Welcome to

Network Tapping

PROSA SURVEIL_IT

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github
surveil_it-workshop.tex in the repo security-courses

Goal

Don’t Panic!

Spend some time sniffing data, multiple tools:

Try different ways to sniff packets

Try The Zeek Network Security Monitor

How to get started using packet capture tools in a network

We try to do a lot, feel free to focus on specific parts

Packet sniffing tools

Tcpdump for capturing packets

Wireshark for dissecting packets manually with GUI

Zeek Network Security Monitor for automated dissection

Often a combination of tools and methods used in practice

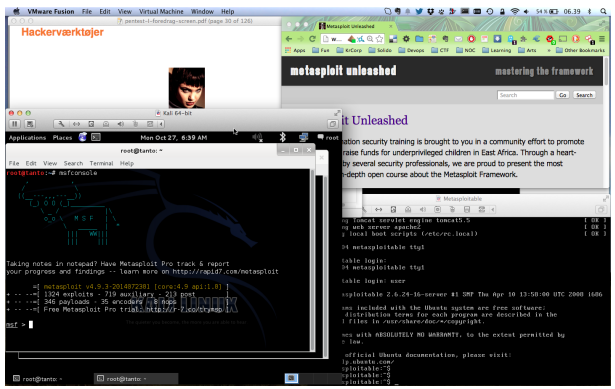
Full packet capture big data tools also exist

Kali Linux the pentest toolbox

Kali `http://www.kali.org/` brings together 100s of tools

100.000s of videos on YouTube alone, searching for kali and $TOOL

Hackerlab setup



- Hardware: most modern laptop CPUs have virtualization support
  May need to enable it in BIOS
- Virtualization software: VMware, Virtual box, choose your poison
- Hackersoftware: Kali as a Virtual Machine `https://www.kali.org/`
- Install sniffing VM - put into *bridge mode* or use USB Ethernet

Your lab setup

- Go to GitHub, Find user Kramse, click through security-courses, courses, network, surveil_it and download the PDF files for the slides and exercises:

  `https://github.com/kramse/security-courses/tree/master/courses/networking/surveil_it`

- And if you want to go full-blown and run your own Zeek then also get the lab instructions, from:

  `https://github.com/kramse/kramse-labs/tree/master/suricatazeek`

  We recommend working in groups and all exercises are optional ☺

What happens today?

Think like a blue team member find traffic

Get basic tools running

Improve situation

- See where the data end up
- What kind of data and metadata can we extract
- How can we collect and make use of it
- Databases and web interfaces, examples shown
- Consider what your deployment could be

Today focus on the lower parts, but user interfaces are important too

Security devops

We need devops skillz in security

automate, security is also big data

integrate tools, transfer, sort, search, pattern matching, statistics, ...

tools, languages, databases, protocols, data formats

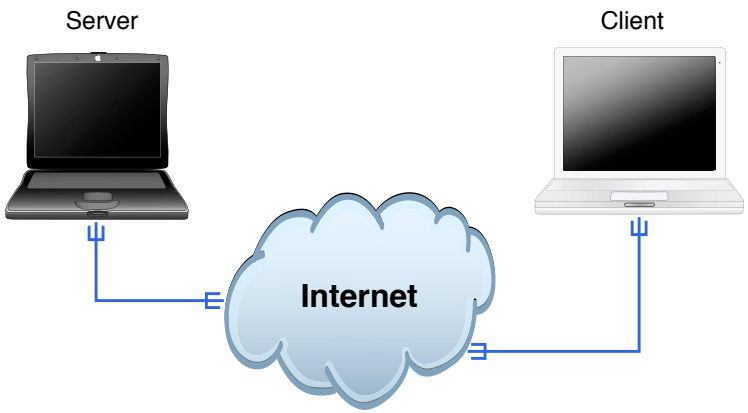
Use GitHub! So many libraries and programs that can help, maybe solve 90% of your problem, and you can glue the rest together

Example introductions:

- Seven languages/database/web frameworks in Seven Weeks
- Elasticsearch the definitive guide

We are all Devops now, even security people!

Internet today



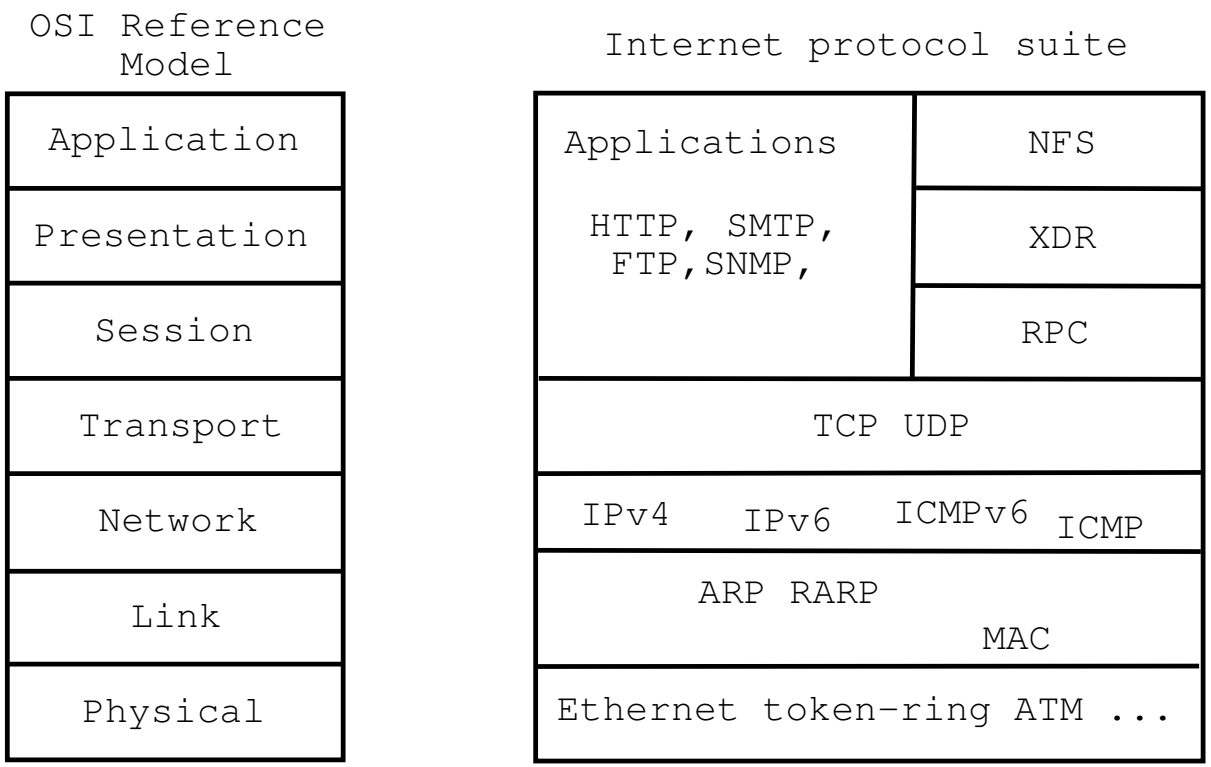
Clients and servers

Roots in academia

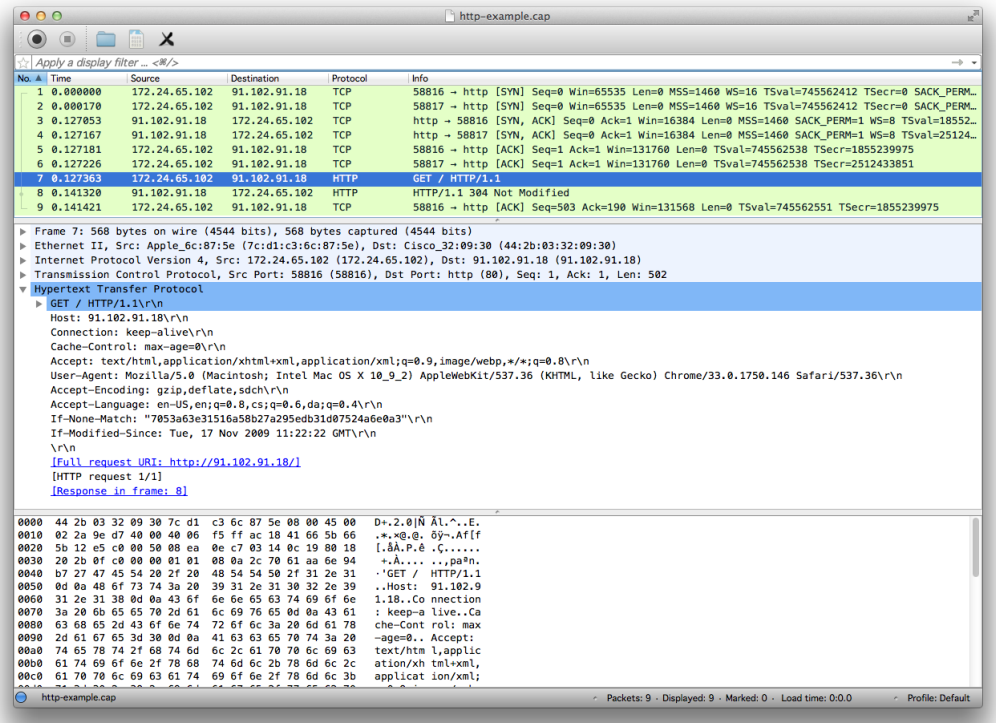
Protocols more than 20 years old

HTTP is becoming encrypted, but a lot other traffic is not

OSI and Internet models

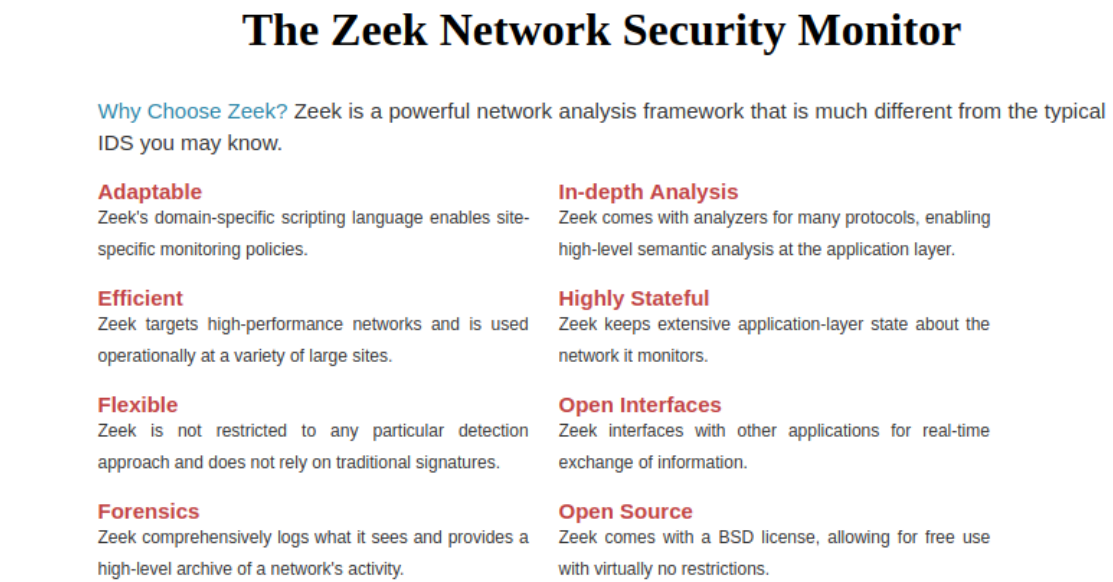


Using Wireshark



https://www.wireshark.org

The Zeek Network Security Monitor



The Zeek Network Security Monitor

Why Choose Zeek? Zeek is a powerful network analysis framework that is much different from the typical IDS you may know.

Adaptable
Zeek's domain-specific scripting language enables site-specific monitoring policies.

Efficient
Zeek targets high-performance networks and is used operationally at a variety of large sites.

Flexible
Zeek is not restricted to any particular detection approach and does not rely on traditional signatures.

Forensics
Zeek comprehensively logs what it sees and provides a high-level archive of a network's activity.

In-depth Analysis
Zeek comes with analyzers for many protocols, enabling high-level semantic analysis at the application layer.

Highly Stateful
Zeek keeps extensive application-layer state about the network it monitors.

Open Interfaces
Zeek interfaces with other applications for real-time exchange of information.

Open Source
Zeek comes with a BSD license, allowing for free use with virtually no restrictions.

The Zeek Network Security Monitor is not a single tool, more of a powerful network analysis framework (former name Bro)

Source `https://www.zeek.org/`, redirects to `https://www.bro.org/zeek.html`

Exercise setup

We will use a combination of your virtual servers, my switch hardware and my virtual systems.

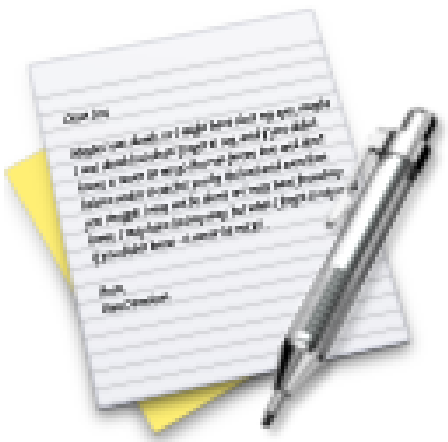
There will be sniffing done on traffic!
Don't abuse information gathered

We try to mimic what you would do in your own networks during the exercises.

Another way of running exercises might be:
`https://github.com/jonschipp/ISLET`

Recommended and used by Zeek and Suricata projects.

Exercise

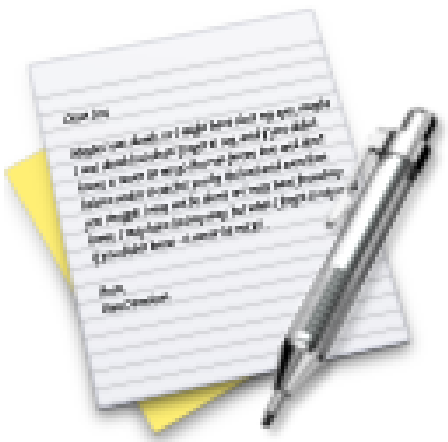


Now lets do the exercise

Wireshark and tcpdump 15min

which is number 1 in the exercise PDF.

Exercise

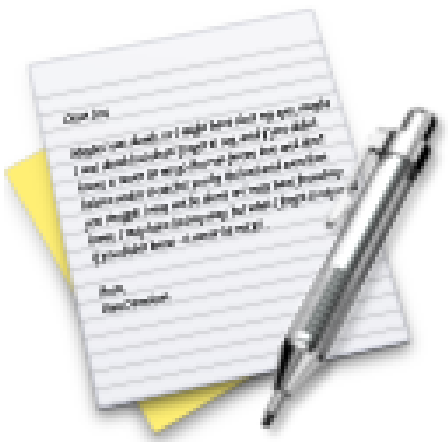


Now lets do the exercise

Capturing network packets 15min

which is number 2 in the exercise PDF.

Exercise



Now lets do the exercise

Zeek on the web 15min

which is number 3 in the exercise PDF.

Questions?

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Need help with infrastructure security or pentesting, ask me!

You are always welcome to send me questions later via email