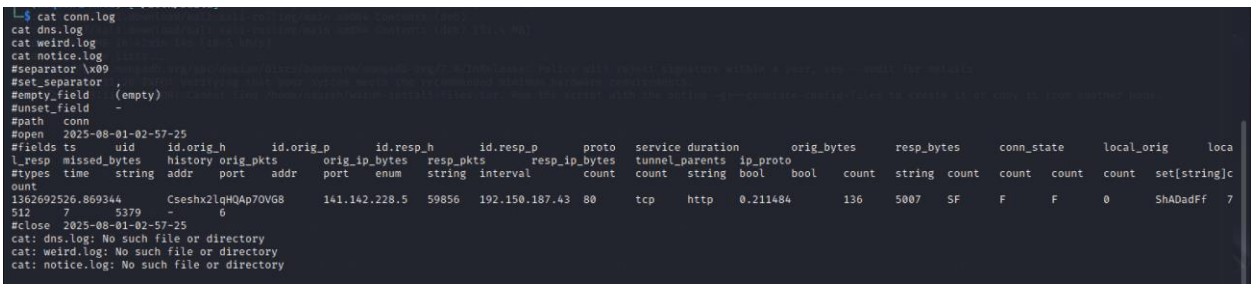
Inspect More Logs

cat conn.log

cat dns.log

cat weird.log

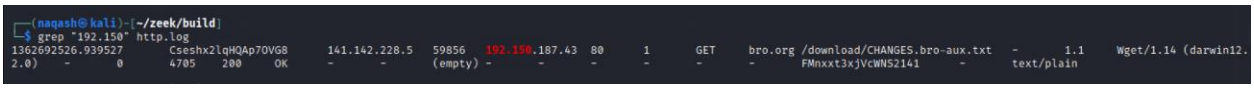
cat notice.log



Analyze Specific Traffic

Use filtering tools like grep:

```
grep "192.150" http.log
```



📦 Bonus: Zeek Package Manager (ZKG)

ZKG lets you install Zeek scripts from the community:

```
zkg list
```

```
zkg install zeek/zeek-af-packet-plugin
```

🧠 Final Thoughts

You've now set up **Zeek** from source on **Kali Linux** — a powerful tool in any security analyst's arsenal.

Zeek can be extended or integrated with:

- Elasticsearch & Kibana
- Wazuh / SIEM
- Suricata / IDS
- Threat intelligence feeds
- Custom detection scripts