MP4: Checkpoint 2

CS461 / ECE422 – UIUC Spring 2016

Simon Kim

Introduction

- 4.2.1. Network attacks
  - Crack the wireless network password (WEP)
  - Sniff and analyze the network
  - Obtain a client’s login credentials
- 4.2.2. Anomaly (port scanning) detection
  - Write a program that takes a pcap filename as an argument and checks TCP flag bits to detect port scanning.

Network attacks

- Read the recommended setup provided in the MP document
  - Use Kali Linux 32 bit
- Kali Linux comes pre-installed with tools you need
  - Aircrack-ng Suite
  - Nmap
  - Wireshark

Network attacks: WEP crack

- Aircrack-ng Suite includes:
  - Airmon-ng - Enable and disable monitor mode on wireless interfaces.
  - Aireplay-ng - Inject and replay wireless frames.
  - Airodump-ng - Capture raw 802.11 frames.
  - Aircrack-ng - 802.11 WEP and WPA/WPA2-PSK key cracking program.
  - More details: http://www.aircrack-ng.org/documentation.html
- WEP crack tutorial: http://www.aircrack-ng.org/doku.php?id=simple_wep_crack

Network attacks: WEP crack

DO NOT USE

- Aircrack-ng Suite includes:
  - Airmon-ng - Enable and disable monitor mode on wireless interfaces.
  - ~~Aireplay-ng - Inject and replay wireless frames.~~
  - Airodump-ng - Capture raw 802.11 frames.
  - Aircrack-ng - 802.11 WEP and WPA/WPA2-PSK key cracking program.
  - More details: http://www.aircrack-ng.org/documentation.html
- WEP crack tutorial: http://www.aircrack-ng.org/doku.php?id=simple_wep_crack
  - Skip any step that uses aireplay-ng.

Wireless network terms

- BSSID – the MAC address of the wireless access point (https://en.wikipedia.org/wiki/Service_set_(802.11_network)#Basic_service_set_identification_.28BSSID.29)
- ESSID – a ID for a set of two or more interconnected wireless BSSs with the same network name (https://en.wikipedia.org/wiki/Service_set_(802.11_network)#Extended_service_set)
- Channel # - the number of the channel that a wireless network is configured to use for communication (https://en.wikipedia.org/wiki/List_of_WLAN_channels)
  - Our network uses 2.4GHz range only.
- # IV (data/packet) - the number of initialization vectors gathered (https://en.wikipedia.org/wiki/Initialization_vector#WEP_IV)

Airmon-ng

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# airmon-ng start wlan0
No interfering processes found
PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)


root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0mon  IEEE 802.11bgn  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

lo        no wireless extensions.

root@kali:~#
```

Source: https://www.kali.org/penetration-testing/pixiewps-reaver-aircrack-ng-updates/

Airodump-ng

```
CH 11 ][ Elapsed: 24 s ][ 2014-11-21 09:39

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:25:9C:97:4F:48  -33       20       14    0   9  54e. WPA2 CCMP   PSK  Mande
78:CD:8E:3B:B7:0B  -47       14        0    0   1  54e  WPA2 CCMP   PSK  <leng
78:CD:8E:3B:B7:09  -42       13        0    0   1  54e  WPA2 CCMP   PSK  <leng
78:CD:8E:3B:B7:0A  -42       12        0    0   1  54e  WPA2 CCMP   PSK  <leng
78:CD:8E:3B:B7:08  -44       14        2    0   1  54e  WPA2 CCMP   PSK  TheDr
B0:C7:45:75:13:9E  -58        4        0    0   9  54e. WPA2 CCMP   PSK  tedpe

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:C0:CA:3F:EE:02    0    0 - 1      0       11
00:25:9C:97:4F:48  00:1E:8F:8D:18:25  -17    0 -36      0       10
B0:C7:45:75:13:9E  10:A5:D0:F5:31:19  -51    0 - 6      0        1
```

Source: http://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/

Aircrack-ng

```
root@kali: ~
File  Edit  View  Search  Terminal  Help

                              Aircrack-ng 1.2 rc1


                [00:04:26] Tested 802 keys (got 32515 IVs)

   KB    depth   byte(vote)
    0    3/  5   22(38144) FA(37888) 57(37632) 1F(37376) D2(37376)
    1    8/  1   48(38400) 02(38144) 3C(38144) C8(37888) AC(37632)
    2    0/  2   4C(45568) 85(40704) 0F(39424) 19(39168) 31(38912)
    3   31/  3   CD(36096) 80(35840) D5(35840) DA(35840) 21(35584)
    4    0/  4   30(45056) 36(40192) 6F(40192) 57(39680) 4C(38912)

     KEY FOUND! [ 74:65:73:74:70:61:73:73:64:61:79:6F:6E ] (ASCII: testpassdayon
 )
        Decrypted correctly: 100%


root@kali:~#
```

Source: http://nvnote.com/wep-crack-kalilinux/

Sidenote: promiscuous vs. monitor

- Promiscuous mode: sniffing after connecting to the access point, becoming part of the network
- Monitor mode: sniffing without connecting to the access point
- https://wiki.wireshark.org/CaptureSetup/WLAN
- http://security.stackexchange.com/questions/36997/what-is-the-difference-between-promiscuous-and-monitor-mode-in-wireless-networks
- http://lazysolutions.blogspot.ca/2008/10/difference-promiscuous-vs-monitor-mode.html

Network attacks: network analysis

- How many hosts are there?
- Which one is the server?
- What services are present on the network?
- Use Wireshark to identify hosts and analyze live traffics
- Use nmap (network mapper) to obtain more details on hosts
- Your own interpretation of network behavior
  - Don’t rely on one result. See if other findings agree with what you observe.
  - For example, how is your IP address assigned? Static? DHCP? Can you confirm this in anyway?

Nmap

```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-19 16:44 IST
Interesting ports on 192.168.1.1:
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: BC:AE:C5:C3:16:93 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

- Open/closed/filtered ports - https://nmap.org/book/man-port-scanning-basics.html
- Port scanning techniques - https://nmap.org/book/man-port-scanning-techniques.html
- Don’t forget about UDP.
- Our network has no services running above port 4096.

Source: http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/

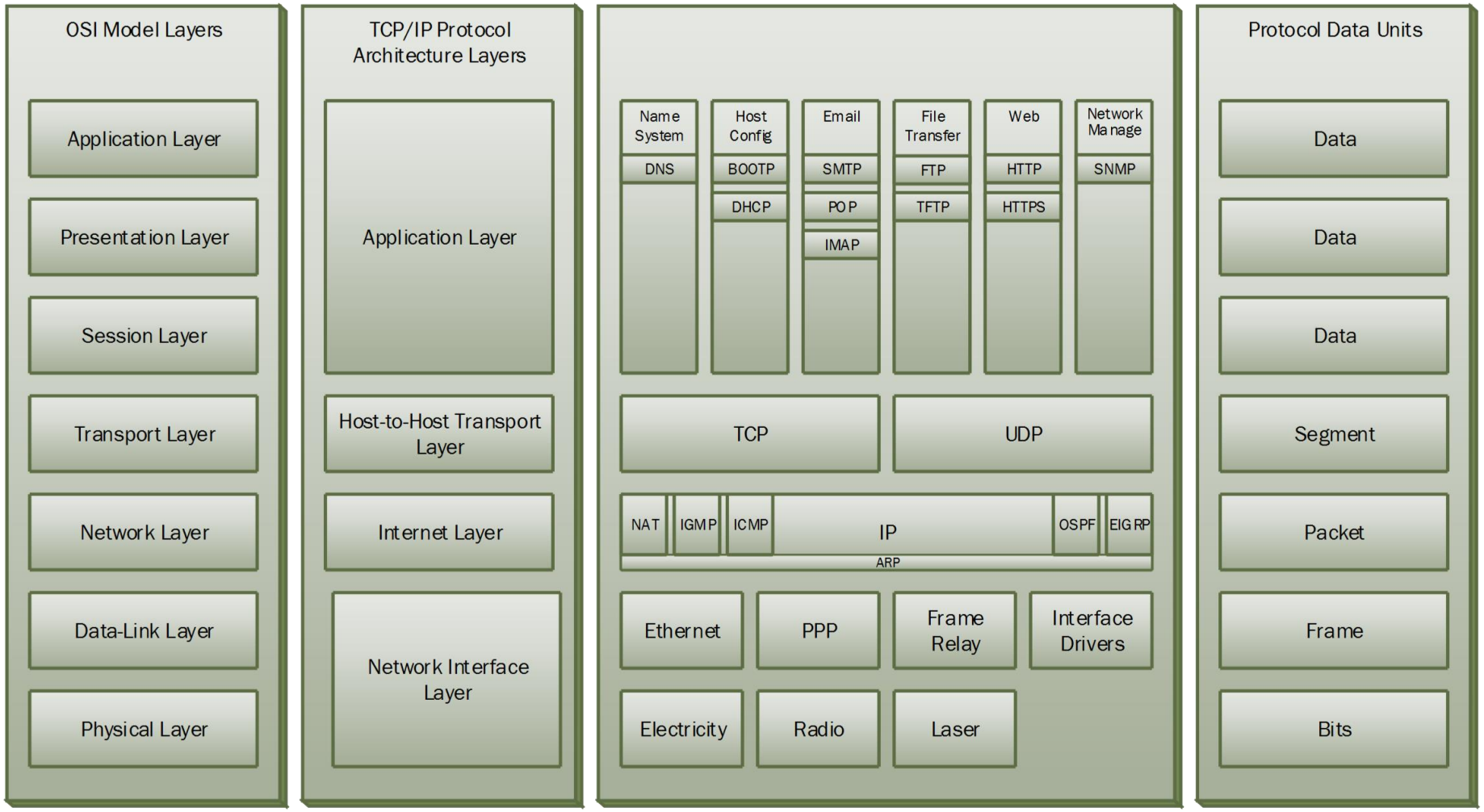
Network attacks: information retrieval

- Client’s login credential is sent over HTTPS
- What do you need to decrypt the content?
- Is it available anywhere accessible?
- No need to perform any sort of attack
- Be curious about what you find.
  - What is it used for?
  - How is it used?

Anomaly detection

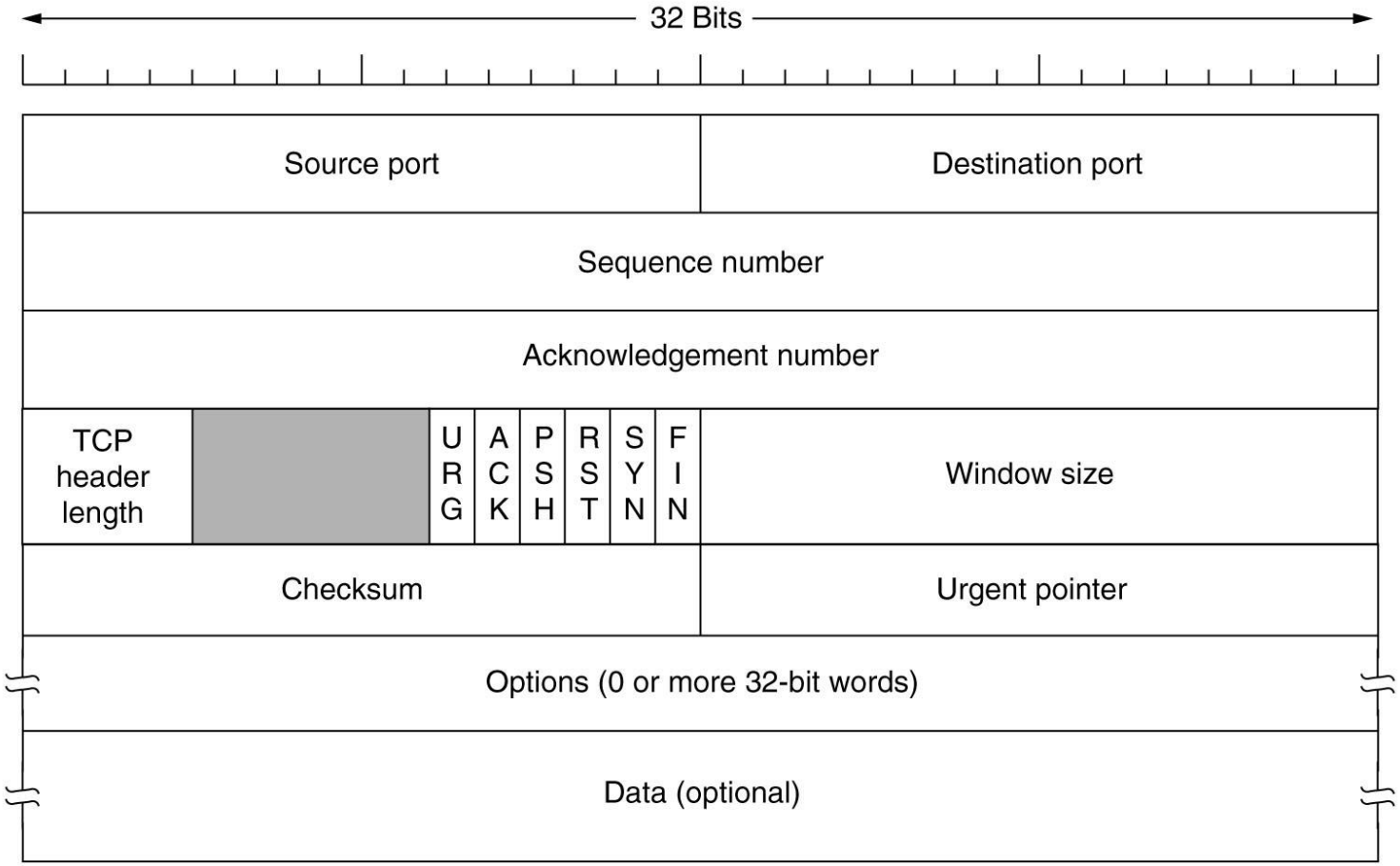
- Assumption: if #SYN > 3 * # SYN+ACK, then consider the activity as attack, port scanning.
- You MUST use dpkt; we will not grade codes using scapy.
- Know the OSI model:
  - Which layer handles which protocols
  - What fields exist within protocol headers

Networking basics:
OSI Model and Protocols



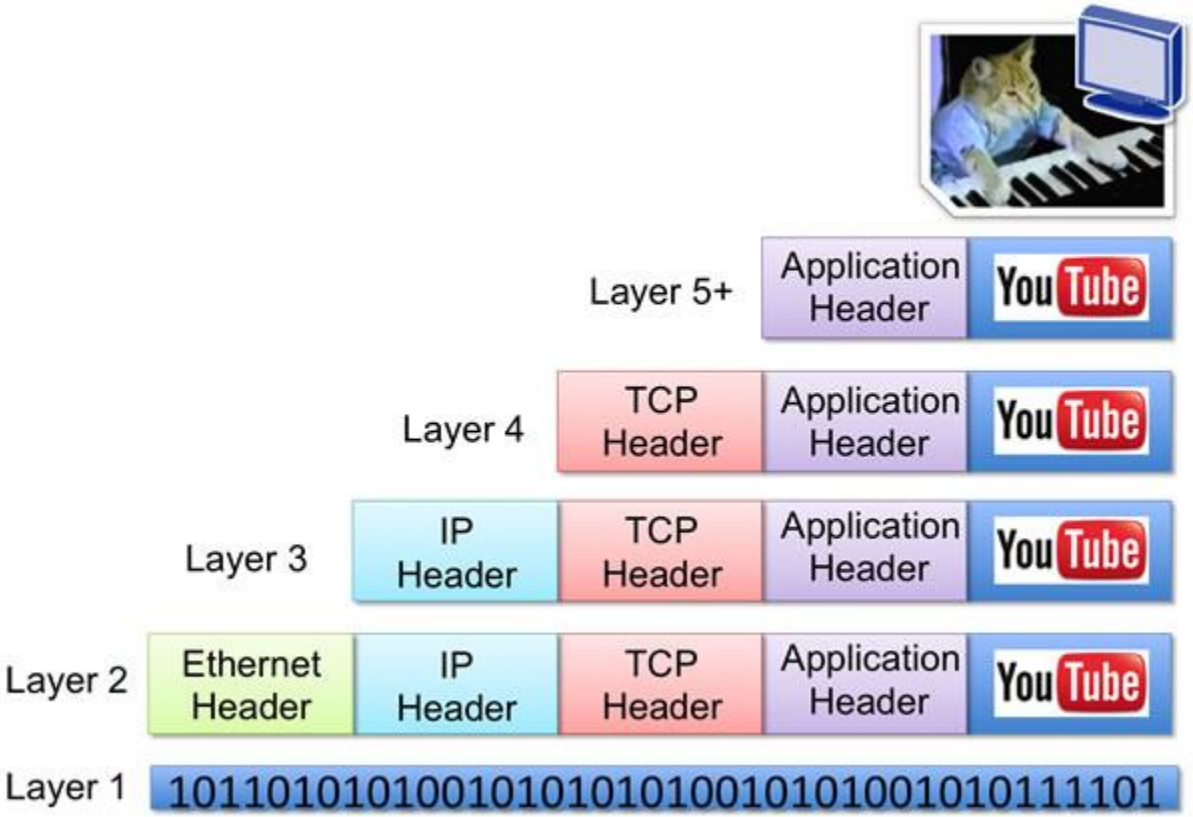
Source: http://teachweb.milin.cc/images/datacommunicatie/TCP-IP_vs_OSI_Model.png

Networking basics: TCP header



Source: https://elguber.wordpress.com/category/networking/page/2/

Networking basics: data encapsulation



Source: http://networkstatic.net/how-headers-encapsulate-in-the-osi-stack/

Anomaly detection: dpkt example

```
#!/usr/bin/python2.7
import dpkt


f = open('test.pcap')
pcap = dpkt.pcap.Reader(f)
for ts, buf in pcap:
    eth = dpkt.ethernet.Ethernet(buf)
    ip = eth.data
    tcp = ip.data

    if tcp.dport == 80 and len(tcp.data) > 0:
        http = dpkt.http.Request(tcp.data)
        print http.uri
f.close()
```

Source: https://jon.oberheide.org/blog/2008/10/15/dpkt-tutorial-2-parsing-a-pcap-file/

Test correctness

- https://subversion.ews.illinois.edu/svn/sp16-ece422/_shared/mp4/lbl-internal.20041004-1305.port002.dump.anon.pcap
  - Source: ftp://ftp.bro-ids.org/enterprise-traces/hdr-traces05
- http://networker.wikia.com/wiki/File:Portscan.pcap
  - A very small example created using Nmap

Tips

- Use try-except to handle/ignore malformed packets
- Don’t just dissect every packet
  - http://stackoverflow.com/questions/8849635/python-dpkt-find-out-if-packet-is-a-tcp-packet-or-a-udp-packet
- dpkt cheatsheet: http://engineering-notebook.readthedocs.org/en/latest/engineering/dpkt.html