



Welcome to

1. Introduction to hacking and pentest methods

KEA Kompetence Penetration Testing 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse  

Slides are available as PDF, kramse@Github

1-pentest-methods-kea-pentest.tex in the repo security-courses

Plan for today



Subjects

- Terminology and methods
- Red, blue and purple teams
- Present hand-in assignment

Exercises

- Try a system for writing pentest reports
- A little bit of Google hacking database

Reading Curriculum:

- Grayhat chapters 1 and 6-9

Do you like the books?

Goals for today



Don't Panic!

- Introduce the term penetration testing and basic pentest methods
- Introduce some of the basic tools in this genre of hacker tools
- Give an insight into the process of doing security testing
- Create an understanding of hacker tools
- Show a hacker lab



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

Later in 1995 release 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>

Use hacker tools!



Port scan can reveal holes in your defense

Web testing tools can crawl through your site and find problems

Pentesting is a verification and proactively finding problems

Its not a silverbullet and mostly find known problems in existing systems

Combined with honeypots they may allow better security

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!

ISC2 code of ethics



Code of Ethics Preamble:

- The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principles.
- Advance and protect the profession.

CISSP certified people sign papers to this extent.

<https://www.isc2.org/ethics/default.aspx>

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

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

Introduction – terms and technologies



Sikkerhedstest / penetrationstest

Afprøvning af sikkerhedsforanstaltninger og evaluering af sikkerhedsniveau ved hjælp af IT systemer og *hackerværktøjer*

Kaldes tillige sårbarhedstest, sårbarhedsanalyse m.v.

Ekstern – udføres fra internet, typisk over WAN

Intern, inside, on-site – udføres hos kunden, typisk over LAN og bag firewall

<https://www.google.com/search?q=sikkerhedstest>

Blackbox, greybox og whitebox



- Forudsætninger og forudgående kendskab til miljøet
- Black Box testen involverer en sikkerhedstestning af et netværk uden nogen form for insider viden om systemet udover den IP-adresse, der ønskes testet. Dette svarer til den situation en fjendtlig hacker vil stå i og giver derfor det mest realistiske billede af netværkets sårbarhed overfor angreb udefra. Men er dårlig ressourceudnyttelse.
- I den anden ende af skalaen har vi White Box testen. I dette tilfælde har sikkerhedsspecialisten både før og under testen fuld adgang til alle informationer om det scannede netværk. Analysen vil derfor kunne afsløre sårbarheder, der ikke umiddelbart er synlige for en almindelig angriber. En White Box test er typisk mere omfattende end en Black Box test og forudsætter en højere grad af deltagelse fra kundens side, men giver en meget detaljeret og tilbundsgående undersøgelse.
- En Grey Box test er som navnet siger et kompromis mellem en White Box og en Black Box test. Typisk vil sikkerhedsspecialisten udover en IP-adresse være i besiddelse af de mest grundlæggende systemoplysninger: Hvilken type af server der er tale om (mail-, webserver eller andet), operativsystemet og eventuelt om der er opstillet en firewall foran serveren.

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.

Målgrupper:

- IT-afdeling og teknisk personale
- Ledelse, koncernledelse
- Eksterne revisorer, VISA PCI, offentligheden

Afleveringer:

- Rapport med tekniske anbefalinger og opsummering/checklister
- Executive summary

Goal is not to find a scape goat to blame – management allocates resources

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

Persongalleri, Godkendelse og tilladelse



Sikkerhedskonsulent – den konsulent der kommer ud til kunden

Inden en test kan udføres skal der indhentes tilladelser fra:

- Systemejer – den ansvarlige for et bestemt system
- Netværksejer – den ansvarlige for netværk hos kunden
- Driftorganisation – dem der driver systemerne
- Sikkerhedsansvarlig – den ansvarlige for sikkerheden hos kunden
- Kontaktperson udpeges – kundens ansatte som kan hjælpe med praktiske spørgsmål og skabe kontakt til de rette personer i kundens organisation

Planlægning af sikkerhedstest



Sårbarhedsanalysens omfang aftales på forhånd

- Scope – hvad skal testes
- Hvornår skal testes – indenfor et aftalt tidsrum, wall clock time
- Hvor testes fra – logfilerne vil afsløre IP-adresser
- Kan overskrides delvist – eksempelvis ved port 80 scan på samme subnet eller tilsvarende
- Skal der forsøges ude af drift angreb – DoS
- Se endvidere slide om Rules of engagement senere

Sårbarhedsanalysen omfatter (targets):

- 192.168.1.1 – firewall/router
- 192.168.1.2 – mailserver
- 192.168.1.3 – webserver
- Testen udføres i tidsrummet mandag 1. til fredag 5.
- Testere udfører *angreb* fra 192.0.2.0/28

Før konsulenten ankommer – forberedelse



Testplan med oversigt over targets og IP-adresser

Netværkstegninger og anden information som er aftalt oplyst

Hvor skal sikkerhedskonsulenten placeres ved insidetest – ikke i serverrum, tak :-)

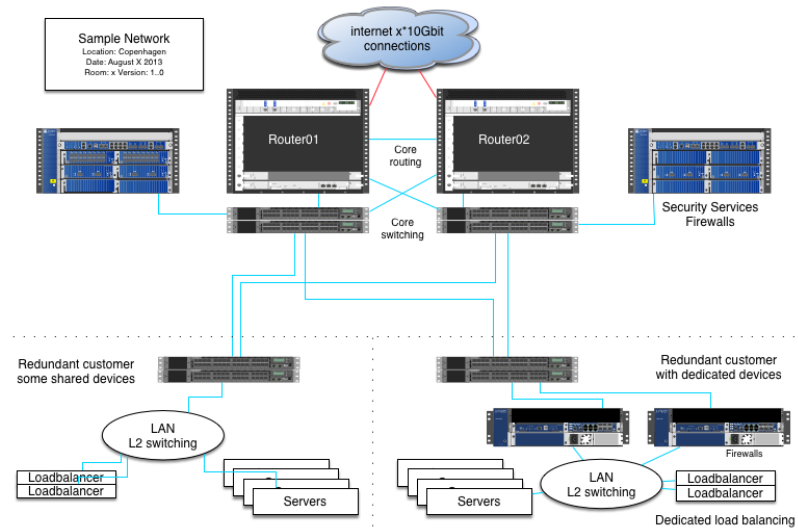
Kabling af netværksstik

Gæstekort – til test over flere dage

Kantine, toiletter osv.

Betragt det som en ny kollega – med tidsbegrænset kontrakt

Udvælgelse af systemer til test



- Routers på netværksvejen til kritiske systemer og netværk - tilgængelighed
- Firewall – begrænser trafikken tilstrækkeligt
- Mailservere – tillades relaying udefra
- Webservere – kan der afvikles kode på systemet, downloades data

Scannerudstyr på insidetest



Scannersystemer, hardware og software kræver en del ekspertise og opsætning. Det er tidskrævende at foretage denne opsætning og konsulenten har på forhånd udvalgt og konfigureret udstyr til testen. Det skal derfor accepteres at konsulenten tilslutter eget udstyr til de pågældende netværk og dette sker naturligvis under strenge krav til konsulentens udstyr.

Det er ikke en mulighed at bruge kundens udstyr!

Testens udførelse



Testen udføres ved samarbejde mellem konsulent og virksomhed

Først og fremmest skal testen startes

- Når konsulenten ankommer kontaktes kontaktpersonen
- Konsulenten vises til rette og pakker ud/stiller op
- Såfremt det ønskes inspiceres og godkendes udstyret
- Konsulenten tilslutter sig netværket og test er officielt igang
- Konsulenten verificerer adgangen til netværk og melder klar, begynder test

... tiden går ... testen udføres ...

Kontaktpersonen er hele tiden til rådighed på mobiltelefon

Testen afsluttes og der pakkes ned i modsat rækkefølge

Afbrydelse af testen – kompromitterede maskiner



Der kan være årsager der medfører at testen skal indstilles

Sikkerhedskonsulenten afbryder testen

- Det anses for uforsvarligt at fortsætte, der er fundet kompromitterede systemer eller beviser der kan ødelægges
- Netværket er dårligt, mulighederne for udførelse er forringet

Kunden ønsker at afbryde testen

- Der opleves for store problemer under udførelsen
- Systemnedbrud på forretningskritiske systemer
- Andre kriser der gør det valgte tidspunkt uegnet

NB: Eksempler! – man afbryder altid når kunden ønsker det!

Oprydning efter testen



Sikkerhedskonsulenten er ansvarlig for:

- Fjerne data fra systemerne
- Fjerne brugerkonti, få fjernet brugeroplysninger og loginmuligheder
- Fjerne software som ikke skal benyttes mere

Driftsorganisationen er ansvarlig for:

- Undersøgelse af systemerne
- Eventuel genstart af systemer, der kan være nedsat effektivitet
- Fjerne patchkabler for stik der er kablet speciet til konsulenten



Hvad indeholder en sikkerhedstest rapport:

- Titel, indholdsfortegnelse, firmanavne – ca. 15-30 sider for 5 hosts
- Fortrolighedserklæring – det er fortrolige oplysninger
- Executive summary – ofte i større virksomheder
- Information om den udførte scanning
- Omfang/scope
- Gennemgang af targets – detaljeret information og med anbefalinger
- Konklusion – ofte mere teknisk
- Bilag – detaljerede oplysninger og oversigter, checklister

Det er organisationen der selv vælger hvilke anbefalinger der følges

Rules of engagement – regler og etik for sikkerhedstest



- NB: Stor forskel på Danmark og udlandet!
- Sikkerhedskonsulenten må ikke give anledning til nye sårbarheder som følge af testen
- Sikkerhedskonsulenten må ikke installere ny software på systemer uden forudgående aftale
- Sikkerhedskonsulenten efterlader ikke usikre systemadministratorkonti eller tilsvarende efter testen
- Sikkerhedskonsulenten tager altid kontakt til kunden ved høj-risiko sårbarheder
- Er man hyret til netværkssikkerhed kan man godt *snuse* lidt rundt om systemerne under test – der kan være et sårbart testsystem lige ved siden af
- Min holdning er at ved opdagelse af åbenlyse sikkerhedsrisici dokumenteres disse i rapporten, uanset scope for opgaven ellers

Det er en balancegang

Konsulentens udstyr – vil du være sikkerhedskonsulent



Laptops, gerne flere, men én er nok til at lære!

- Sikkerhedskonsulenterne bruger typisk Open Source værktøjer på Linux og enkelte systemer med Windows – jeg bruger helst Windows 7 i dag
- Netværkserfaring *TCP/IP protocol suite* – TCP, UDP, ICMP osv. i detaljer
- Programmeringserfaring er en fordel
- Linux/Unix kendskab er ofte en **nødvendighed**
 - fordi de nyeste værktøjer er skrevet til Unix i form af Linux og BSD
- *A Hands-On Introduction to Hacking by Georgia Weidman, June 2014*
<http://www.nostarch.com/pentesting>
- Metasploit Unleashed – gratis kursus i Metasploit
<https://www.offensive-security.com/metasploit-unleashed/>

Hackerværktøjer



- Alle bruger nogenlunde de samme værktøjer, se også <http://www.sectools.org/>
- Portscanner Nmap, Nping – tester porte, godt til firewall admins <https://nmap.org>
- Generel sårbarhedsscanner Metasploit Framework <https://www.metasploit.com/>
- Specielle scannere – wifi Aircrack-ng, web Burpsuite, Nikto, Skipfish <http://portswigger.net/burp/>
- Wireshark avanceret netværkssniffer – <https://www.wireshark.org/>
- og scripting, PowerShell, Unix shell, Perl, Python, Ruby, ...

Billedet: Angelina Jolie fra Hackers 1995

Hvad skal der ske?



Tænk som en hacker

Rekognoscering

- ping sweep, port scan
- OS detection – TCP/IP eller banner grab
- Servicescan – rpcinfo, netbios, ...
- telnet/netcat interaktion med services

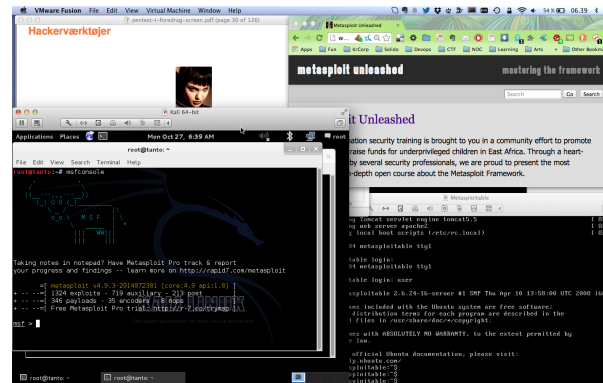
Udnyttelse/afprøvning: Metasploit, Nikto, exploit programs

Oprydning/hærdning vises måske ikke, men I bør i praksis:

- Lav en rapport
- Ændre, forbedre og hærde systemer
- Gennemgå rapporten, registrer ændringer
- Opdater programmer, konfigurationer, arkitektur, osv.


I skal jo også VISE andre at I gør noget ved sikkerheden.

Hackertlab opsætning



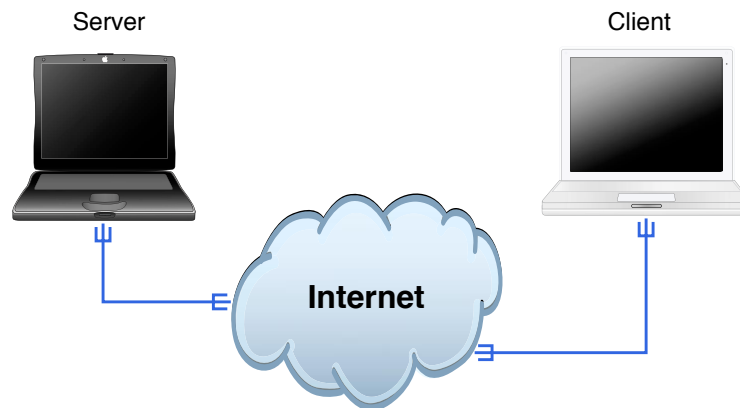
- Hardware: en moderne laptop med CPU der kan bruge virtualisering
- Husk at slå virtualisering til i BIOS
- Software: dit favoritoperativsystem, Windows, Mac, Linux
- Virtualiseringssoftware: VMware, Virtual box, vælg selv
- Hackersoftware: Kali som Virtual Machine <https://www.kali.org/>
- Soft targets: Metasploitable, Windows 2000, Windows XP, ...

Teknisk hvad er hacking



```
main(int argc, char **argv)
{
    char buf[200];
    strcpy(buf, argv[1]);
    printf("%s\n", buf);
}
```

Internet i dag



Klienter og servere

Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

Meget lidt kryptering, mest på http til brug ved e-handel

Trinity breaking in



```
80/tcp      open       http
81/tcp      open       hosts2-ns
10.0.0.0    [mobile]
11 # nmap -v -ss -O 10.2.2.2
11
13 Starting nmap V. 2.54BETA25
13 Insufficient responses for TCP sequencing (3). OS detection
13 accurate
14 Interesting ports on 10.2.2.2:
44 (The 1539 ports scanned but not shown below are in state: cl
51 Port      State      Service
51 22/tcp     open       ssh
58
68 No exact OS matches for host
68
24 Nmap run completed -- 1 IP address (1 host up) scanned
50 # sshnuke 10.2.2.2 -rootpw="210H0101"
Connecting to 10.2.2.2:ssh ... successful.
Re Attempting to exploit SSHv1 CRC32 ... successful.
IP Resetting root password to "210H0101".
System open: Access Level <9>
Na # ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

Meget realistisk - sådan foregår det næsten:

<https://nmap.org/movies/>

https://youtu.be/51lGCTgqE_w

Hacking er magi



Hacking ligner indimellem magi

Hacking er ikke magi



Hacking kræver blot lidt ninja-træning

Hacking eksempel – det er ikke magi



MAC filtrering på trådløse netværk

Alle netkort har en MAC adresse – BRÆNDT ind i kortet fra fabrikken

Mange trådløse Access Points kan filtrere MAC adresser

Kun kort som er på listen over godkendte adresser tillades adgang til netværket

Det virker dog ikke 😊

De fleste netkort tillader at man overskriver denne adresse midlertidigt

og man kan aflæse de godkendte når de er aktive på netværket

Derudover har der ofte været fejl i implementeringen af MAC filtrering

Myten om MAC filtrering



Eksemplet med MAC filtrering er en af de mange myter

Hvorfor sker det?

Marketing – producenterne sætter store mærkater på æskerne

Manglende indsigt – forbrugerne kender reelt ikke koncepterne

Hvad er en MAC adresse egentlig

Relativt få har forudsætningerne for at gennemskue dårlig sikkerhed

Løsninger?

Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere

MAC filtrering



OSI og Internet modellerne



OSI Reference
Model

Application
Presentation
Session
Transport
Network
Link
Physical

Internet protocol suite

Applications HTTP, SMTP, FTP, SNMP,	NFS
	XDR
	RPC
TCP UDP	
IPv4	IPv6 ICMPv6 ICMP
ARP RARP	
MAC	
Ethernet token-ring ATM ...	

Kali Linux the pentest toolbox



The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - [What's new ?](#)

KALI LINUX
"the quieter you become, the more you are able to hear"

**PENETRATION TESTING,
REDEFINED.**

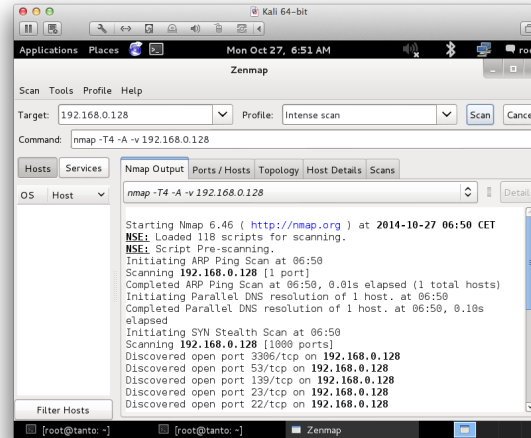
A Project By Offensive Security

Kali <http://www.kali.org/>

100.000s of videos on youtube alone, searching for kali and \$TOOL

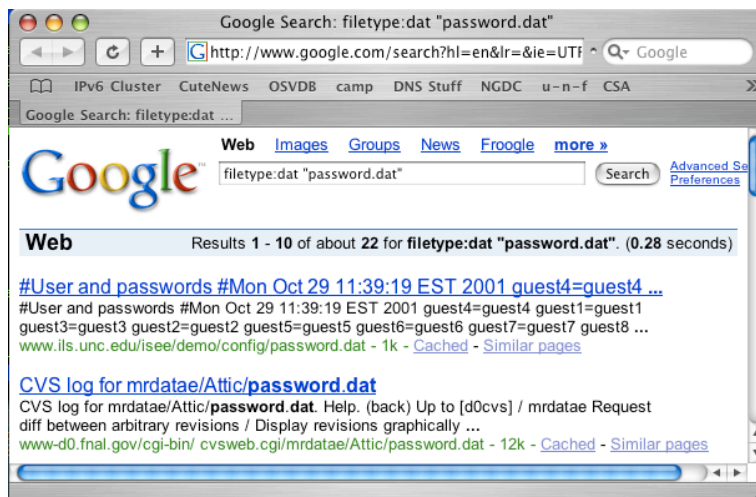
Also versions for Raspberry Pi, mobile and other small computers

Really do Nmap your world



- Nmap is a port scanner, but does more
- Finding your own infrastructure available from the guest network?
- See your printers having all the protocols enabled AND a wireless?

Getting to your data: Google for it



- Google as a hacker tool? oprindeligt beskrevet af Johnny Long
- Concept named googledorks when google indexes information not supposed to be public
- <http://www.exploit-db.com/google-dorks/>

Security devops



We need devops skillz in security

automate, security is also big data

integrate tools, transfer, sort, search, pattern matching, statistics, ...

tools, languages, databases, protocols, data formats

Use Github! Der er så mange biblioteker og programmer, noget eksisterende løser måske dit problem 90

Example introductions:

- Seven languages/database/web frameworks in Seven Weeks
- Elasticsearch the definitive guide

We are all Devops now, even security people!

Exercise

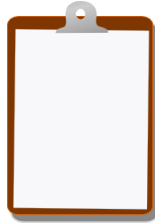


Now lets do the exercise

Try a system for writing pentest reports 30 min

which is number **3** in the exercise PDF.

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Most days have less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools