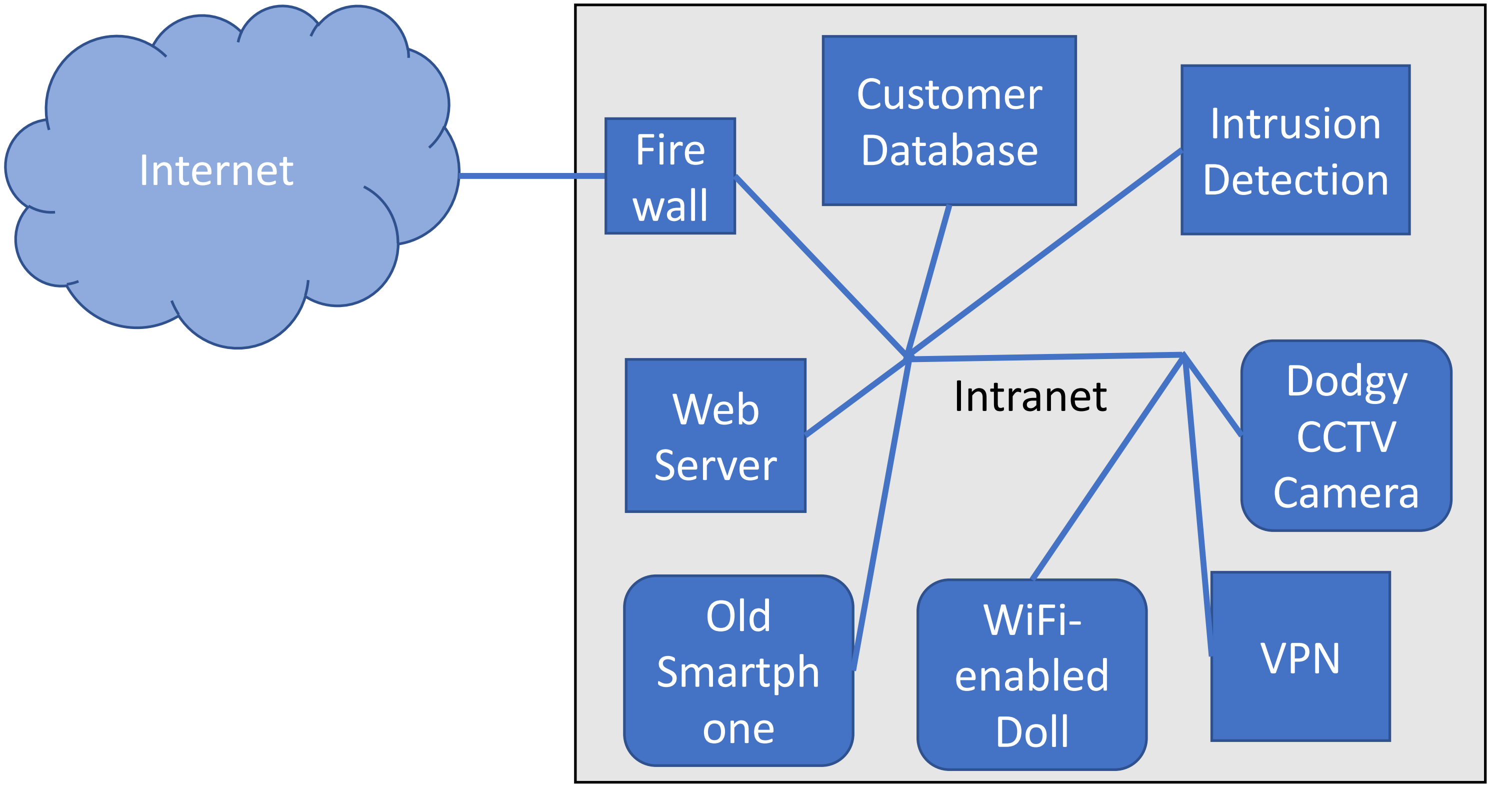
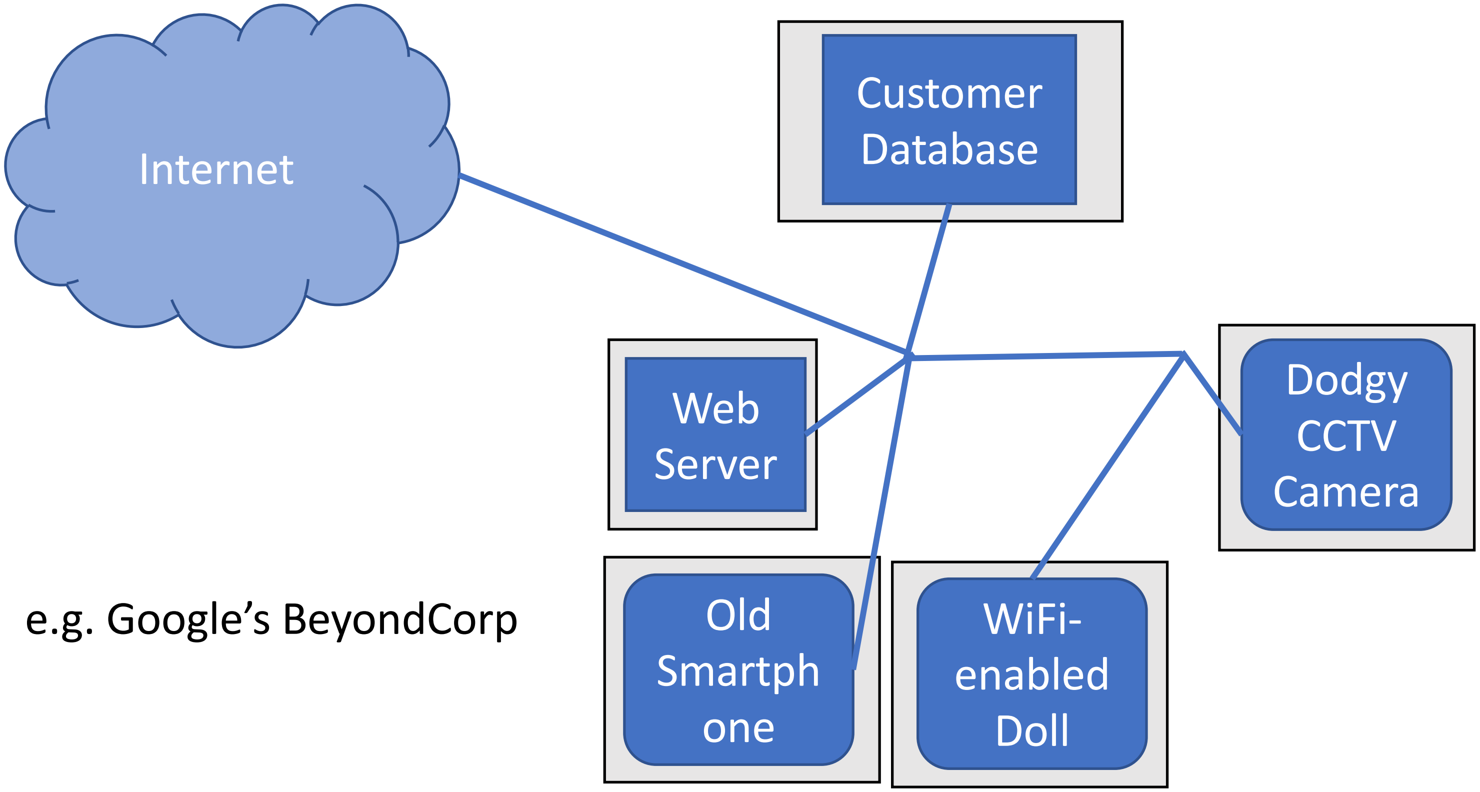
Security Engineering

Network security: integrating threat hunting, firewalls, intrusion detection, network logging and supporting services.

Perimeterisation



(De)perimeterisation



e.g. Google’s BeyondCorp

BGP

- Used for networking between Autonomous Systems in the internet (e.g. ISPs, telcos, large organisations)
- No intrinsic security – so lots of examples of false routes
- 2008: YouTube taken down after Pakistan tried to censor it locally
- 2010 China Telecom: 100000 invalid routes for 18 minutes – 15% of addresses.
- Various instances of intelligence collection via MITM

BGP Attacks: countermeasures

- Accept a limited number of routes from each peer
- Internet Routing Registries: at least there’s a log, but it’s filled with known incorrect data.
- Cloudflare: BGP collectors
- Resource Public Key Infrastructure: “*Autonomous system X announces IP address range Y*” – but do public keys really make things more robust? And how do you get widespread deployment?
- HTTPS: at least somewhere along the line, you’ll reach the destination or get DOS (but MITM attacks and attacks on public key infrastructure)

Denial of Service

- Take out your rivals’ service
- Country? Company? Video-game player?

Denial of Service

- Take out your rivals’ service
- Country? Company? Video-game player?
- Amplifier attacks

```
A -> B: SYN; my number is X
B -> A: ACK; now X+1
SYN; my number is Y
A -> B: ACK; now Y+1
(start talking)
```

TCP

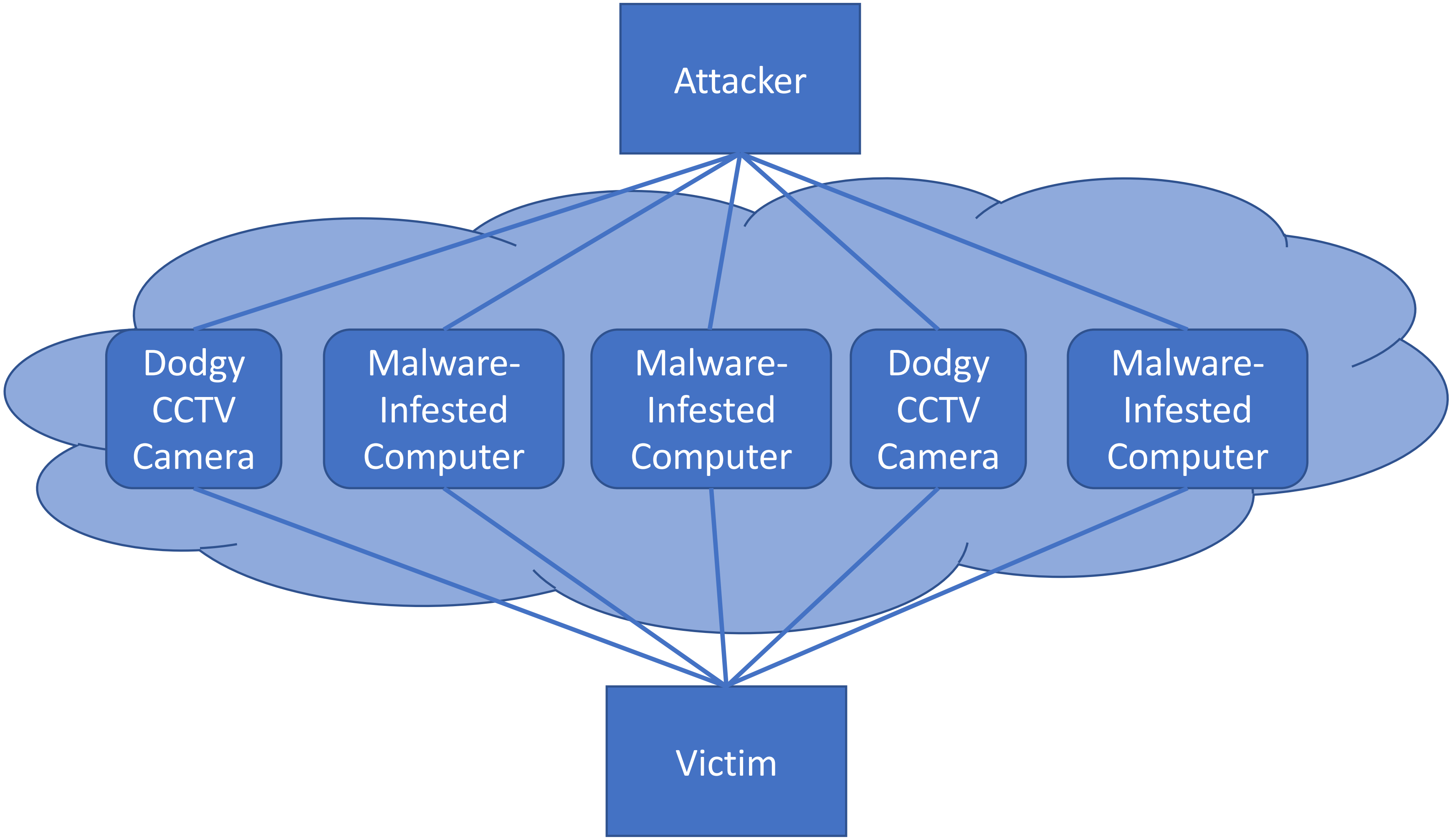
Denial of Service

- Amplifier attacks

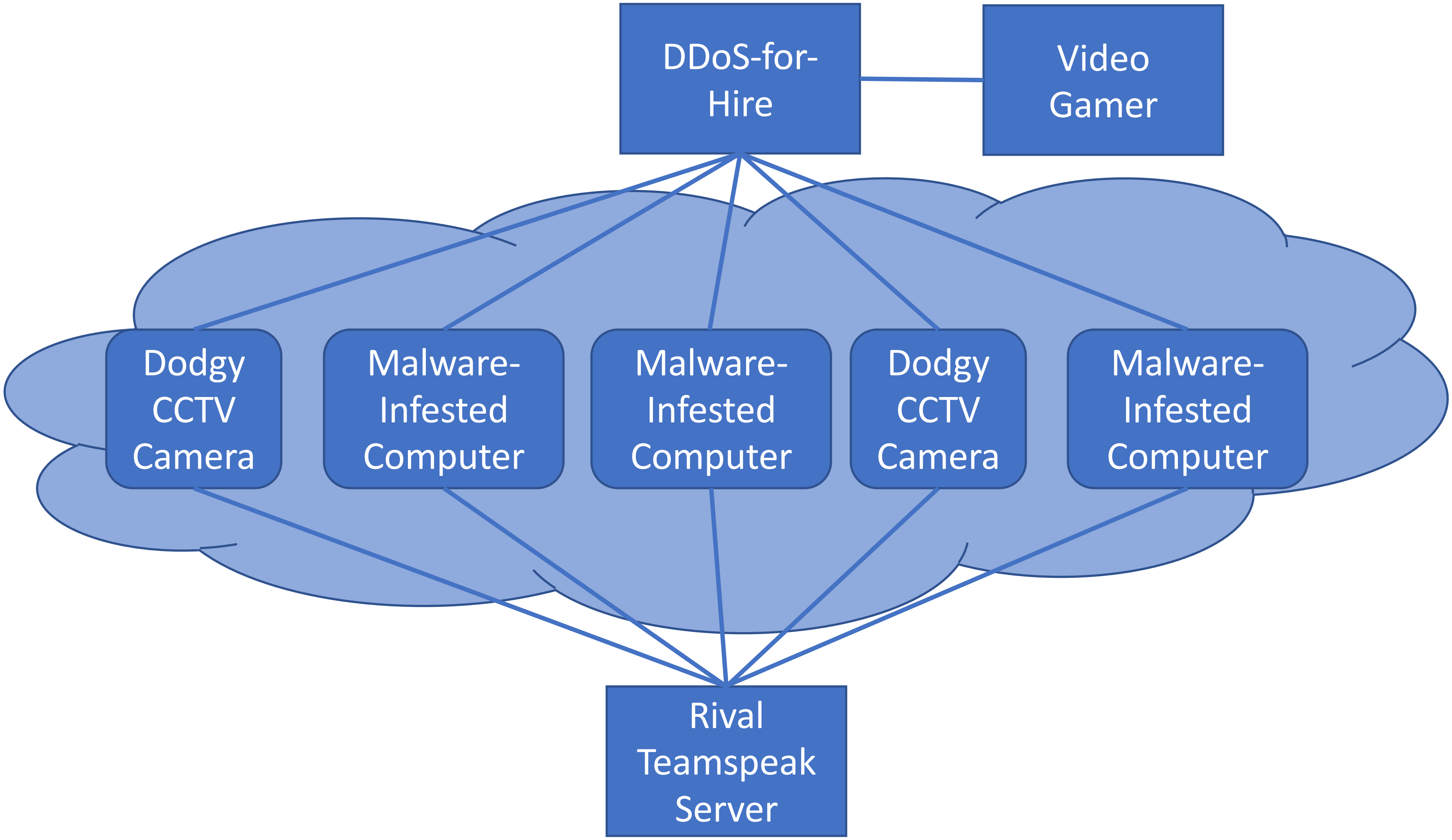
“C” -> B: SYN; my number is X
B -> C: **ACK**; now X+1
SYN; my number is Y
B -> C: **ACK**; now X+1
SYN; my number is Y
B -> C: **ACK**; now X+1
SYN; my number is Y
…

TCP Syn Reflection

Distributed Denial of Service


Attacker
Dodgy CCTV Camera
Malware-Infested Computer
Malware-Infested Computer
Dodgy CCTV Camera
Malware-Infested Computer
Victim

Distributed Denial of Service



DDoS-for-Hire

Video Gamer

Dodgy CCTV Camera

Malware-Infested Computer

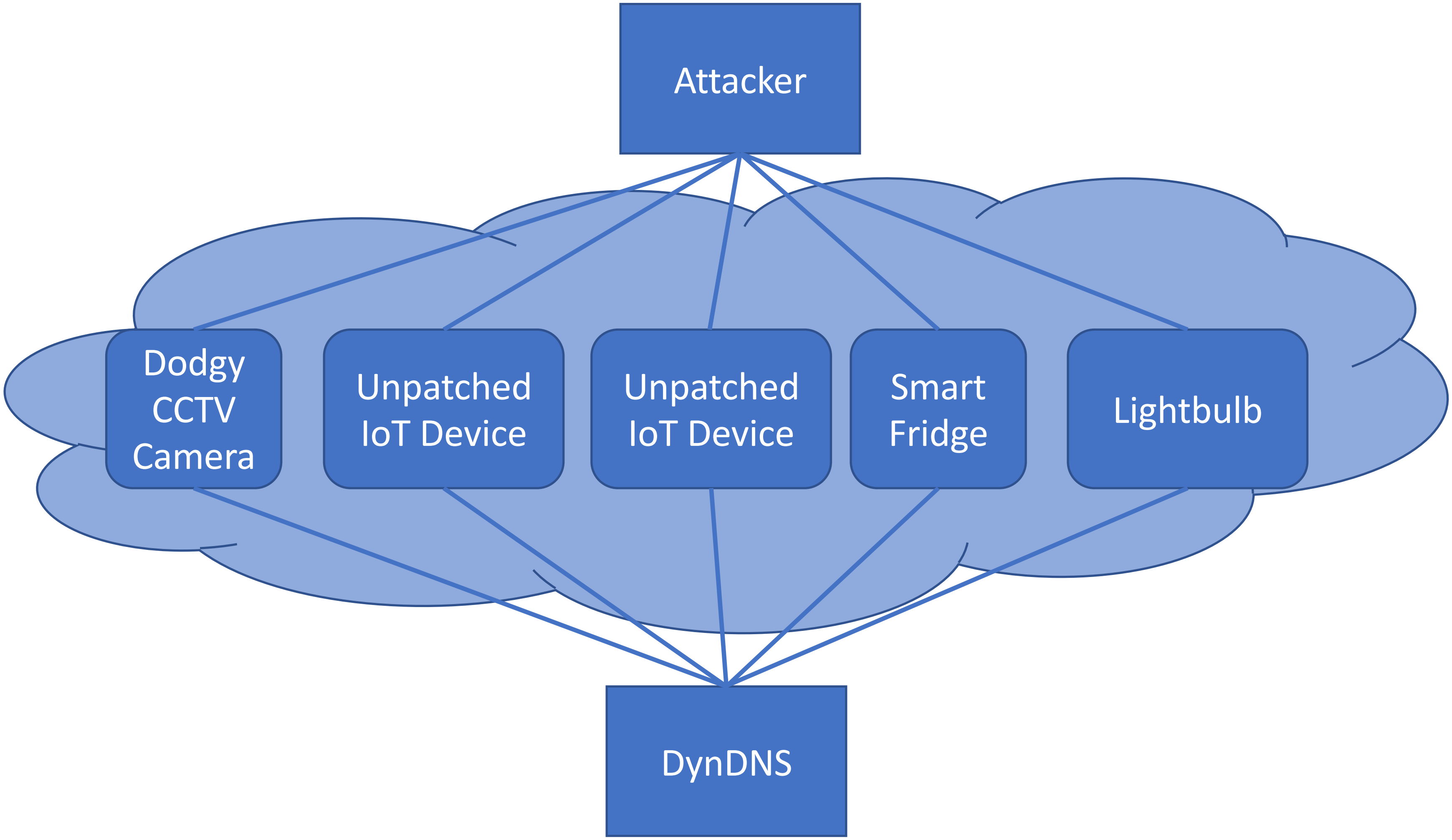
Malware-Infested Computer

Dodgy CCTV Camera

Malware-Infested Computer

Rival Teamspeak Server

Mirai Botnet



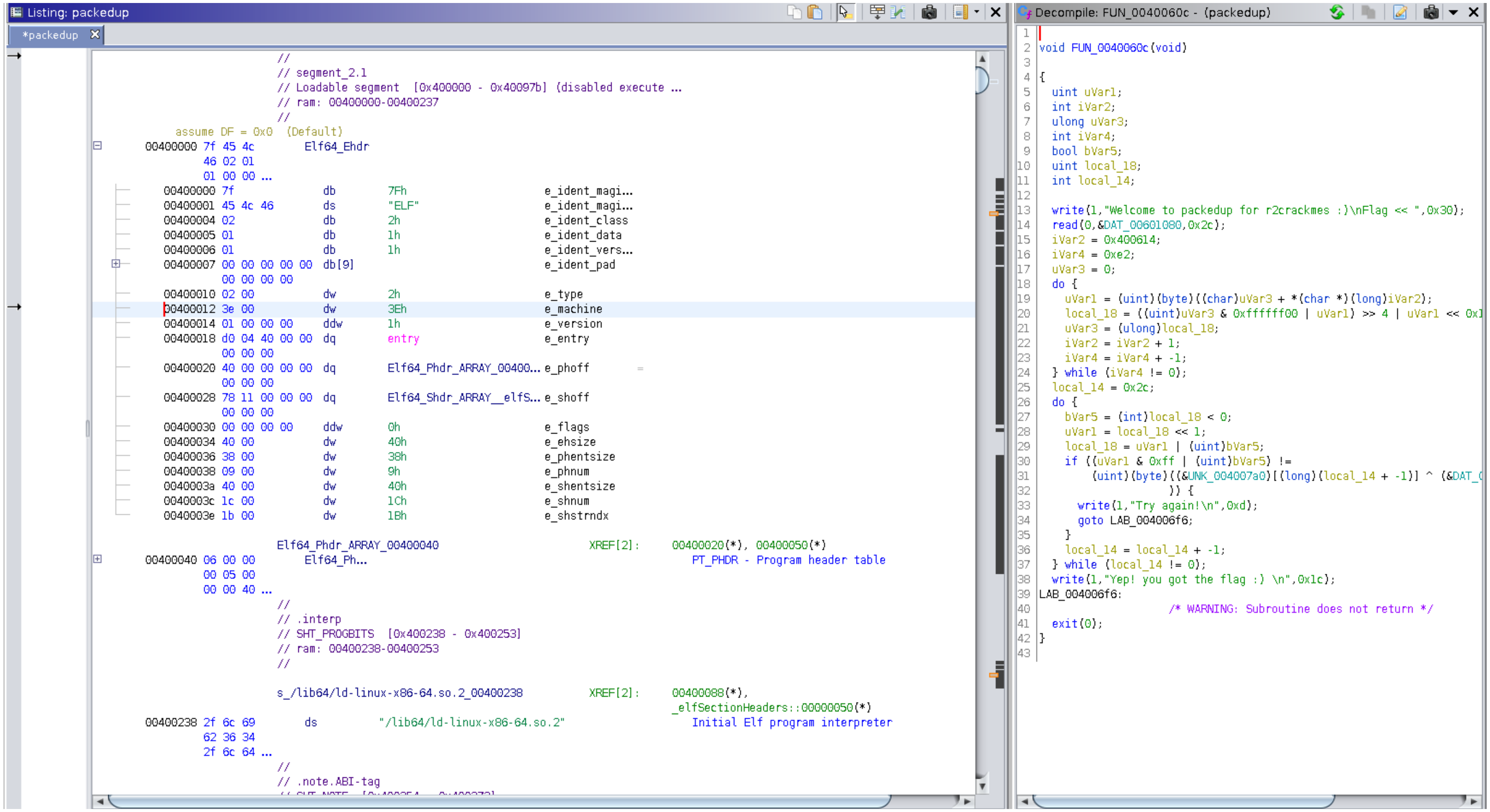
Malware

- Viruses
- Worms
- Trojans
- Remote Access Trojans

Malware

- Viruses
- Worms
- Trojans
- Remote Access Trojans
- Rootkits
- Potentially Unwanted Software
- Stalkerware?
- Antivirus Software Itself???

Malware Analysis



```
                    //
                    // segment_2.1
                    // Loadable segment  [0x400000 - 0x40097b] (disabled execute ...
                    // ram: 00400000-00400237
                    //
          assume DF = 0x0  (Default)
     00400000 7f 45 4c        Elf64_Ehdr
              46 02 01
              01 00 00 ...
       00400000 7f             db       7Fh                  e_ident_magi...
       00400001 45 4c 46       ds       "ELF"                e_ident_magi...
       00400004 02             db       2h                   e_ident_class
       00400005 01             db       1h                   e_ident_data
       00400006 01             db       1h                   e_ident_vers...
       00400007 00 00 00 00 00 db[9]                         e_ident_pad
                00 00 00 00
       00400010 02 00          dw       2h                   e_type
       00400012 3e 00          dw       3Eh                  e_machine
       00400014 01 00 00 00    ddw      1h                   e_version
       00400018 d0 04 40 00 00 dq       entry                e_entry
                00 00 00
       00400020 40 00 00 00 00 dq       Elf64_Phdr_ARRAY_00400... e_phoff
                00 00 00
       00400028 78 11 00 00 00 dq       Elf64_Shdr_ARRAY__elfS... e_shoff
                00 00 00
       00400030 00 00 00 00    ddw      0h                   e_flags
       00400034 40 00          dw       40h                  e_ehsize
       00400036 38 00          dw       38h                  e_phentsize
       00400038 09 00          dw       9h                   e_phnum
       0040003a 40 00          dw       40h                  e_shentsize
       0040003c 1c 00          dw       1Ch                  e_shnum
       0040003e 1b 00          dw       1Bh                  e_shstrndx

                    Elf64_Phdr_ARRAY_00400040          XREF[2]:     00400020(*), 00400050(*)
     00400040 06 00 00        Elf64_Ph...                              PT_PHDR - Program header table
              00 05 00
              00 00 40 ...
                    //
                    // .interp
                    // SHT_PROGBITS  [0x400238 - 0x400253]
                    // ram: 00400238-00400253
                    //

                    s_/lib64/ld-linux-x86-64.so.2_00400238     XREF[2]:     00400088(*),
                                                                            _elfSectionHeaders::00000050(*)
     00400238 2f 6c 69        ds        "/lib64/ld-linux-x86-64.so.2"          Initial Elf program interpreter
              62 36 34
              2f 6c 64 ...
                    //
                    // .note.ABI-tag
```

```

void FUN_0040060c(void)

{
  uint uVar1;
  int iVar2;
  ulong uVar3;
  int iVar4;
  bool bVar5;
  uint local_18;
  int local_14;

  write(1,"Welcome to packedup for r2crackmes :)\nFlag << ",0x30);
  read(0,&DAT_00601080,0x2c);
  iVar2 = 0x400614;
  iVar4 = 0xe2;
  uVar3 = 0;
  do {
    uVar1 = (uint)(byte)((char)uVar3 + *(char *)(long)iVar2);
    local_18 = ((uint)uVar3 & 0xffffff00 | uVar1) >> 4 | uVar1 << 0x1
    uVar3 = (ulong)local_18;
    iVar2 = iVar2 + 1;
    iVar4 = iVar4 + -1;
  } while (iVar4 != 0);
  local_14 = 0x2c;
  do {
    bVar5 = (int)local_18 < 0;
    uVar1 = local_18 << 1;
    local_18 = uVar1 | (uint)bVar5;
    if ((uVar1 & 0xff | (uint)bVar5) !=
        (uint)(byte)((&UNK_004007a0)[(long)(local_14 + -1)] ^ (&DAT_0
                   )) {
      write(1,"Try again!\n",0xd);
      goto LAB_004006f6;
    }
    local_14 = local_14 + -1;
  } while (local_14 != 0);
  write(1,"Yep! you got the flag :) \n",0x1c);
LAB_004006f6:
                    /* WARNING: Subroutine does not return */
  exit(0);
}

```

Screenshot of Ghidra, https://commons.wikimedia.org/wiki/File:Ghidra-disassembly,March_2019.png

Malware and Incentives

- Why do all of these exist?
- Hobbyists, maybe
- Profit, e.g. Ransomware
- Surveillance (State Actors, or Jealous Partners?)
- Hacktivism
- Profit, more indirectly e.g. Botnets
- Hacking as a service?

Intrusion Detection and Mitigation

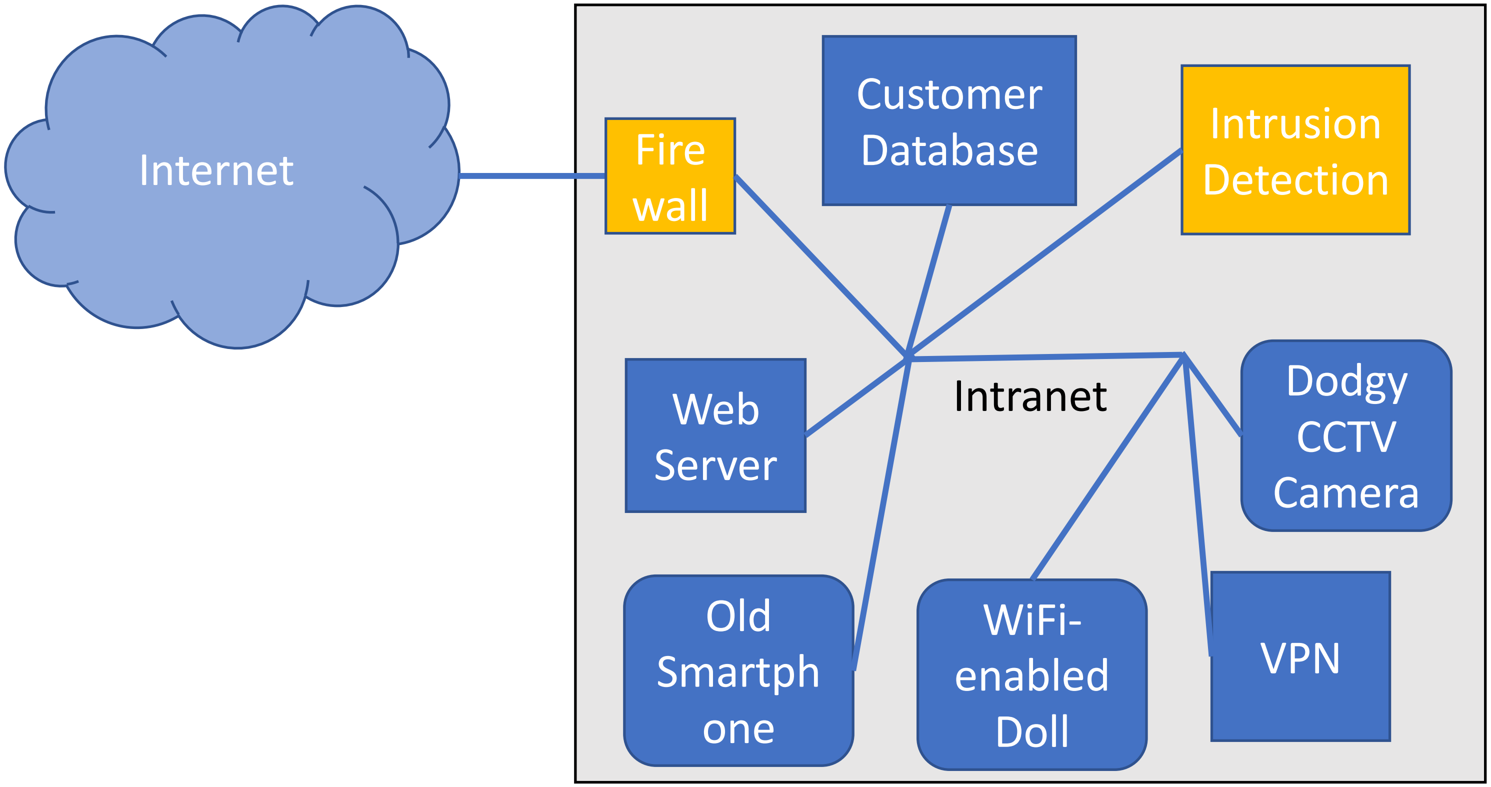
- Intranets of any reasonable size will get infected.
- What is the perimeter, really (VPN, BYOD)?
- Spearphishing: if YOUR sysadmin gets attacked, will you just “blame and train”?
- Adkins et al.: Make criminal adversaries’ attacks expensive (e.g. CAPTCHA) so they go after easier targets

Insider Risk -- Defences

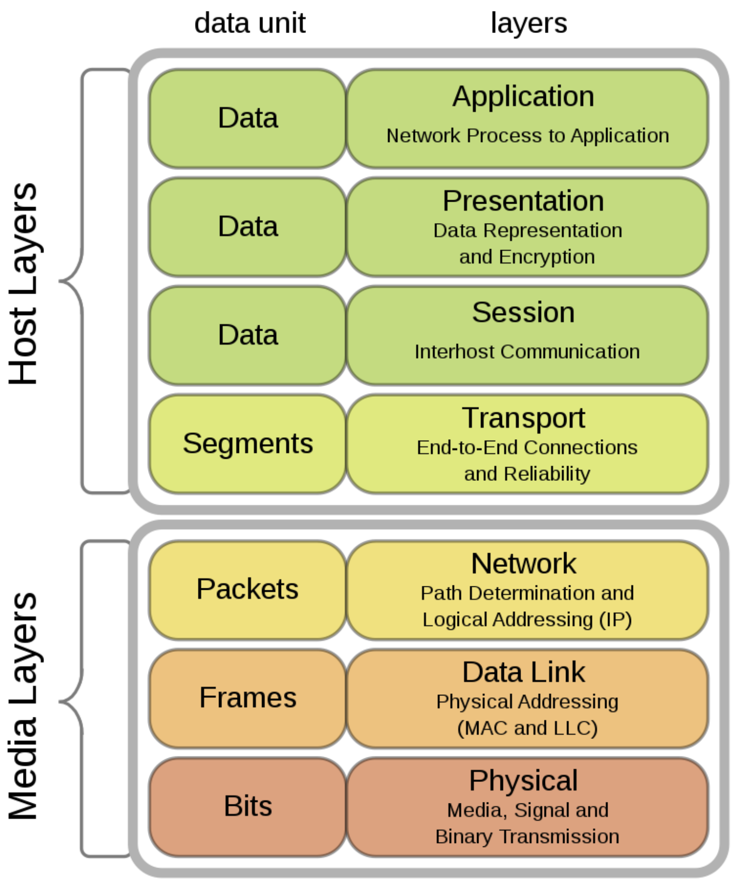
- Least Privilege
- Zero Trust
- Multi-party Authorisation
- Business Justifications
- Auditing and Detection
- Recoverability

From *Building Secure & Reliable Systems: Best Practices for Designing, Implementing and Maintaining Systems*, Heather Adkins, Betsy Beyer, Paul Blankinship, Piotr Lewandowski, Ana Oprea & Adam Stubblefield

Intrusion Detection and Mitigation



Filtering: Firewalls

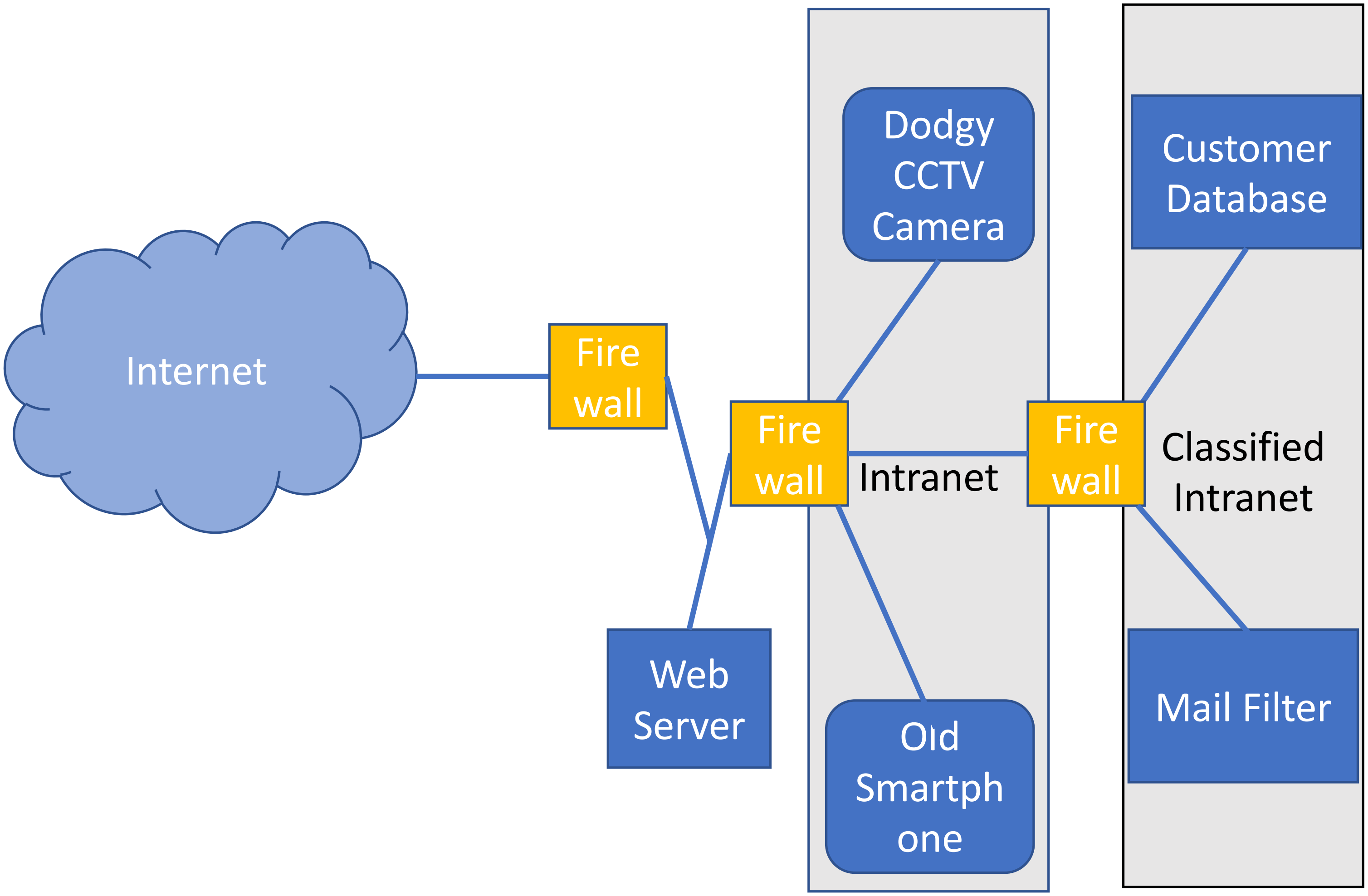

data unit
layers
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and Logical Addressing (IP)
Frames
Data Link
Physical Addressing (MAC and LLC)
Bits
Physical
Media, Signal and Binary Transmission

Content Filtering: Application Layer

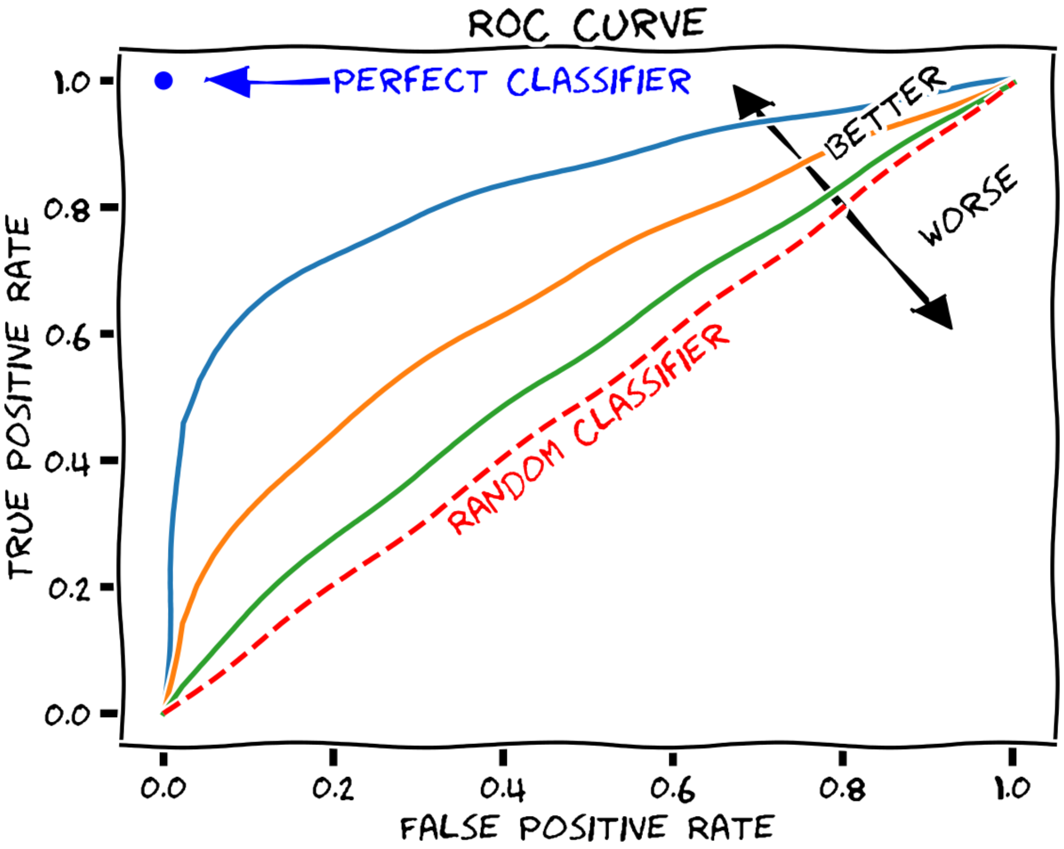
Circuit Gateways: Full TCP sessions.

Packet Filtering: IP-address spoofing, IP deny lists, port blocking

Where should your protections be?



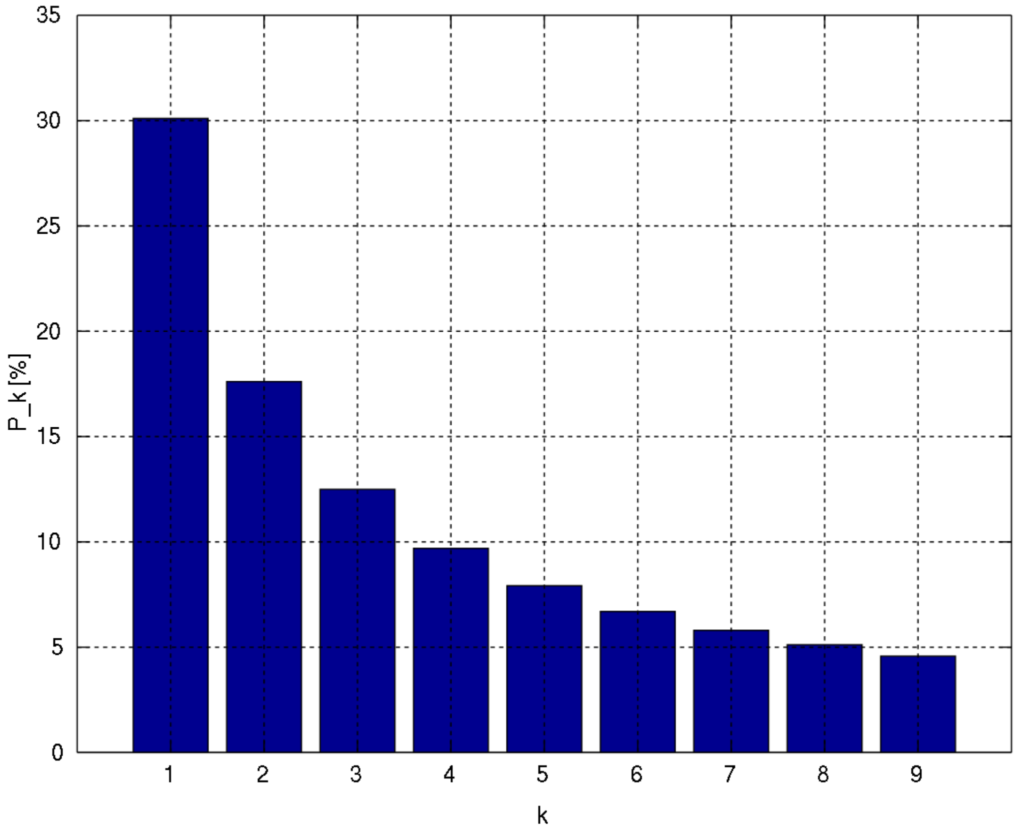
ROC Curve


ROC CURVE
PERFECT CLASSIFIER
BETTER
WORSE
RANDOM CLASSIFIER
TRUE POSITIVE RATE
FALSE POSITIVE RATE
1.0
0.8
0.6
0.4
0.2
0.0
0.0
0.2
0.4
0.6
0.8
1.0

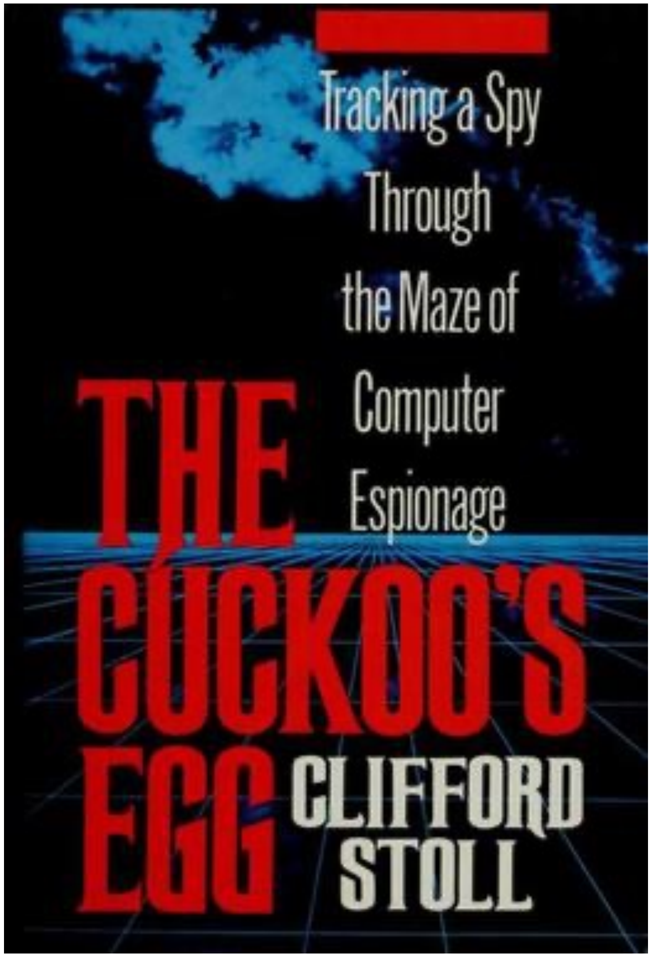
Intrusion Detection Systems

- Monitoring and Logging: Don’t block, just sound and alarm or forward on.
- Misuse Detection: known bad things
- Anomaly Detection: unusual things?

Example: Benford’s Law



Honeypots


Tracking a Spy Through the Maze of Computer Espionage
THE CUCKOO'S EGG
CLIFFORD STOLL

Challenges in Intrusion Detection

- The internet is noisy: malice or error?
- Signal-to-noise ratios
- We should always be wary of machine learning
- Audit trails (or lack thereof)
- Compliance vs real defence
- Global vs Local detection issues

Networks and Cryptography

- WiFi: WEP was weak, but WPA2 supported widely, and uses AES
- Is WiFi a “perimeter”? Issues around trust (default router passwords, IoT devices, unpatched devices)
- VPNs: Funnel packets over untrusted internet into trusted perimeters. IPSec probably weak by default ☹

Networks and Cryptography: HTTPS

- HTTPS (via TLS) now on >60% of connections
- Exchange session keys based on public-key infrastructure
- How do you identify who you’re talking to? Certificating Authorities.
- Are CAs trustworthy?
- False positives: ROC curves again
- LetsEncrypt was a real game-changer

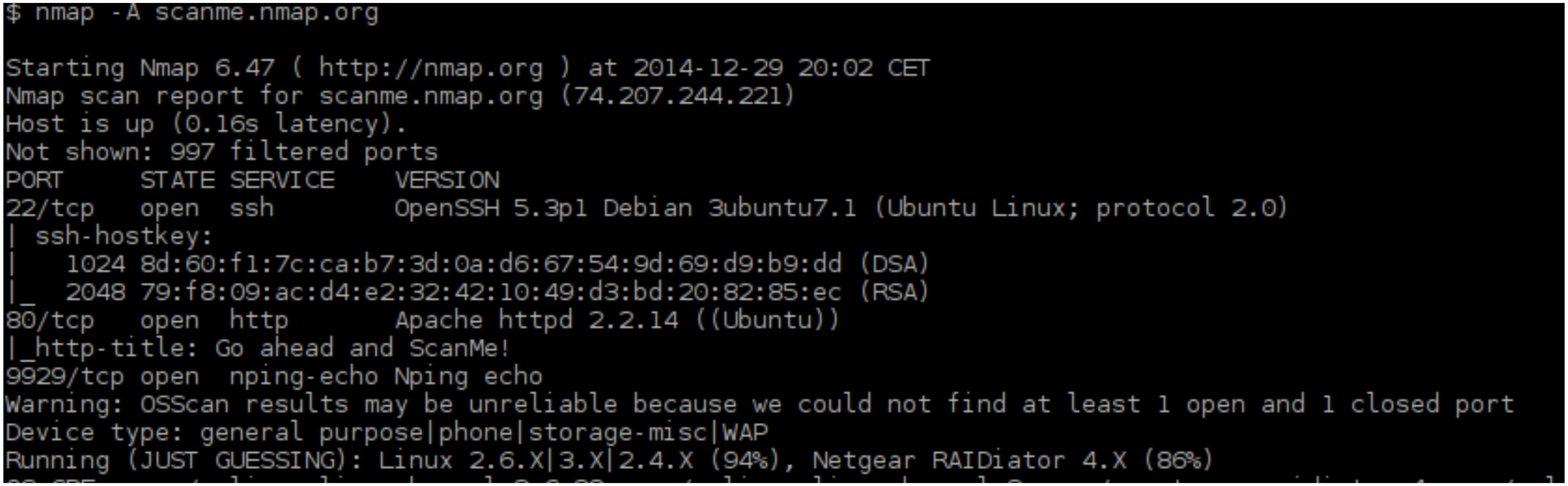
Networks and Cryptography: Email

- SMTP is old, and neither encrypted nor authenticated by default.
- PGP: Why Johnny Can’t Encrypt
- Mail-Server Filters: less good than you’d think
- Interception Prevention: STARTTLS and MTA-STS

XSS Game

- https://xss-game.appspot.com/
- Also, https://injection.pythonanywhere.com/ (XSS and SQL Injection)

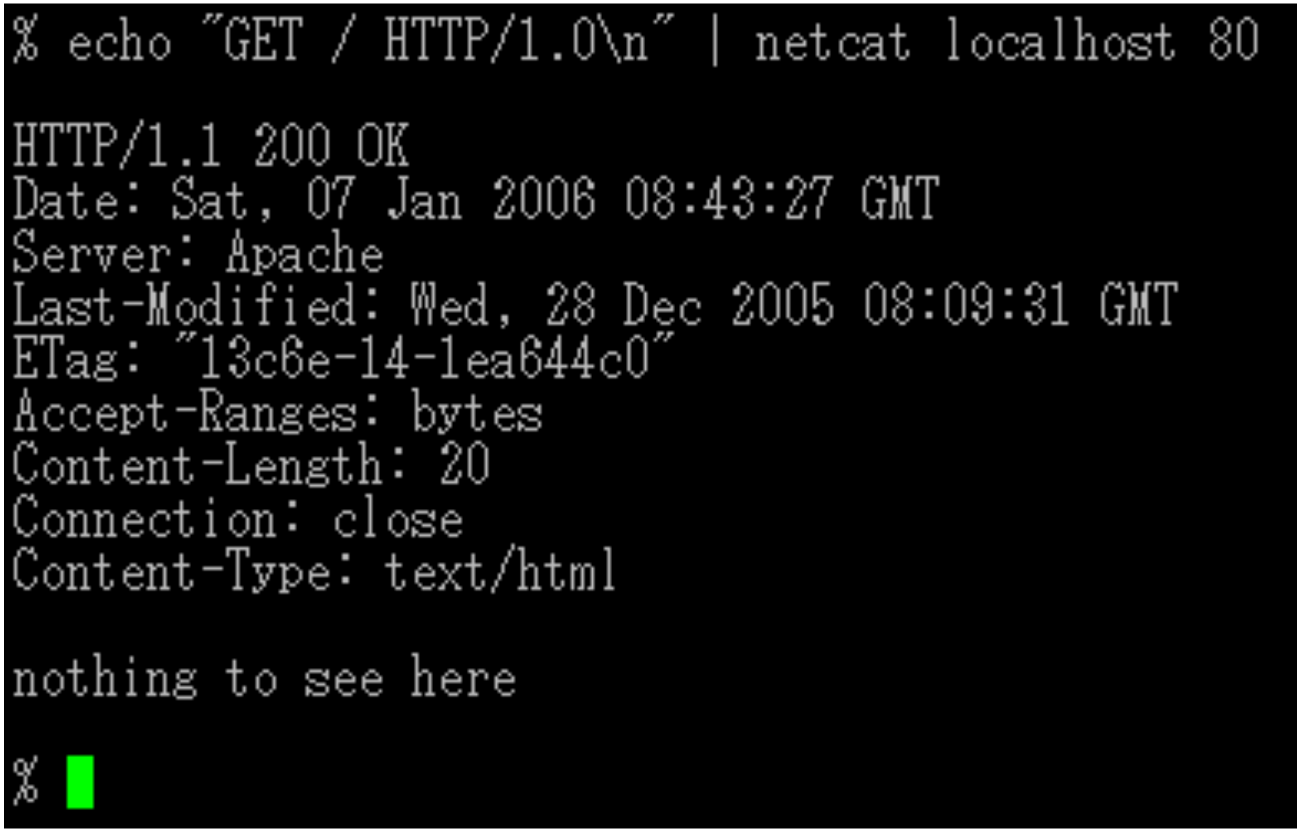
Tools of Attack/Defence



```
$ nmap -A scanme.nmap.org

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-29 20:02 CET
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.16s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_  2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open  http       Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
9929/tcp open  nping-echo Nping echo
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|storage-misc|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (94%), Netgear RAIDiator 4.X (86%)
```

Nmap: Port scanning

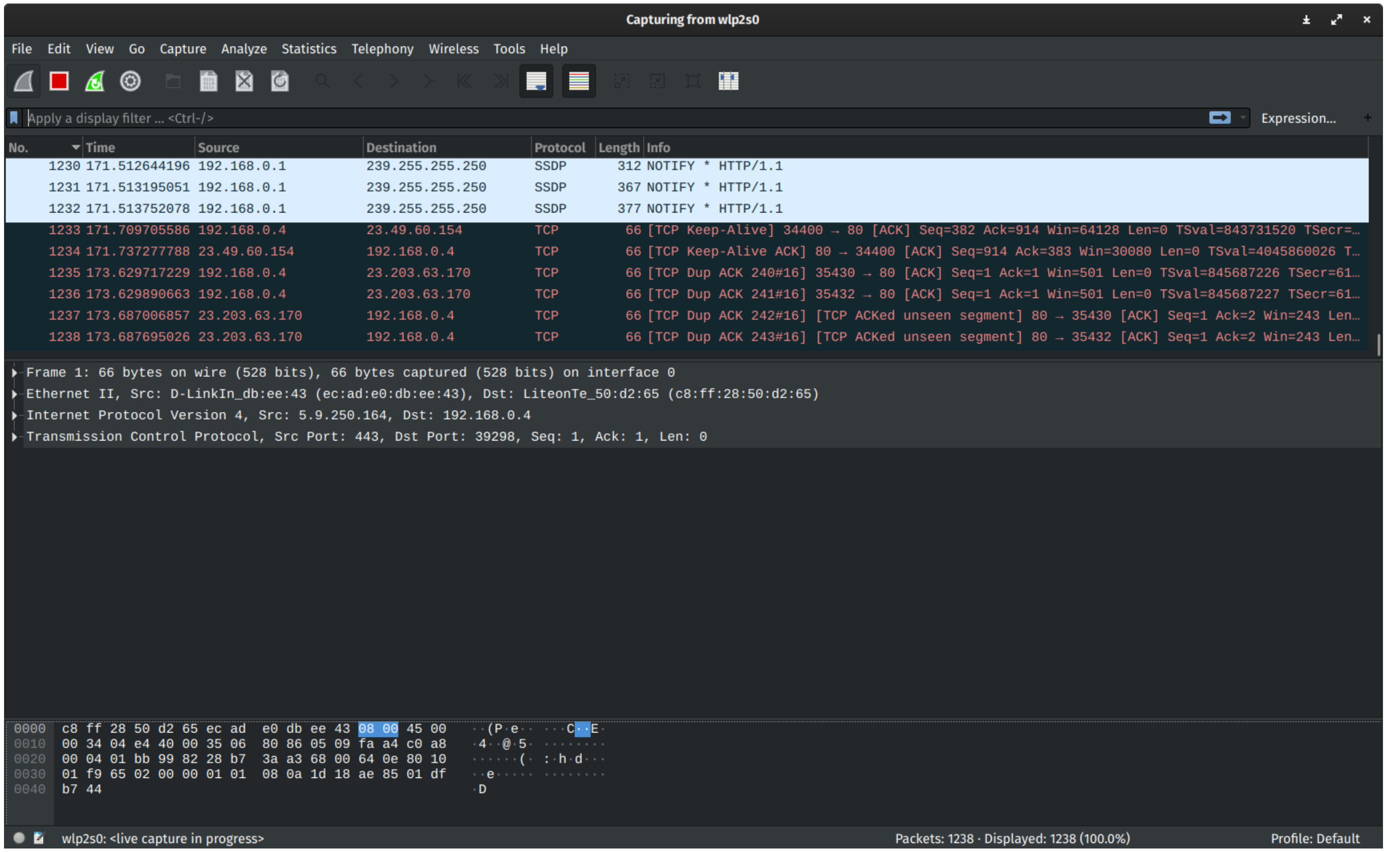
Tools of Attack/Defence



```
% echo "GET / HTTP/1.0\n" | netcat localhost 80

HTTP/1.1 200 OK
Date: Sat, 07 Jan 2006 08:43:27 GMT
Server: Apache
Last-Modified: Wed, 28 Dec 2005 08:09:31 GMT
ETag: "13c6e-14-1ea644c0"
Accept-Ranges: bytes
Content-Length: 20
Connection: close
Content-Type: text/html

nothing to see here

% 
```

Netcat: Port Scanning / Listening (of specific ports)

Tools of Attack/Defence



No.	Time	Source	Destination	Protocol	Length	Info
1230	171.512644196	192.168.0.1	239.255.255.250	SSDP	312	NOTIFY * HTTP/1.1
1231	171.513195051	192.168.0.1	239.255.255.250	SSDP	367	NOTIFY * HTTP/1.1
1232	171.513752078	192.168.0.1	239.255.255.250	SSDP	377	NOTIFY * HTTP/1.1
1233	171.709705586	192.168.0.4	23.49.60.154	TCP	66	[TCP Keep-Alive] 34400 → 80 [ACK] Seq=382 Ack=914 Win=64128 Len=0 TSval=843731520 TSecr=…
1234	171.737277788	23.49.60.154	192.168.0.4	TCP	66	[TCP Keep-Alive ACK] 80 → 34400 [ACK] Seq=914 Ack=383 Win=30080 Len=0 TSval=4045860026 T…
1235	173.629717229	192.168.0.4	23.203.63.170	TCP	66	[TCP Dup ACK 240#16] 35430 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=845687226 TSecr=61…
1236	173.629890663	192.168.0.4	23.203.63.170	TCP	66	[TCP Dup ACK 241#16] 35432 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=845687227 TSecr=61…
1237	173.687006857	23.203.63.170	192.168.0.4	TCP	66	[TCP Dup ACK 242#16] [TCP ACKed unseen segment] 80 → 35430 [ACK] Seq=1 Ack=2 Win=243 Len…
1238	173.687695026	23.203.63.170	192.168.0.4	TCP	66	[TCP Dup ACK 243#16] [TCP ACKed unseen segment] 80 → 35432 [ACK] Seq=1 Ack=2 Win=243 Len…

```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: D-LinkIn_db:ee:43 (ec:ad:e0:db:ee:43), Dst: LiteonTe_50:d2:65 (c8:ff:28:50:d2:65)
Internet Protocol Version 4, Src: 5.9.250.164, Dst: 192.168.0.4
Transmission Control Protocol, Src Port: 443, Dst Port: 39298, Seq: 1, Ack: 1, Len: 0
```

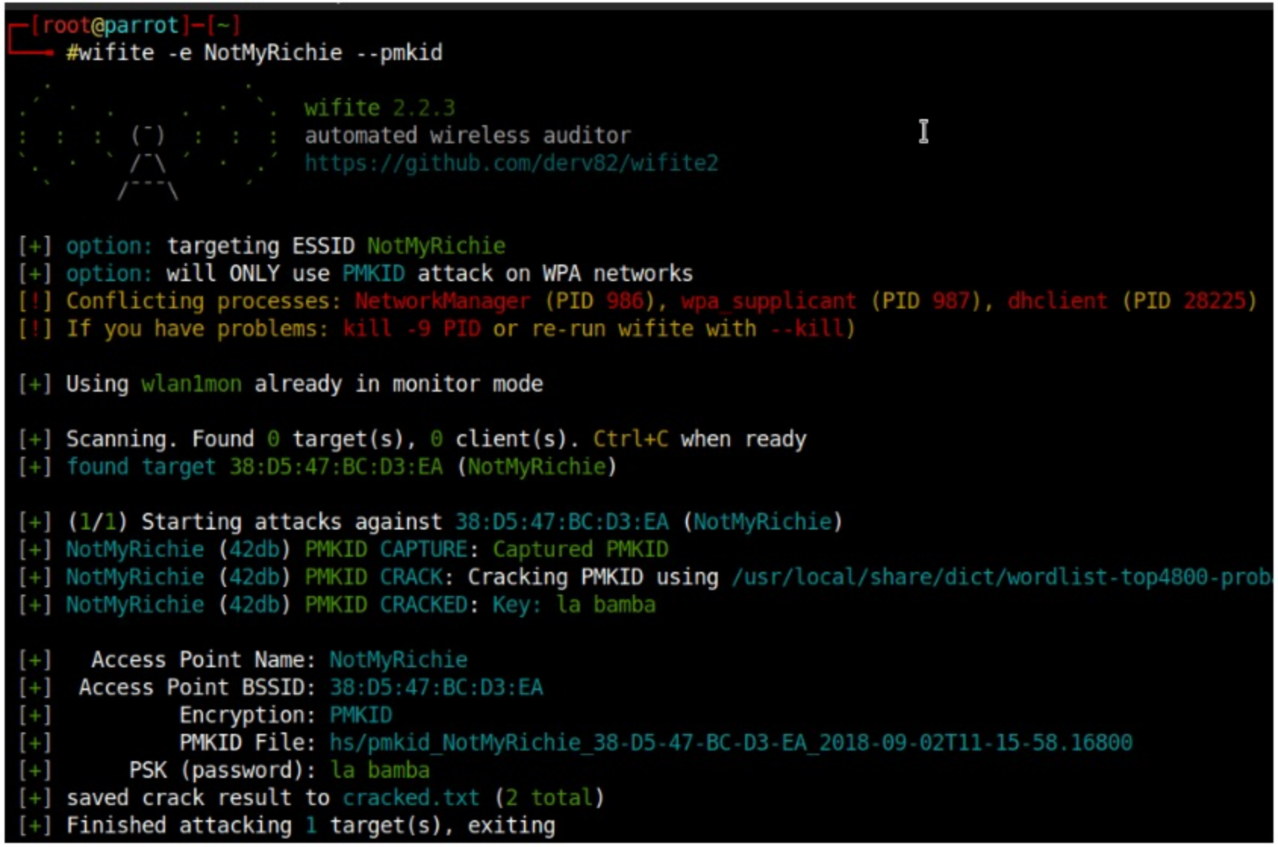
```
0000  c8 ff 28 50 d2 65 ec ad  e0 db ee 43 08 00 45 00   ··(P·e·· ···C··E·
0010  00 34 04 e4 40 00 35 06  80 86 05 09 fa a4 c0 a8   ·4··@·5· ········
0020  00 04 01 bb 99 82 28 b7  3a a3 68 00 64 0e 80 10   ······(· :·h·d···
0030  01 f9 65 02 00 00 01 01  08 0a 1d 18 ae 85 01 df   ··e····· ········
0040  b7 44                                              ·D
```

wlp2s0: <live capture in progress>   Packets: 1238 · Displayed: 1238 (100.0%)   Profile: Default

Wireshark: Packet Sniffing

Tools of Attack/Defence

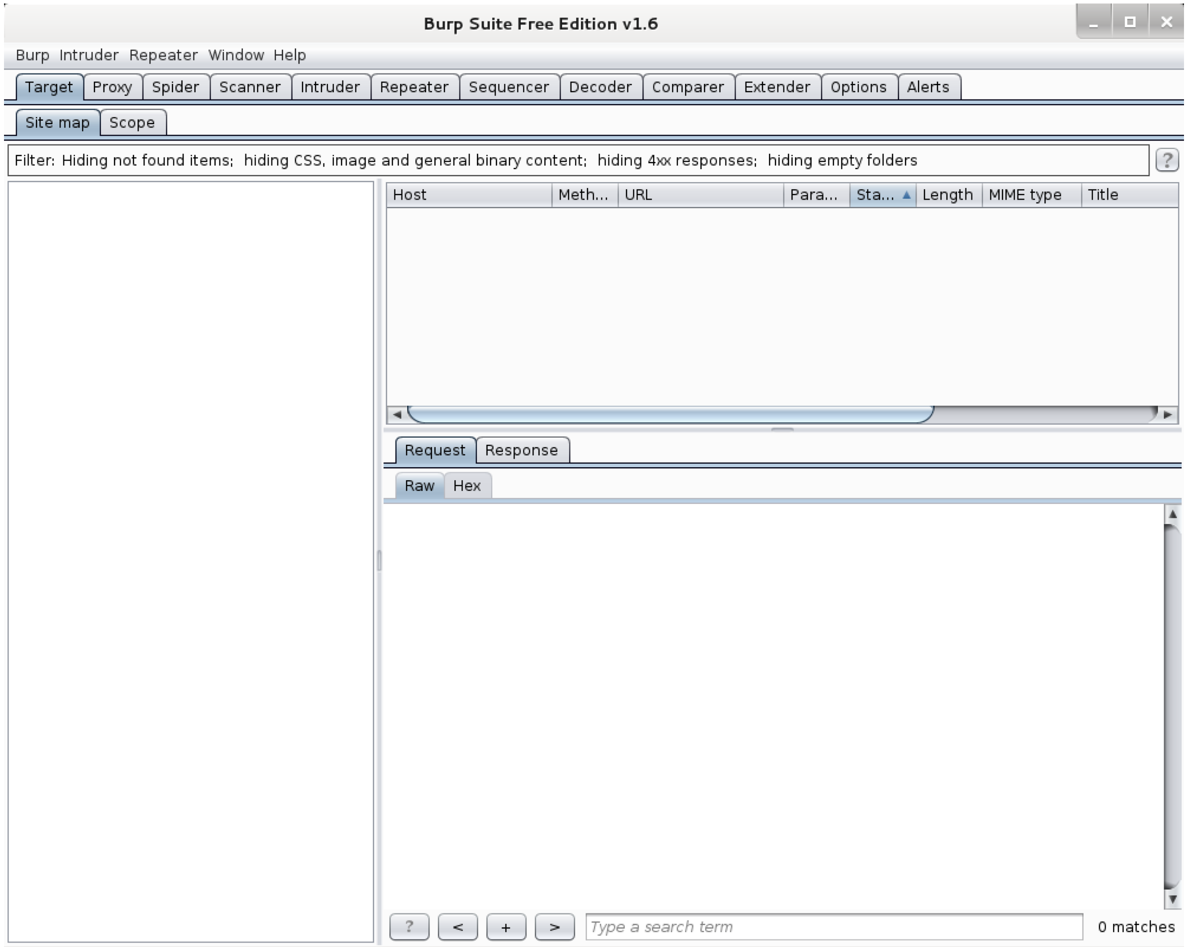
Cracking WPA key using PMKID attack:



```
┌─[root@parrot]─[~]
└──╼ #wifite -e NotMyRichie --pmkid
   .                     .
 .´  ·  .         .  ·  `.  wifite 2.2.3
 :  :  :  (¯)  :  :  :   automated wireless auditor
 `.  ·  ` /¯\ ´  ·  .´   https://github.com/derv82/wifite2
   `     /¯¯¯\      ´

[+] option: targeting ESSID NotMyRichie
[+] option: will ONLY use PMKID attack on WPA networks
[!] Conflicting processes: NetworkManager (PID 986), wpa_supplicant (PID 987), dhclient (PID 28225)
[!] If you have problems: kill -9 PID or re-run wifite with --kill)

[+] Using wlan1mon already in monitor mode

[+] Scanning. Found 0 target(s), 0 client(s). Ctrl+C when ready
[+] found target 38:D5:47:BC:D3:EA (NotMyRichie)

[+] (1/1) Starting attacks against 38:D5:47:BC:D3:EA (NotMyRichie)
[+] NotMyRichie (42db) PMKID CAPTURE: Captured PMKID
[+] NotMyRichie (42db) PMKID CRACK: Cracking PMKID using /usr/local/share/dict/wordlist-top4800-prob
[+] NotMyRichie (42db) PMKID CRACKED: Key: la bamba

[+]   Access Point Name: NotMyRichie
[+]  Access Point BSSID: 38:D5:47:BC:D3:EA
[+]          Encryption: PMKID
[+]          PMKID File: hs/pmkid_NotMyRichie_38-D5-47-BC-D3-EA_2018-09-02T11-15-58.16800
[+]      PSK (password): la bamba
[+] saved crack result to cracked.txt (2 total)
[+] Finished attacking 1 target(s), exiting
```

WiFite: WiFi hacking

Tools of Attack/Defence


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
?
Host Meth... URL Para... Sta... Length MIME type Title
Request Response
Raw Hex
? < + >
Type a search term
0 matches

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Burp Suite: Attack and Defend Web *Applications*