Nhóm 7

Zeek Scripting

B20DCAT090 - Nguyễn Mạnh Hưng
B20DCAT094 - Ninh Chí Hướng
B20DCAT098 - Hoàng Trung Kiên
B20DCAT102 - Nguyễn Văn Khang

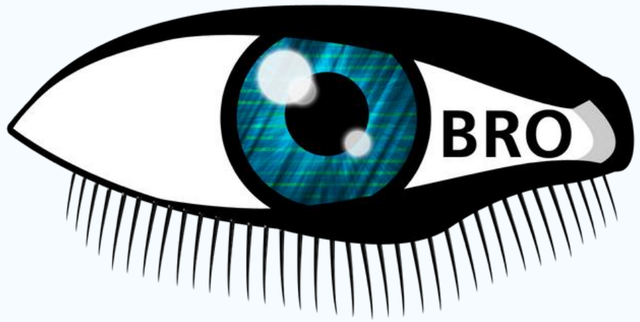
Nội dung

- Giới thiệu
- Kiến trúc
- Zeek Script
- Frameworks
- Demo

Giới thiệu

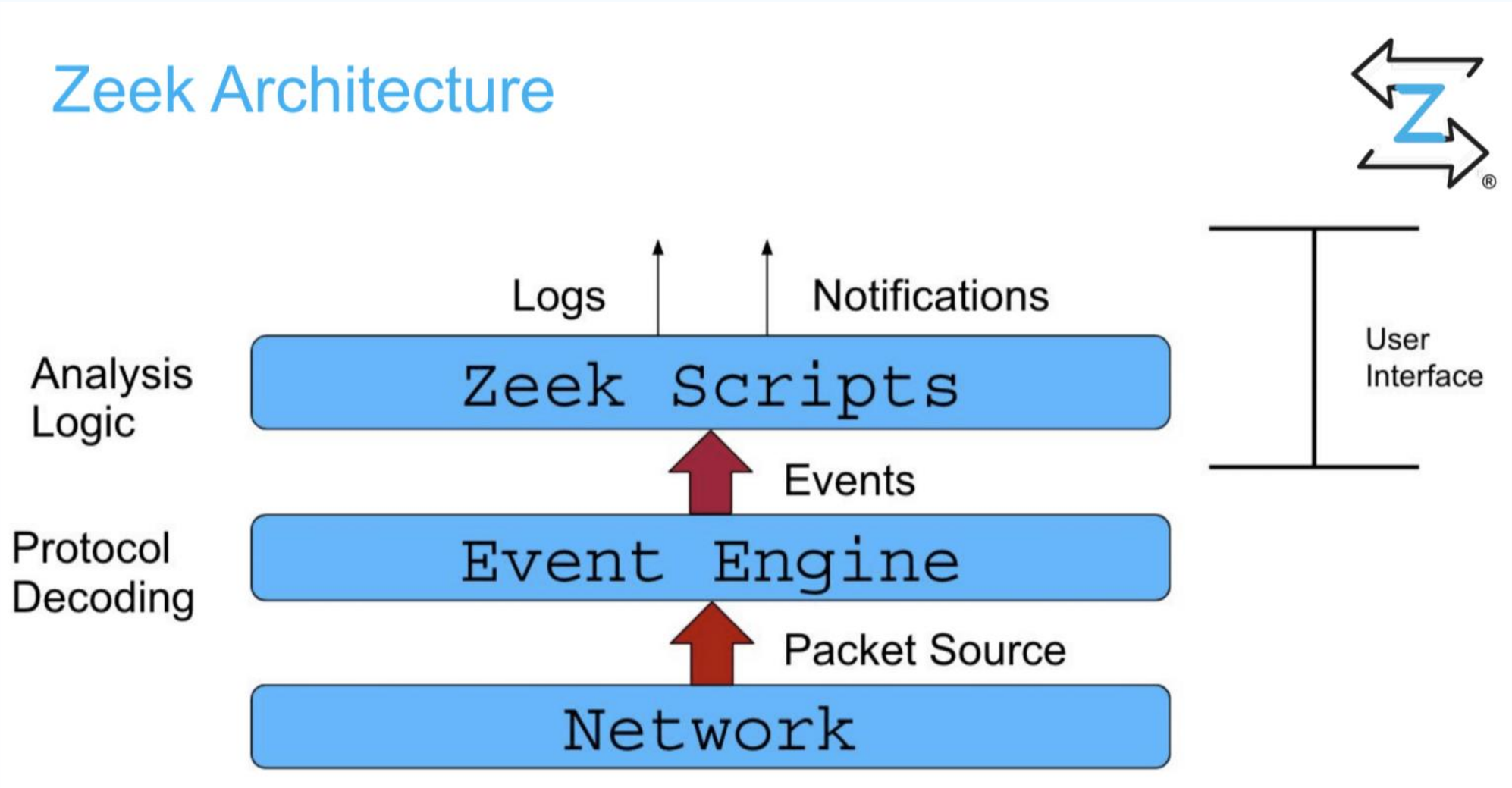
1. Giới thiệu

- **Zeek** (trước đây được gọi là Bro) là một công cụ phân tích lưu lượng mạng mã nguồn mở thụ được phát triển bởi Lawrence Berkeley Labs.
- **Zeek scripting** là một ngôn ngữ kịch bản được thiết kế riêng cho việc phân tích và giám sát mạng. Cho phép bạn viết các tập lệnh để trích xuất dữ liệu từ lưu lượng mạng, phát hiện các mối đe dọa bảo mật và thực hiện các tác vụ tự động hóa.



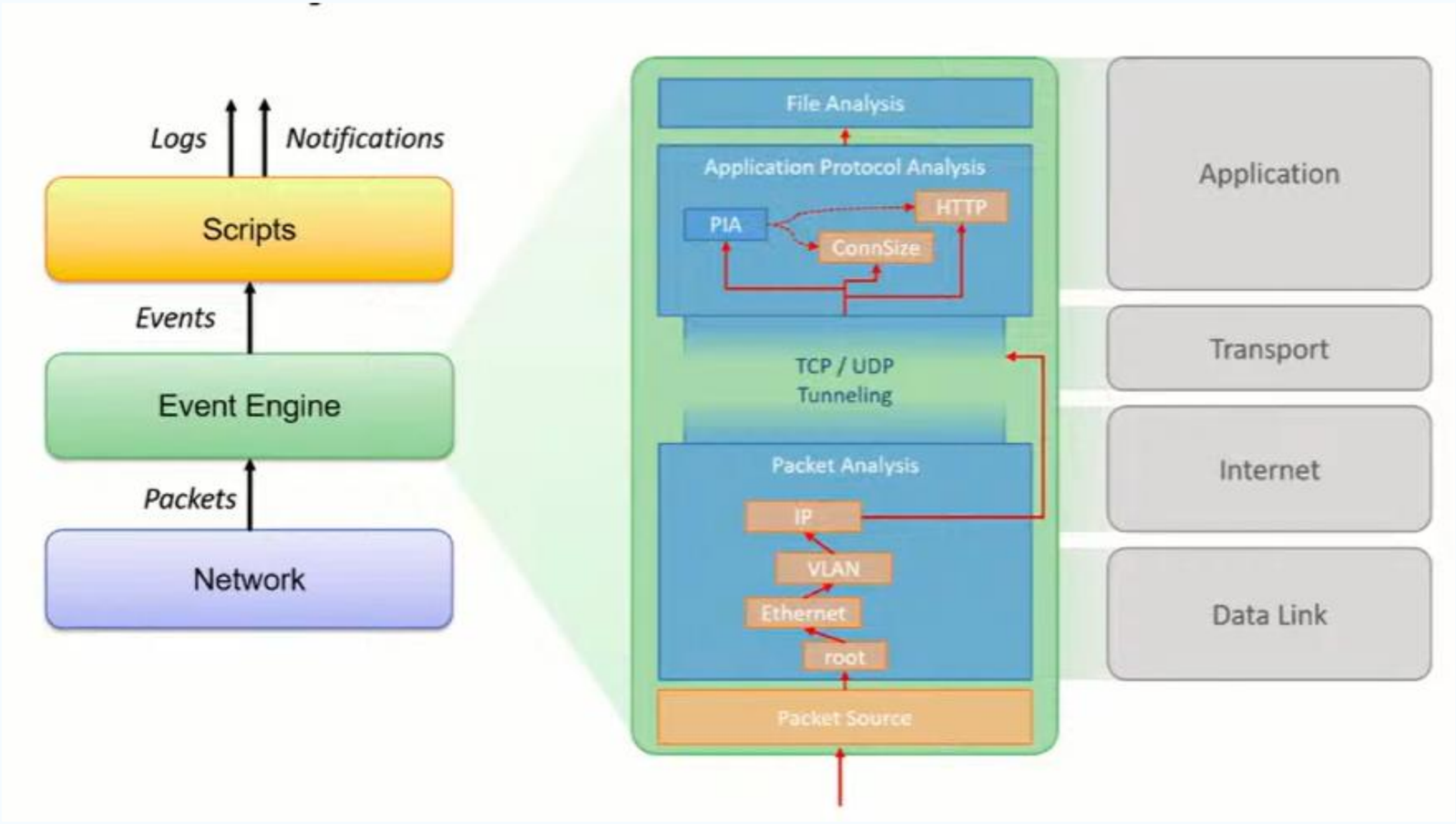
Kiến trúc

2. Kiến trúc


Zeek Architecture
Logs
Notifications
Analysis Logic
Zeek Scripts
User Interface
Events
Protocol Decoding
Event Engine
Packet Source
Network

2. Kiến trúc

- Input sources
- Packet analysis
- Session analysis
- And file analysis



Zeek Script

3. Zeek Script

```
##! Detect various potentially bad FTP activities.

@load base/frameworks/notice
@load base/protocols/ftp

module FTP;

export {
        redef enum Notice::Type += {
                ## Indicates that a successful response to a "SITE EXEC"
                ## command/arg pair was seen.
                Site_Exec_Success,
        };
}

event ftp_reply(c: connection, code: count, msg: string, cont_resp: bool) &priority=3
        {
        local response_xyz = parse_ftp_reply_code(code);

        # If a successful SITE EXEC command is executed, raise a notice.
        if ( response_xyz$x == 2 &&
             c$ftp$cmdarg$cmd == "SITE" &&
             /[Ee][Xx][Ee][Cc]/ in c$ftp$cmdarg$arg )
                {
                NOTICE([$note=Site_Exec_Success, $conn=c,
                        $msg=fmt("FTP command: %s %s", c$ftp$cmdarg$cmd, c$ftp$cmdarg$arg),
                        $identifier=cat(c$id$orig_h, c$id$resp_h, "SITE EXEC")]);
                }
        }
```

Có ba phần riêng biệt của ZeekScripting.

- Đầu tiên, khai báo thư viện thông qua @load và Namespace với module.
- Tiếp theo là phần giải thích các biến tùy chỉnh (export) như một phần của script’s namespace.
- Cuối cùng, mô tả các hướng dẫn cần thực hiện cho một sự kiện cụ thể event ftp_reply( ).

Framework

4. Framework

Zeek bao gồm một số Framework cung cấp chức năng thường được sử dụng cho lớp Scripts.

- Broker Communication Framework
- Cluster Framework
- Configuration Framework
- File Analysis Framework
- Input Framework
- Intelligence Framework
- Logging Framework
- Management Framework
- NetControl Framework
- Notice Framework
- Packet Analysis
- Signature Framework
- Summary Statistics
- Supervisor Framework
- Telemetry Framework
- TLS Decryption

Example:
Notice Framework

Action	Description
`Notice::ACTION_LOG`	Write the notice to the `Notice::LOG` logging stream.
`Notice::ACTION_ALARM`	Log into the `Notice::ALARM_LOG` stream which will rotate hourly and email the contents to the email address or addresses in the *email_dest* field of that notice's `Notice::Info` record.
`Notice::ACTION_EMAIL`	Send the notice in an email to the email address or addresses in the *email_dest* field of that notice's `Notice::Info` record.
`Notice::ACTION_PAGE`	Send an email to the email address or addresses in the *email_dest* field of that notice's `Notice::Info` record.

```
@load protocols/ssh/detect-bruteforcing

redef SSH::password_guesses_limit=10;

hook Notice::policy(n: Notice::Info)
    {
    if ( n$note == SSH::Password_Guessing && /192\.168\.56\.103/ in n$sub )
        {
        add n$actions[Notice::ACTION_EMAIL];
        n$email_dest = "ssh_alerts@example.net";
        }
    }
```

References

More Zeek Resources

Zeek Documentation:
https://docs.zeek.org/en/master/
Zeek packages:
https://packages.zeek.org/packages
Zeek btest pcaps:
https://github.com/zeek/zeek/tree/master/testing/btest/Traces
Zeek Github source:
https://github.com/zeek/zeek
Zeek online:
https://try.zeek.org/#/?example=hello

Demo


Thank
You