Welcome to

10. Network Attacks

KEA Kompetence OB2 Software Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github
10-network-attacks.tex in the repo security-courses

Plan for today

Subjects

- Auditing Application Protocols
- Example protocols and vulnerabilities
- Abstract Syntax Notation (ASN.1) problems
- Domain Name System (DNS) problems

Exercises

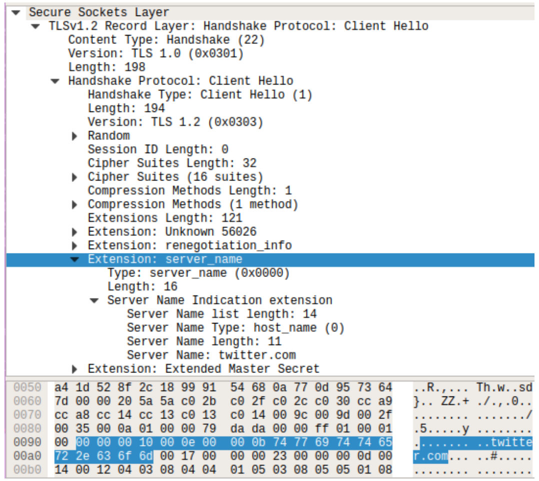
- Examples from AoSSA chapters 17 and 18

Reading Summary

AoSSA chapter 16: Network Application Protocols

Will also use examples from chapters 17: Web Applications, 18: Web Technologies so browse Table of Contents for those.

Goals: Introduction to Auditing Application Protocols



```
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 198
    ▾ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 194
        Version: TLS 1.2 (0x0303)
      ▸ Random
        Session ID Length: 0
        Cipher Suites Length: 32
      ▸ Cipher Suites (16 suites)
        Compression Methods Length: 1
      ▸ Compression Methods (1 method)
        Extensions Length: 121
      ▸ Extension: Unknown 56026
      ▸ Extension: renegotiation_info
      ▾ Extension: server_name
          Type: server_name (0x0000)
          Length: 16
        ▾ Server Name Indication extension
            Server Name list length: 14
            Server Name Type: host_name (0)
            Server Name length: 11
            Server Name: twitter.com
      ▸ Extension: Extended Master Secret
0050  a4 1d 52 8f 2c 18 99 91  54 68 0a 77 0d 95 73 64   ..R.,... Th.w..sd
0060  7d 00 00 20 5a 5a c0 2b  c0 2f c0 2c c0 30 cc a9   }.. ZZ.+ ./.,.0..
0070  cc a8 cc 14 cc 13 c0 13  c0 14 00 9c 00 9d 00 2f   ........ ......./
0080  00 35 00 0a 01 00 00 79  da da 00 00 ff 01 00 01   .5.....y ........
0090  00 00 00 00 10 00 0e 00  00 0b 74 77 69 74 74 65   ........ ..twitte
00a0  72 2e 63 6f 6d 00 17 00  00 00 23 00 00 00 0d 00   r.com... ..#.....
00b0  14 00 12 04 03 08 04 04  01 05 03 08 05 05 01 08   ........ ........
```

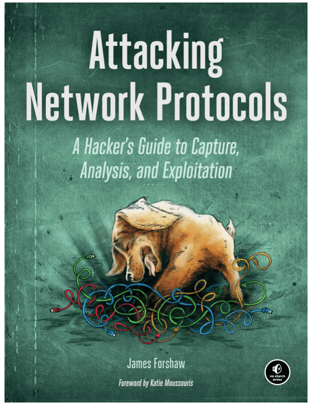
Often you dont need to audit the whole protocol in detail

Sometimes people can't tell which protocols, ports and services they use ...

And you need to configure a firewall/network filter

Picture: Wireshark with TLS SNI, recent Exim CVE-2019-15846 was SNI parsing

Reversing and Attacking Network Protocols


Attacking Network Protocols
A Hacker's Guide to Capture, Analysis, and Exploitation
James Forshaw
Foreword by Katie Moussouris

A method with lots detail can be found in the book,
Attacking Network Protocols A Hacker's Guide to Capture, Analysis, and Exploitation
by James Forshaw December 2017, 336 pp. ISBN-13: 9781593277505

`https://nostarch.com/networkprotocols`

Auditing Application Protocols

- Collect documentation
- Identify Elements of Unknown Protocols
- Use packet sniffers, tcpdump and Wireshark
- Initiate the Connection Several Times
- Replay traffic, can sometimes replay even encrypted traffic, see wireless WEP attacks

Note: We investigate protocols, so we can see what is sent, so we can design *payloads* which create problems for implementations - applications

Reverse Engineer Applications

```
(gdb) disas main
Dump of assembler code for function main:
   0x0000000000000580 <+0>: lea    0x1ed(%rip),%rdi        # 0x774
   0x0000000000000587 <+7>: sub    $0x8,%rsp
   0x000000000000058b <+11>: mov    $0x7fff,%esi
   0x0000000000000590 <+16>: xor    %eax,%eax
   0x0000000000000592 <+18>: callq  0x560 <printf@plt>
   0x0000000000000597 <+23>: lea    0x1ed(%rip),%rdi        # 0x78b
   0x000000000000059e <+30>: mov    $0xffff8000,%esi
   0x00000000000005a3 <+35>: xor    %eax,%eax
   0x00000000000005a5 <+37>: callq  0x560 <printf@plt>
   0x00000000000005aa <+42>: xor    %eax,%eax
   0x00000000000005ac <+44>: add    $0x8,%rsp
   0x00000000000005b0 <+48>: retq
End of assembler dump.
```

- It is possible to debug, disassemble and reverse engineer applications
- Calling socket functions, seeing structs, data types etc.
- Examine strings: HTTP, FTP, SMTP etc. all uses semi-english words GET, EHLO, PASS

Special values

- Examine special values
- What are the defined/used values
- What happens if this is changed? Do they cover values outside of the used ranges? Case/switch constructs
- Use trace functions in the operating system, can capture, analyze and replay sometimes

Buffer Overflow when receiving

- When you see data enter the application, identify functions
- Consider if they use dangerous functions, strcpy and friends
- How much space is available, allocated etc.
- Basic stuff and similar across applications

- Repeat everything we learned about string processing, integeroverflows/underflows etc. Just from the network
- Often trying to abuse will lead to denial of service

- If some rock solid service starts bouncing down and up, maybe look into traffic received.
- This is what honeypots also do

Vigtigste protokoller

ARP Address Resolution Protocol

IP og ICMP Internet Control Message Protocol

UDP User Datagram Protocol

TCP Transmission Control Protocol

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

Ovenstående er omtrent minimumskrav for at komme på internet

Binary Protocols

- Some protocols use binary formats
- Example DNS, which is a complex protocol
- When parsing DNS use standard libraries!
- When attacking DNS applications, use standard libraries! ☺
- DNS is just an example, new protocols may not be implemented - but someone might have analyzed it or parts already!

Network Authentication

> **IPMI Authentication Bypass via Cipher 0**
> Dan Farmer identified a serious failing of the IPMI 2.0 specification, namely that cipher type 0, an indicator that the client wants to use clear-text authentication, actually allows access with any password. Cipher 0 issues were identified in HP, Dell, and Supermicro BMCs, with the issue likely encompassing all IPMI 2.0 implementations. It is easy to identify systems that have cipher 0 enabled using the `ipmi_cipher_zero` module in the Metasploit Framework.

- Sometimes people add network functionality to existing applications
- - and do this badly
- We have seen applications like IPMI and others

Source: `https://blog.rapid7.com/2013/07/02/a-penetration-testers-guide-to-ipmi/`

Book uses ISAKMP example

- IKE(v1) has been critized as being overly complex
- Needed bake-off sessions where vendors meet and tried negotiating
- Searching for CVE ISAKMP show multiple vulnerabilities in various implementations, including firewalls and tcpdump
- AoSSA chapter 16: Network Application Protocols

Exercise

Now lets do the exercise

Sniff Your Browser 15min

which is number **27** in the exercise PDF.

ASN.1 problems

- Abstract format designed for representing objects in a machine independent format
- Used for various technologies in use on the internet:
- Certificates and key encoding
- Simple Network Management Protocol (SNMP)
- ISAKMP part of IPsec
- Lightweight Directory Access Protocol (LDAP)

Linux Kernel ASN.1

- CVE-2016-0758 Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via crafted ASN.1 data.
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0758
- Linux kernel have about 5 ASN.1 parsers
  https://www.x41-dsec.de/de/lab/blog/kernel_userspace/

Type Length Value TLVs

> TLV sequences are easily searched using generalized parsing functions; New message elements which are received at an older node can be safely skipped and the rest of the message can be parsed. This is similar to the way that unknown XML tags can be safely skipped; TLV elements can be placed in any order inside the message body; TLV elements are typically used in a binary format which makes parsing faster and the data smaller than in comparable text based protocols.

Source: `https://en.wikipedia.org/wiki/Type-length-value`

- Type Length Value is an encoding used in data communication
- For example in Link Layer Discovery Protocol (LLDP)

Cisco Application Centric Infrastructure, aka Security Device

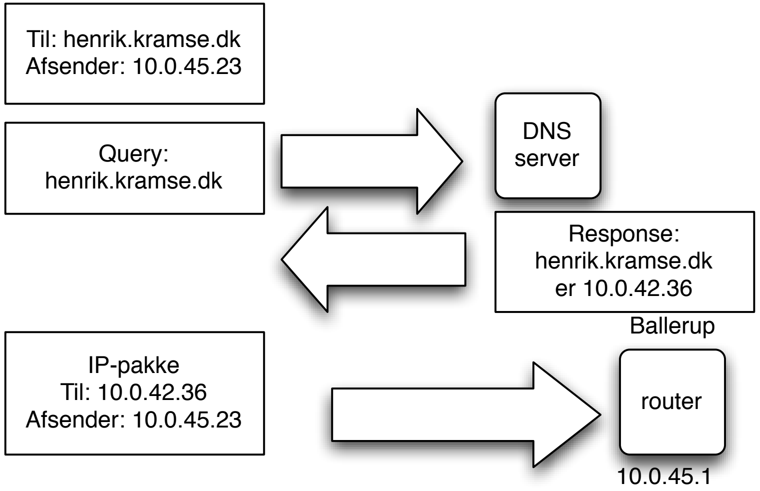
> The first time an APIC gets physically connected to one of the leaf switches of an ACI fabric, it will initiate a configuration process for the switches. The initial packets sent by the APIC are Link Layer Discovery Protocol (LLDP) packets containing information that is used by the leaf switch to initiate the configuration process. The LLDP protocol is used to advertise the identity, capabilities and certain other parameters of the APIC via TypeLength-Value (TLV) fields.

ERNW WHITEPAPER 68, SECURITY ASSESSMENT OF CISCO ACI, 2019

`https://static.ernw.de/whitepaper/ERNW_Whitepaper68_Vulnerability_Assessment_Cisco_ACI_signed.pdf`

- Cisco Nexus 9000 Series Fabric Switches ACI Mode Fabric Infrastructure VLAN Unauthorized Access Vulnerability (CVE-2019-1890)
- Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure Mode Link Layer Discovery Protocol Buffer Overflow Vulnerability (CVE-2019-1901)

Domain Name System



Gennem DHCP får man typisk også information om DNS servere

En DNS server kan slå navne, domæner og adresser op

Foregår via query og response med datatyper kaldet resource records

DNS er en distribueret database, så opslag kan resultere i flere opslag

DNS systemet

navneopslag på Internet

tidligere brugte man en **hosts** fil
hosts filer bruges stadig lokalt til serveren - IP-adresser

UNIX: /etc/hosts

Windows `c:\windows\system32\drivers\etc\hosts`

Eksempel: www.zencurity.com har adressen 185.129.60.130

skrives i database filer, zone filer

```
ns1     IN      A       185.129.60.130
        IN      AAAA    2a06:d380:0:3065::53
www     IN      A       185.129.60.130
        IN      AAAA    2a06:d380:0:3065::80
```

Mere end navneopslag

består af resource records med en type:

- IPv4 adresser A-records
- IPv6 adresser AAAA-records
- autoritative navneservere NS-records
- post, mail-exchanger MX-records
- flere andre: md , mf , cname , soa , mb , mg , mr , null , wks , ptr , hinfo , minfo , mx ....

```
IN      MX      10      mail.zencurity.com.
IN      MX      20      mail2.zencurity.com.
```

BIND DNS server

Berkeley Internet Name Daemon server

Mange bruger BIND fra Internet Systems Consortium - altså Open Source

konfigureres gennem `named.conf`

det anbefales at bruge BIND version 9

- Biblen omkring DNS og BIND er:
  DNS and BIND, Paul Albitz & Cricket Liu, O'Reilly, 5th edition Maj 2006
- BIND has had sooo many vulnerabilities across versions and releases

Unbound and NSD

> Unbound is a validating, recursive, caching DNS resolver. It is designed to be fast and lean and incorporates modern features based on open standards.
>
> To help increase online privacy, Unbound supports DNS-over-TLS which allows clients to encrypt their communication. In addition, it supports various modern standards that limit the amount of data exchanged with authoritative servers.

`https://www.nlnetlabs.nl/projects/unbound/about/`

My preferred local DNS server. We will now stop and look at this configuration file and function.

Also check out uncensored DNS and his DNS over TLS setup!
Even has pinning information available:
`https://blog.censurfridns.dk/blog/32-dns-over-tls-pinning-information-for-unicastcensurfridnsdk/`

DNS problems

> The Domain Name System (DNS) [32][33] provides for a distributed database mapping host names to IP addresses. An intruder who interferes with the proper operation of the DNS can mount a variety of attacks, including denial of service and password collection. There are a number of vulnerabilities.

We have a lot of the same problems in DNS today

Plus some more caused by middle-boxes, NAT, DNS size, DNS inspection

- DNS must allow both UDP and TCP port 53
- Your DNS servers must have updated software, see DNS flag day https://dnsflagday.net/ after which kludges will be REMOVED!
- DNS is unencrypted

DNS over TLS vs DNS over HTTPS - DNS encryption

Protocols exist that encrypt DNS data, like dnscrypt which is not RFC standard `https://dnscrypt.info/` `https://en.wikipedia.org/wiki/DNSCrypt`

Today we have competing standards:

Specification for DNS over Transport Layer Security (TLS) (DoT), RFC 7858 MAY 2016 `https://en.wikipedia.org/wiki/DNS_over_TLS`

DNS Queries over HTTPS (DoH) RFC 8484

How to cofigure DoT `https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients`

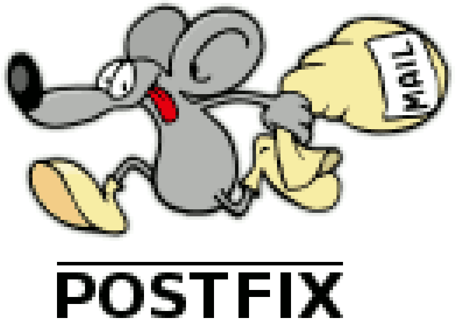
DNS problems

- From the book: AoSSA chapter 16: Network Application Protocols
- Failure to Deal with Invalid Label Lengths
- Insufficient Destination Lengths Check
- Insufficient Source Length Checks
- Pointer Values Not Verified In Packet
- Special Pointer Values
- Length Variables

- Labels and pointers within packets save bytes, but make it more complex!

Does anything sound familiar?

Postfix postserveren



Lavet af Wietse Venema for IBM

Nem at konfigurere og sikker

`main.cf` findes typisk i kataloget `/etc/postfix`

Audit af postservere

Typisk findes konfigurationsfilerne til postservere under `/etc`

- `/etc/mail`
- `/etc/postfix`

Det vigtigste er at den er opdateret og IKKE tillader relaying

Der findes diverse test-scripts til relaycheck på internet

Husk også at checke domæne records, MX og A

Test af e-mail server

```
[hlk]$  telnet localhost 25
Connected.
Escape character is '^]'.
220 server ESMTP Postfix
 helo test
250 server
 mail from: postmaster@pentest.dk
250 Ok
 rcpt to: root@pentest.dk
250 Ok
 data
354 End data with <CR><LF>.<CR><LF>
 skriv en kort besked
.
250 Ok: queued as 91AA34D18
 quit
```

Skal ikke tillade relaying, og vil blive misbrugt meget hurtigt.

Idag benyttes ofte en stjålet brugerkonto med brugernavn og kodeord til at sende spam.

For Next Time

Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books
Most days have less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools

Buy the books!