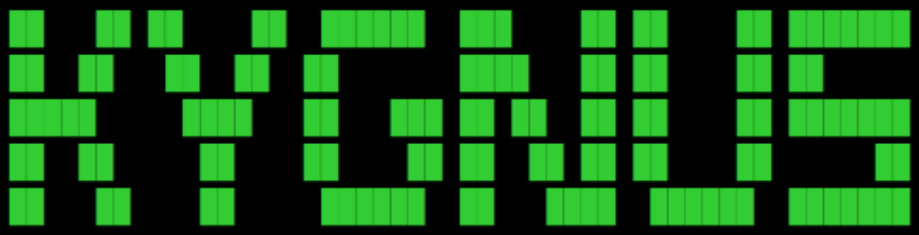

KooshaYeganehGnuLinuxSoftwares

|<[][]$#/-\ `/[-(_+[-|\|[-# (_+|\||_| |_!|\||_|)($[]|='|'\|//-\/2[-$

Linux Security

Zeek

Zeek is an open-source network intrusion detection system and a network traffic analyzer that uses a domain-specific scripting language. With Zeek you can detect suspicious signatures and anomalies, track DNS, HTTP, and FTP activity. This tool is capable of automatically downloading suspicious files it spots on the network, sending them for analysis, notifying relevant parties if anything is uncovered, blacklisting the source and shutting down the device that downloaded it. In this path, you will learn how to utilize Zeek in your environment to detect intrusions and anomalies.

Dependencies

1. Libpcap (**http://www.tcpdump.org**)
2. OpenSSL libraries (https://www.openssl.org)
3. BIND8 library
4. Libz
5. Bash (for ZeekControl)
6. Python 3.5 or greater (https://www.python.org/)

Download From SUSE :

https://software.opensuse.org/download.html?project=security%3Azeek&package=zeek-lts

Download From Git :

➜ git clone --recursive https://github.com/zeek/zeek

➜ ./configure

➜ make

> make install

Download From Website

➜ wget https://download.zeek.org/zeek-x.y.z.tar.gz

➜ tar -xzvf zeek-x.y.z.tar.gz

➜ cd zeek-x.y.z

➜ ./configure

➜ make

➜ sudo make install

Now cd into the **zeek** folder located at **/opt/zeek/bin**.

➜ cd /opt/zeek/bin

Next, navigate to **/opt/zeek/etc,** and modify the **node.cfg file**. In the node.cfg file, modify the interface. Use **ifconfig** to find out what your interface is, and then just replace that after the equal sign in the **node.cfg file**. In my case, the interface was **enp4s0**, so I set the interface=**enp4s0**.

It would be wise to also configure the networks.cfg file (/opt/zeek/etc). In the networks.cfg file, choose the ip addresses that you wish to monitor. Put a hashtag next to the ones that you would like to omit.

We have to set the path using:

➜ echo "export PATH=$PATH:/opt/zeek/bin" >> ~/.bashrc

➜ source ~/.bashrc

Next, type ZeekControl and install it:

➜ Zeekctl > install

you can start zeek using the following command:

➜ Zeekctl > start

You can check the status using:

➜ Zeekctl > status

And you can stop zeek using:

➜ Zeekctl > stop

Once zeek has been stopped, log files are created in

/opt/zeek/logs/current.

In the notice.log, zeek will put those things that it considers odd, potentially dangerous, or altogether bad. This file is definitely worth noting because this is the file where inspection-worthy material is placed!.

In the weird.log, zeek will put any malformed

connections,malfunctioning/misconfigured hardware/service, or even a hacker trying to confuse the system. Either way, it's, at the protocol level, weird.

So even if you ignore the weird.log, it is suggested that you do not do so with the notice.log. The notice.log is similar to an intrusion detection system alert. Further information about the various logs created can be found at

https://docs.zeek.org/en/master/logs/index.html.

By default, Zeek Control takes the logs it creates, compresses them, and archives them by date. This is done every hour. You can change the rate at which it's done via LogRotationInterval, which is located in

/opt/zeek/etc/zeekctl.cfg.

By default, all logs are created in a TSV format. Now we're going to turn the logs into JSON format. For that, stop zeek.

In /opt/zeek/share/zeek/site/local.zeek, add the following:

➜ @load policy/tuning/json-logs

Further, you can write scripts to detect malicious activity yourself. Scripts are used to extend the functionality of zeek. This allows the administrator to analyze network events. In-depth information and methodology can be found at

https://docs.zeek.org/en/master/scripting/basics.html#understanding-scripts.

At this point, you can use a SIEM (security information and event management) to analyze the data collected. In particular, most SIEMs that I've come across use the JSON file format and not TSV (which is the default log files). In fact, the produced logs are great, but visualizing them and analyzing them is a pain! This is where SIEMs come into the picture. SIEMs can analyze data in real-time. Further, there are many SIEMs available on the market, some are pricey, and some are open source. Which one you pick

is completely up to you, but one such open source SIEM that you might want to consider is Elastic Stack. But that's a lesson for another day.

Here are some sample SIEMs:

- OSSIM
- OSSEC
- SAGAN
- SPLUNK FREE
- SNORT
- ELASTICSEARCH
- MOZDEF
- ELK STACK
- WAZUH
- APACHE METRON

Configure Zeek To Detect Malware

Configuring Zeek to detect malware involves using its scripting capabilities to create or leverage existing scripts that focus on identifying patterns or behaviors associated with malicious activities. While Zeek itself doesn't detect malware directly, it's highly extensible, and you can enhance its capabilities through scripts.

Configuring Zeek to detect malware involves using its scripting capabilities to create or leverage existing scripts that focus on identifying patterns or behaviors associated with malicious activities. While Zeek itself doesn't detect malware directly, it's highly extensible, and you can enhance its capabilities through scripts.

Here are general steps to configure Zeek for malware detection:

1. Use Existing Scripts:

Zeek has an extensive community and a library of scripts that cover various use cases, including malware detection. You can explore the Zeek Package Manager for packages that suit your needs. These packages may include specific scripts for detecting malware patterns or behaviors.

2. Enable DNS Logging:

DNS can be a valuable source for detecting malware-related activities. Enable DNS logging in Zeek by configuring the dns.log script. In your local.zeek file or equivalent, include:

➜ @load protocols/dns/main

➜ redef Log::default_scope = Log::DNS;

This will log DNS activity, which can be used for identifying suspicious domains.

3. HTTP Logging:

If you have web traffic, enable HTTP logging in Zeek. Modify your local.zeek file:

➜ @load protocols/http/main

➜ redef Log::default_scope = Log::HTTP;

HTTP logs can reveal patterns associated with malware communication or compromised web servers.

4. File Extraction:

Configure Zeek to extract files from network traffic for further analysis. In your local.zeek file, include:

```
➜ @load base/files/extract
➜ redef FileExtract::prefix = "extracted";
```

This will extract files to the extracted directory. You can analyze these files for malware signatures or behaviors.

5. Signature-Based Detection:

Create custom signatures or use existing ones for detecting known malware patterns. Zeek supports signature-based detection through its sigs framework. Create a signature file (e.g., malware.sig) and load it in your local.zeek:

```
➜ @load base/protocols/sigs
➜ @load policy/protocols/conn-size
➜ redef ConnSize::default_threshold = 1000000; # Adjust threshold as needed

➜ redef sigs_detection_filter += {
        ["malware.sig"] = "Malware Detection",
};
```

6. Behavioral Analysis:

Leverage Zeek's scripting capabilities to create custom scripts that analyze network behavior for signs of compromise. Behavioral analysis can identify unusual patterns or anomalies.

7. Threat Intelligence Integration:

Integrate threat intelligence feeds into Zeek to enhance its detection capabilities. Zeek can use threat intelligence data to identify connections to known malicious IP addresses, domains, or URLs.

8. Regularly Update Signatures and Feeds:

Malware threats evolve rapidly, so it's crucial to keep your Zeek installation up-to-date with the latest threat intelligence feeds and signatures.

9. Logging and Analysis:

Log the relevant data and use external tools or platforms for in-depth analysis of the logs generated by Zeek. Tools like ELK Stack (Elasticsearch, Logstash, Kibana) can be useful for centralized logging and analysis.

10. Continuous Monitoring:

Implement continuous monitoring practices to quickly detect and respond to new threats. Regularly review Zeek logs for any suspicious or anomalous activities.

Remember that while Zeek is a powerful tool, it's just one component of a comprehensive cybersecurity strategy. Integrating Zeek with other security tools and practices is essential for building a robust defense against malware and other threats.

In order for the documents to be available and shareable in environments without internet, we will try to prepare some files in PDF format and put them on the site and the rest of the links related to KYGnus.

It is hoped that free access to information will be available for everyone.

If you are interested in these documents, you can donate to children with cancer or any other charity anywhere in the world.

Resources

https://zeek.org/

https://linuxhint.com/install-zeek-bro/

https://docs.zeek.org/en/master/

https://github.com/zeek/zeek

https://packages.zeek.org/

https://software.opensuse.org/download.html?project=security%3Azeek&package=zeek-lts

Contact :

➜ **KYGnus** : Koosha Yeganeh Gnu Linux Softwares

➜ **website** : https://kooshayeganeh.github.io/

➜ **GitHub** : https://github.com/KooshaYeganeh

➜ **GitLab** : https://gitlab.com/KooshaYeganeh

➜ **DockerHub** : https://hub.docker.com/u/kooshakooshadv

➜ **GitBook** : https://kooshayeganeh.gitbook.io/

➜ **Gmail** : kooshakooshadv@gmail.com