IT-Security (ITS) B1

DIKU, E2019

Today’s agenda

Part 1: Course overview.

Part 2: Who hacks? - The current threat picture

Lectures

Lectures

Mondays at 09-11 in Teilum A, Frederik Vs vej 1
Fridays at 09-11 in Aud 6, HCØ

Instructors:

Michael Kirkedal Thomsen (course organiser)
Troels Langkjær
Carsten Jørgensen

Lecture plan

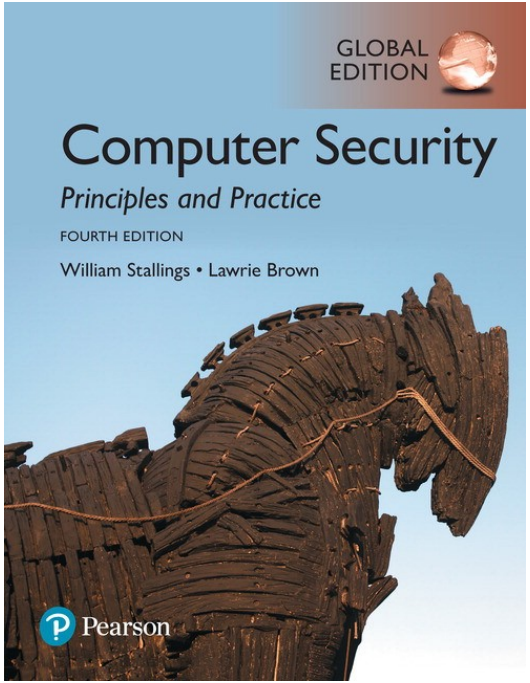
Week	Date	Time	Lecture	Topic
36	02 Sep	09-11	TL	Introduction, security concepts and the threat of hacking
	06 Sep	09-11	TL	Buffer overflow
37	09 Sep	09-11	CJ	Software security, Operating system security
	13 Sep	09-11	CJ	User authentication and access control
38	16 Sep	09-11	TJ	Malicious software
	20 Sep	09-11	CJ	Firewalls and denial-of-service attacks
39	23 Sep	09-11	CJ	Cloud and IoT
	27 Sep	09-11	TL	Cryptography
40	30 Sep	09-11	TL	Internet security protocols
	04 Oct	09-11	TL	Intrusion detection
41	07 Oct	09-11	TL	Forensics
	12 Oct	09-11	CJ	IT security management
42				Fall Vacation - No lectures
43	22 Oct	09-11	CJ	Privacy 1
	25 Oct	09-11	CJ	Privacy 2 - GDPR
44	29 Oct	15-16	Guest	TBA
		16-17	All	Recap and Q/A
45	06 Nov			Exam

Reading material

Computer Security: Principles and Practice, William Stalling & Lawrie Brown, 4th and Global Edition, Pearson, ISBN 13: 978-1292220611.

Some notes and book chapters that will be made available through the detailed course schedule.

(Lectures focus on the big picture and are not 1:1 with the reading material.)



Expectation for ITS

CompSys.

Assignments

There are 6 weekly assignments during the course.

Assignments are pass/fail; expect at least 75 % correct to get a pass.

It will be possible to re-handin one (and only one) assignment (1-4); deadline 19 Oct @ 10:00AM.

All assignments are individual.

To qualify for the exam you are required to pass at least 4 of the 6 assignments.

	Deadline
Assignment 1	14 Sep @ 10:00AM
Assignment 2	20 Sep @ 10:00AM
Assignment 3	27 Sep @ 10:00AM
Assignment 4	05 Oct @ 10:00AM
Assignment 5	12 Oct @ 10:00AM
Assignment 6	26 Oct @ 10:00AM

Exercises

Exercise Classes

- Tuesdays 13-17

TAs

- Oscar Nelin - Hold 1
- Ole-Christian Galbo Engstrøm - Hold 2
- Lasse Grønborg - Hold 3

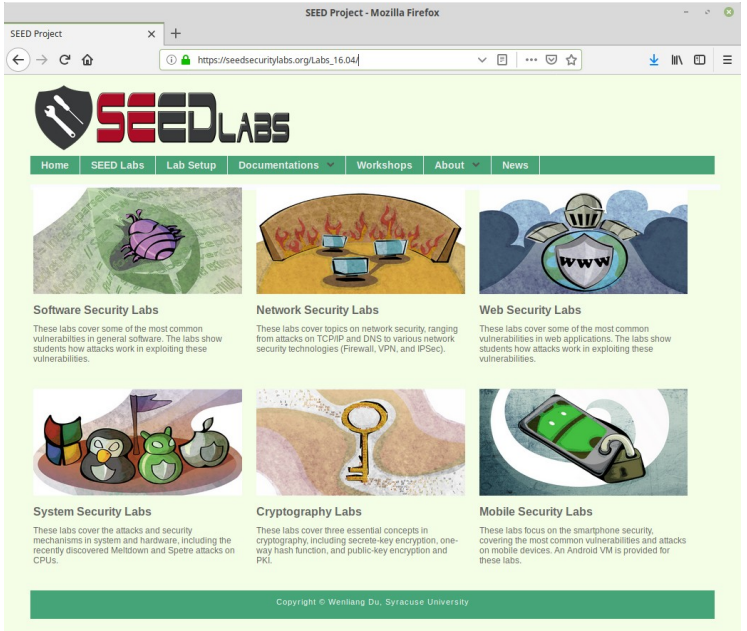
Rooms - Hold 1: DIKU 1-0-04, Hold 2: DIKU 1-0-14, Hold 3: DIKU 1-0-37

Exercises, *cont.*

Exercises include:

- Help getting started on the assignment.
- Feedback on the assignments.
- Optional SEED labs.

At some there will also be a recap of material relating to CompSys.



Exam

Nov 6 2019.

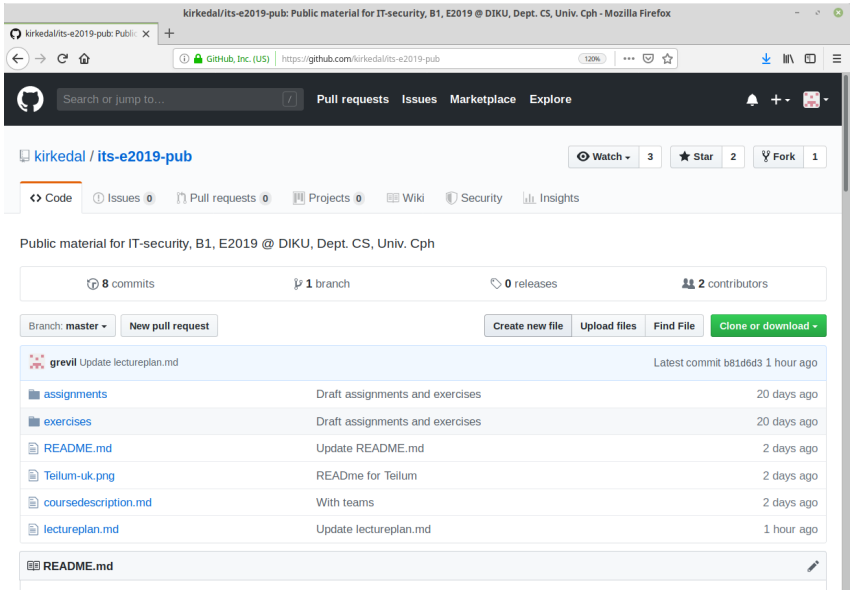
4-hour written exam.

All aids allowed except Internet.

(Oral re-exam.)

Course web site

Check out the course web site.



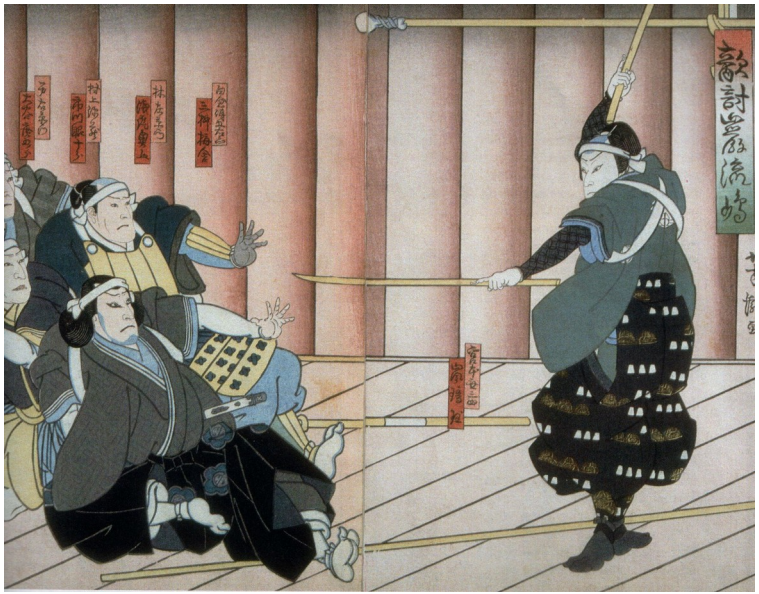
What you will learn

Introduction to the field of IT-security.

How to think about breaking systems.

And defending them from hackers.

Hands-on experience during exercises.



What this course is *not*

Not a course in how to hack stuff

Not the latest and greatest in hacks
– read the news

Not every aspect of IT-security
- we focus on breadth, not depth

Ethics and legal disclaimer

So, what is this IT-Security everybody talks about?

IT-security is many things

Firewalls

Cryptopgraphy

Software flaws

Code review

Reverse engineering

Security management

Passwords

Patching

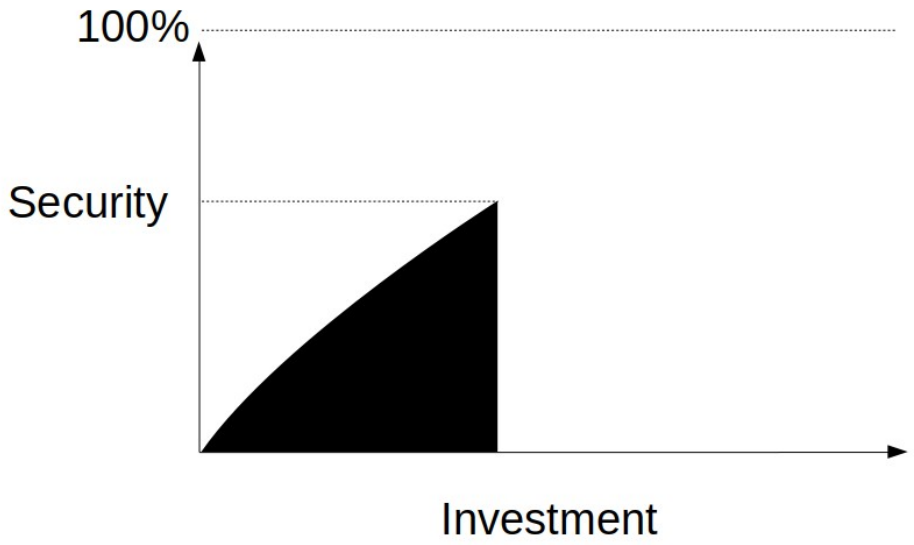
Threat models

Intrusion detection

Incident handling

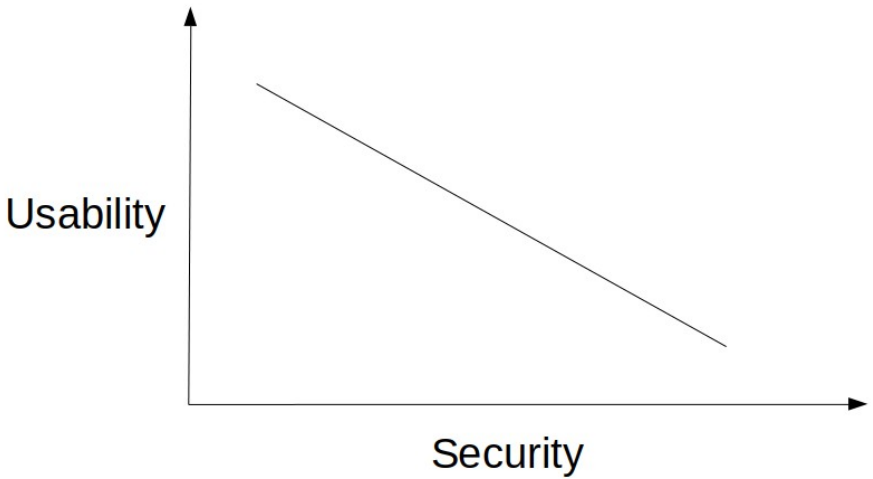
And much more

100% security is an illusion



Even big firms get hacked

And there’s a flip side - usability



Bad security

But does it have to be so? (Hint: No)

Balance security with the likelihood and consequences
of what you are afraid of could happen.

(We'll get back to that.)

Security vs business

November 20, 2015

69% of users would avoid security controls to make big business deals

Share this content: 

Some 69 percent of users would bypass security controls so they could win business.

Don’t make it too easy to bypass

Security *is* very important

WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION SIGN IN

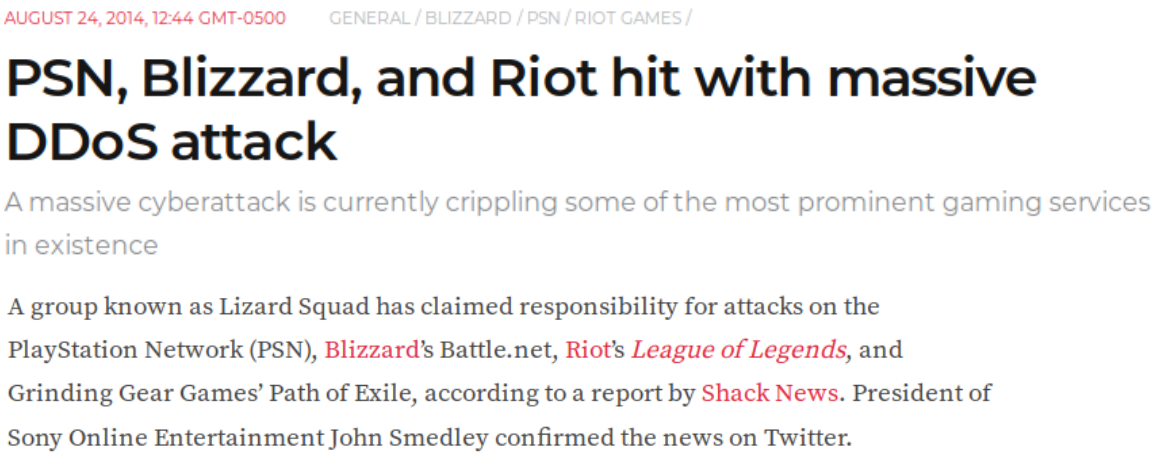
ANDY GREENBERG SECURITY 07.01.2017 08:00 AM

Security News This Week: How Shipping Giant Maersk Dealt With a Malware Meltdown

Petya ransomware, NSO malware, hacked wind farms, and more in this week's top security news.

What does IT-security mean to *you*?

Is this security?



AUGUST 24, 2014, 12:44 GMT-0500 GENERAL / BLIZZARD / PSN / RIOT GAMES /

PSN, Blizzard, and Riot hit with massive DDoS attack

A massive cyberattack is currently crippling some of the most prominent gaming services in existence

A group known as Lizard Squad has claimed responsibility for attacks on the PlayStation Network (PSN), Blizzard's Battle.net, Riot's *League of Legends*, and Grinding Gear Games' Path of Exile, according to a report by Shack News. President of Sony Online Entertainment John Smedley confirmed the news on Twitter.

Is this security?

GitHub hit by Massive DDoS Attack From China

Friday, March 27, 2015 Mohit Kumar

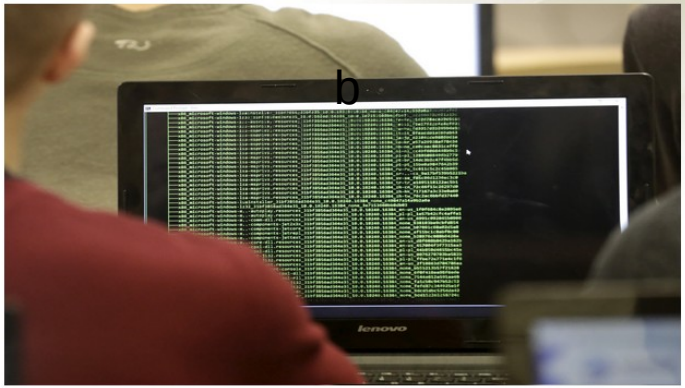
Github – a popular coding website used by programmers to collaborate on software development – was hit by a large-scale *distributed denial of service (DDoS) attack* for more than 24 hours late Thursday night.

Is this security?

15. DEC. 2015 KL. 14.41

Folketinget lagt ned af utrolig lille cyberangreb

Et såkaldt distributet denial of service-angreb har over flere omgange tvunget folketingets hjemmeside i knæ. Nu viser det sig, at angrebet var lillebitte.



Et lillebitte angreb lagde folketinget.dk ned. (Foto: Ints Kalnins © Scanpix)

Is this security?

DANMARK 28. SEP. 2012 KL. 15.37

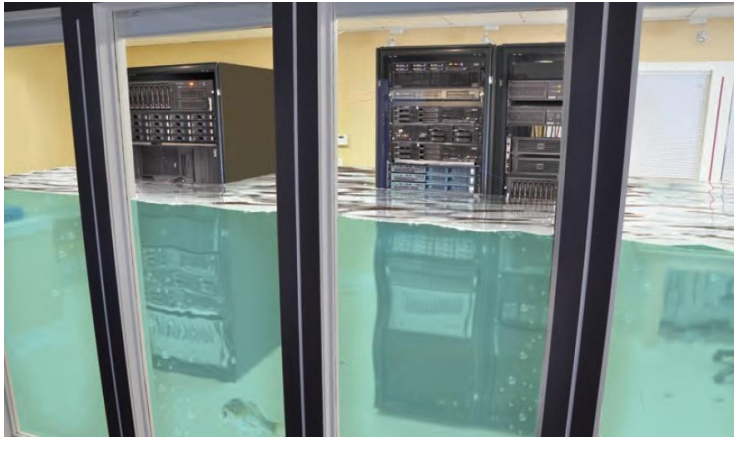
Hovedstadens sygehuse er ramt af stort it- og telefonnedbrud

Patienter på Rigshospitalet må belave sig på aflysninger og længere ventetid.

Is this security?

Massive Flooding Damages Several NYC Data Centers

BY RICH MILLER ON OCTOBER 30, 2012 26 COMMENTS



Is this security?

10 December 2012 Last updated at 12:13 GMT

Apple Maps 'is life-threatening' to motorists lost in Australia heat

Inaccuracies in Apple Maps could be "life-threatening" to motorists in Australia's searing heat, police have warned.

Officers in Mildura, Victoria, say they have had to assist drivers stranded after following the software's directions.

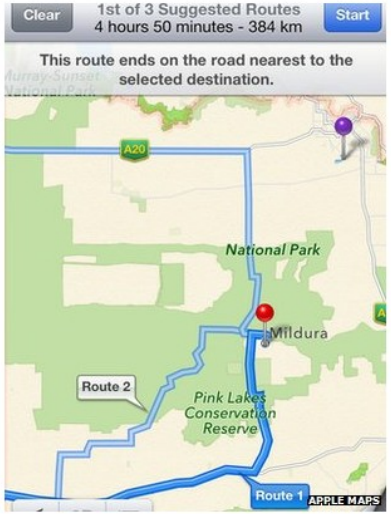
Some of the drivers had been without food or water for 24 hours.

Apple's software was heavily criticised by users when it was released in September.

Last week, chief executive Tim Cook admitted Apple had "screwed up" and was working to improve the program.

'No water supply'

In a press release, Victoria police's acting senior sergeant Sharon Darcy made her force's concerns clear.



Is this security?

Texas students hijack superyacht with GPS-spoofing luggage

Don't panic, yet

29 Jul 2013 at 18:04, Iain Thomson

Is this security?

SAMFUND

Kæmpe brøler: Over 5 mio danske CPR-numre leveret til kinesisk firma ved en fejl

20. jul. 2016, 14:07

Is this security?

Sony Breach Exposed Employee Healthcare Data, Salaries

MACK GELBER

Dec 2nd 2014 1:48PM

Security defined

So, computers fail for many reasons.

Reliability deals with accidental fails.

Usability deals with problems arising from operating mistakes made by users.

Security deals with intentional failures made by malicious parties.

Security is about computing in the *presence of an adversary*

A flat tire analogy

Key questions in security

What is important to me?

> My web site where customers go to buy, my research data, my production facilities, my pictures, my brand, my ...

Who threatens this? - And what are their motivations and capabilities?

Am I secure enough?

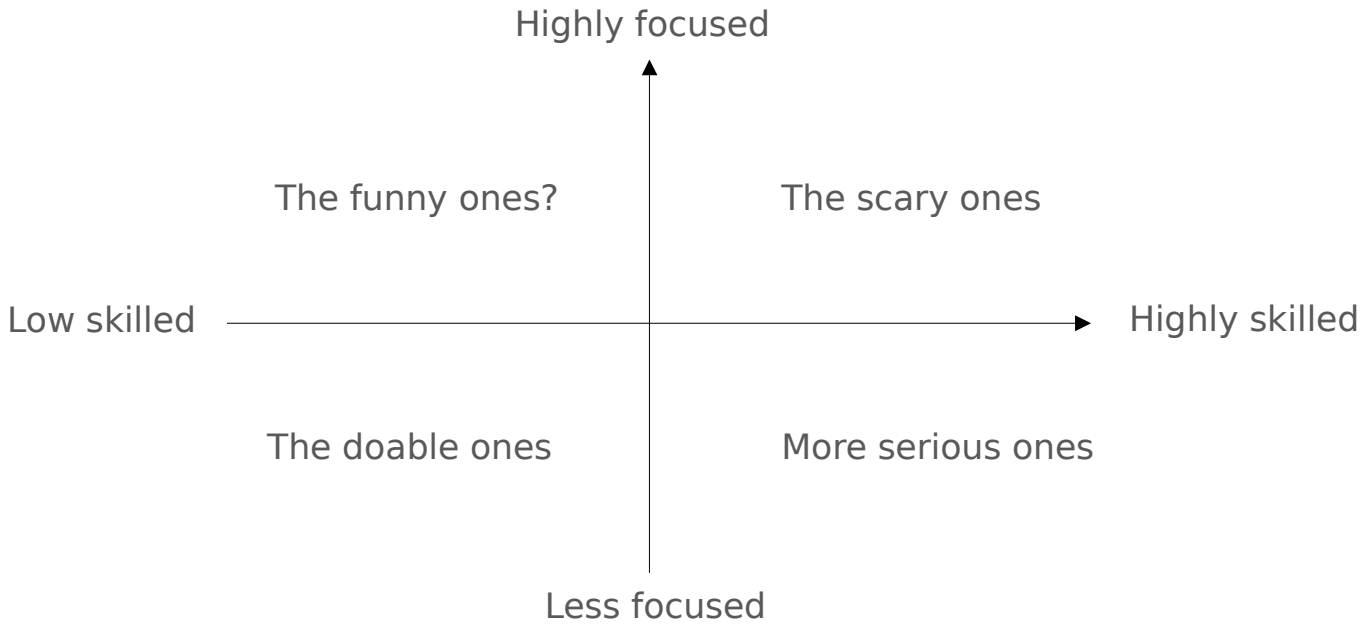
Plan, do, check, act. Repeat.

Security goals and their threats

STRIDE is threat model that helps to answer "what can go wrong in this system we're working on?"

Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Who hacks? (At a glance)



Who hacks?

Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

Hacktivists

Espionage

Cyber crime

A little bit about how hackers hack

The cyber kill chain

Some definitions and distinctions

Vulnerability: A bug in a piece of software

Exploit: Code that takes advantage of a vulnerability

Zero-day: Previously unknown vulnerability and/or exploit

Malware: Malicious software to maintain unauthorised access, gather private information, disrupt operation, delete data, etc.

TLDR; vulnerabilities are exploited to install malware

How hackers *most often* hack

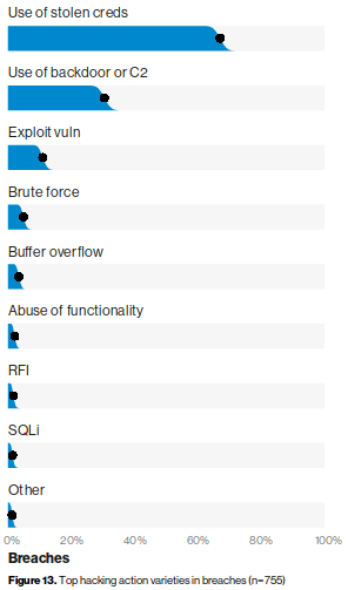


Figure 13. Top hacking action varieties in breaches (n=755)

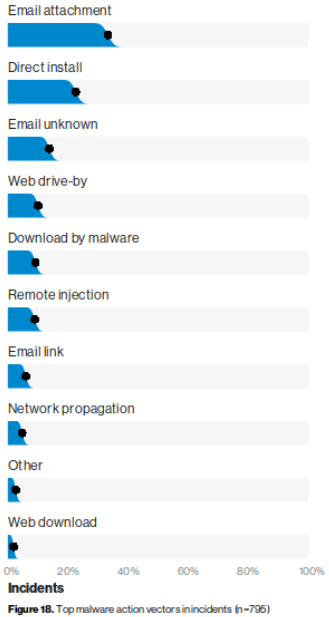
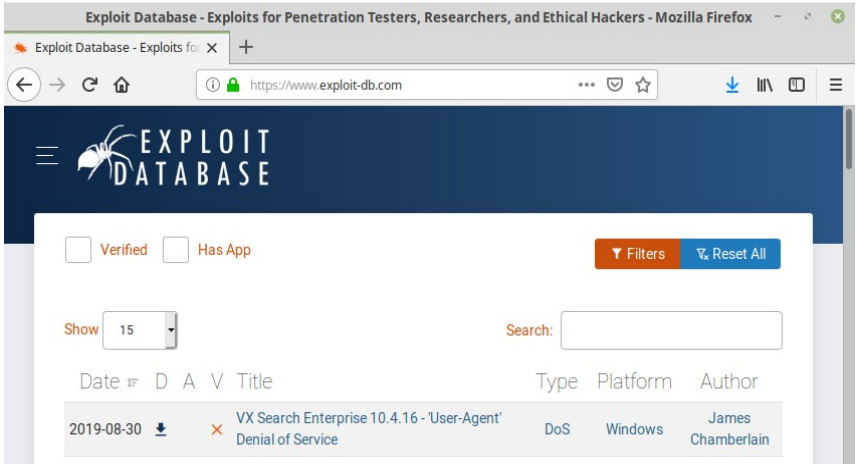


Figure 18. Top malware action vectors in incidents (n=795)

How hackers hack: Some tools



How hackers hack: More tools

KALI
BY OFFENSIVE SECURITY

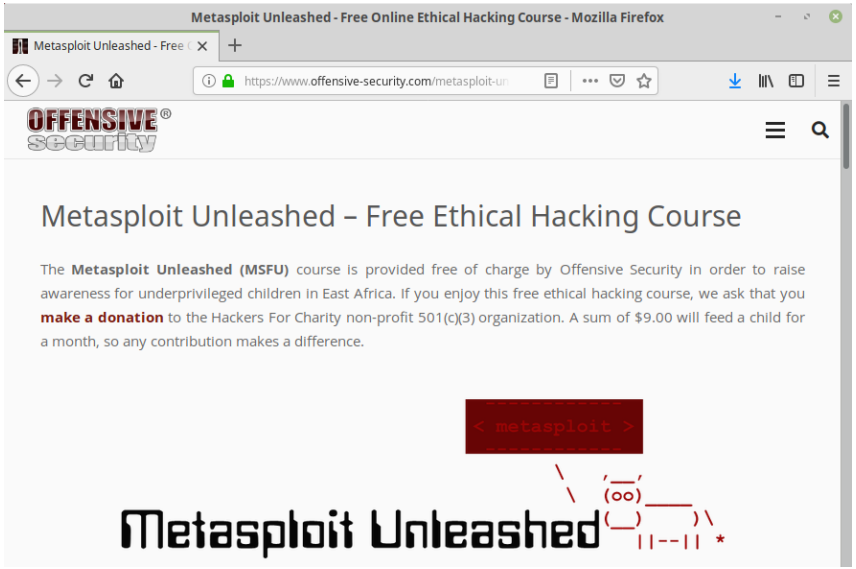
metasploit®

Or, Do It Yourself (DIY)

Find a new vulnerability and exploit it

(Next time.)

Try it yourself



A note on offense vs defense

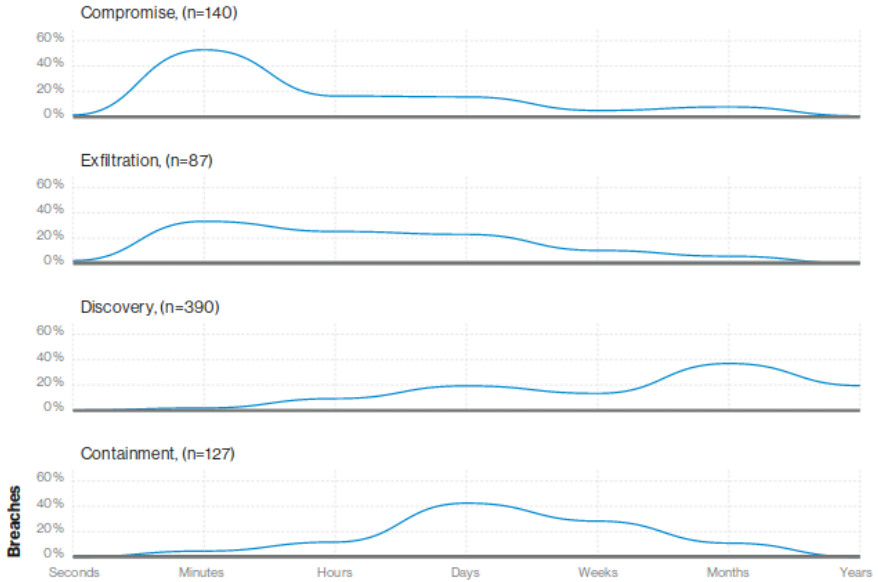
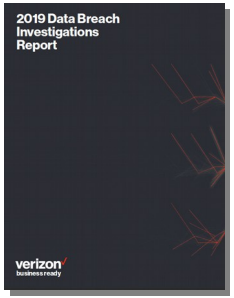
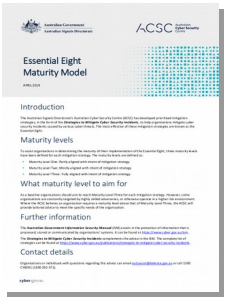


Figure 28. Breach timelines

What to do?

Study how breaches occur





And raise the bar according to your critical assets, threat picture and ambition level