Welcome to

6. Managing Pentests and Vulnerabilities

KEA Kompetence Penetration Testing

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

6-managing-test-and-misc.tex in the repo security-courses

Plan for today

Subjects

- Terminology and methods

Exercises

- JuiceShop attacks
- a complete test, walk-through
- Exam trial

Reading Curriculum:

- Grayhat chapters 1 and 6-9

Reading Related resources:

- *Policies, governance and best Practice*

Goals for today

Don't Panic!

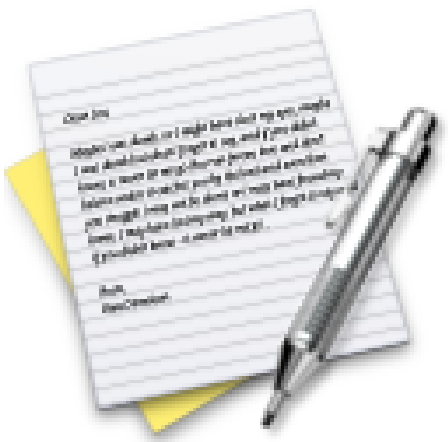
1h continue from last time, JuiceShop Attacks

1h a complete test, going through the process of investigating a network, decisions and alternatives during testing

1h Exam preparation, going over questions, trial exam

Continue from last time, Web Application Attacks

Exercise



Now lets do the exercise

JuiceShop Attacks 60min

which is number 21 in the exercise PDF.

A complete Test

1h a complete test, going through the process of investigating a network, decisions and alternatives during testing

Planlægning af sikkerhedstest

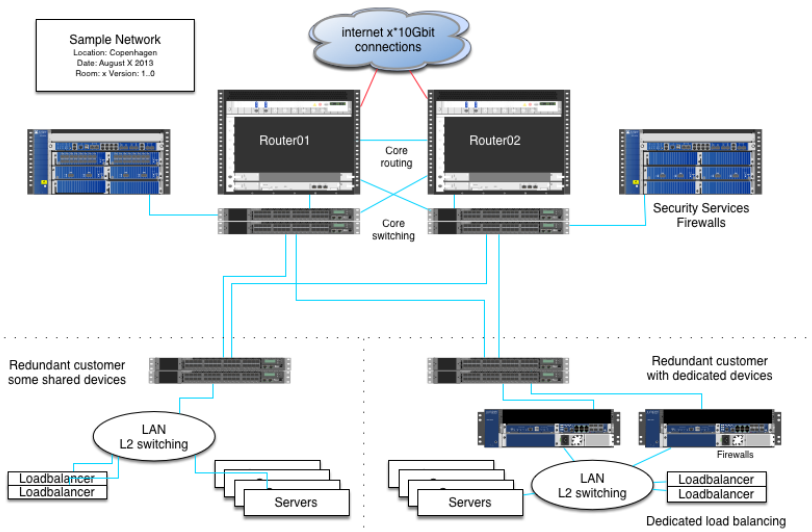
Sårbarhedsanalysens omfang aftales på forhånd

- 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):

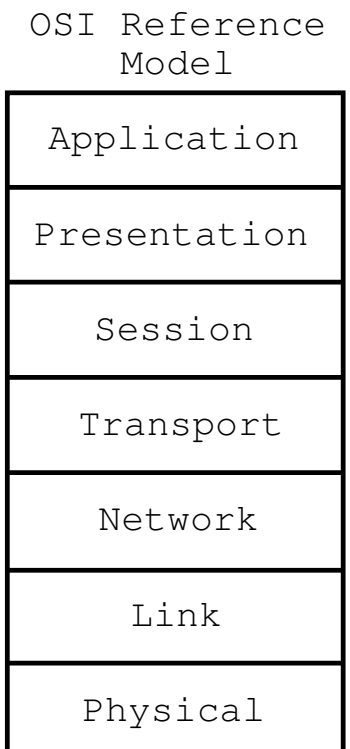
- 192.168.1.1 – firewall/router
- 192.168.1.2 – mailserver
- 192.168.1.3 – webserver
- Testen udføres i tidsrummet mandag 1. til fredag 5.
- Testere udfører *angreb* fra 192.0.2.0/28

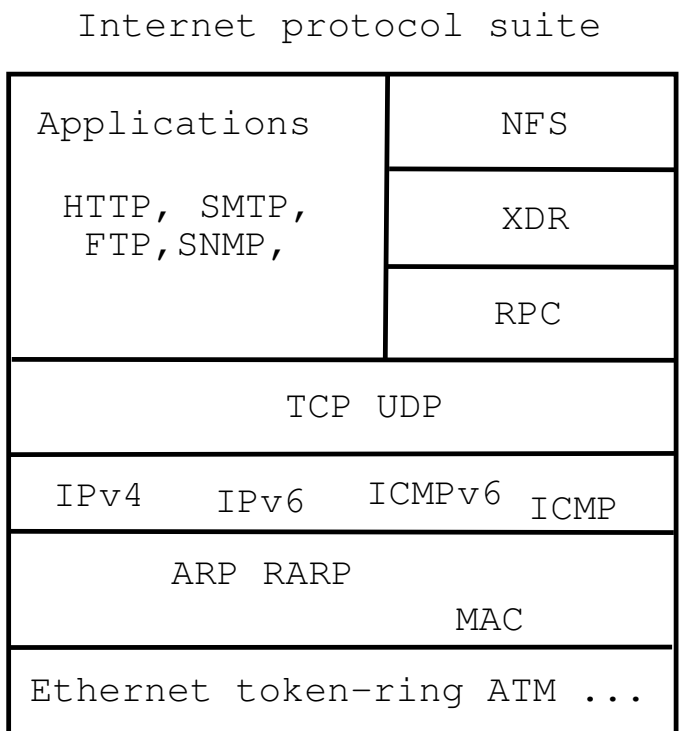
Udvælgelse af systemer til test



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

OSI og Internet modellerne





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.

Afrapportering – resultater

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

Exam preparation

Primary literature are these books and papers:

- *Gray Hat Hacking: The Ethical Hacker's Handbook*, fifth edition Allen Harper and others ISBN: 978-1-260-10841-5, May 2018, 640 pp.- shortened grayhat
- *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 - shortened LBfH
- *Smashing The Stack For Fun And Profit*, by Aleph One
- *Return-Oriented Programming:Systems, Languages, and Applications* Ryan Roemer, Erik Buchanan, Hovav Shacam and Stefan Savage University of California, San Diego

Deliverables and Exam

- Exam
- Individual: Oral based on curriculum
- Graded (7 scale)
- Draw a question with no preparation. Question covers a topic
- Try to discuss the topic, and use practical examples
- Exam is 30 minutes in total, including pulling the question and grading
- Count on being able to present talk for about 10 minutes
- Prepare material (keywords, examples, exercises, wireshark captures) for different topics so that you can use it to help you at the exam

- Deliverables:
- 1 Mandatory assignments
- Mandatory assignments are required in order to be entitled to go to the exam.

Eksamensemner

Eksamensemner til Pentest hos KEA Kompetence

Hjælp og keywords står under hvert emne.

Disse keywords vil IKKE være på sedlen inde i eksamenslokalet!

Pensum:
Bogens kapitler 1-3, 6-14, 22-25

Smashing The Stack For Fun And Profit, by Aleph One

Return-Oriented Programming:Systems, Languages, and Applications Ryan Roemer, Erik Buchanan, Hovav Shacam and Stefan Savage University of California, San Diego

Emner og keywords

- **1. Programming and basic buffer overflows**
  Trusler mod software, sårbarheder i software opstår, hvad er buffer overflow
- **2. Advanced Vulnerabilities**
  ROP mv. - en lille intro til buffer overflows vil være godt
- **3. Network spoofing**
  ARP spoofing, lav niveau, L2, MAC, og jeg ville tage lidt wifi sikkerhed - aflytningsdele med, Man in the middle angreb
- **4. Cracking Passwords and secrets**

- **5. Ethics and executing pentest**
  Hvordan udføres pentest, processen

Bemærk der er IKKE keywords inde i eksamenslokalet

Emner og keywords, fortsat

- **6. Vulnerability disclosure**
  Hvordan rapporteres vulnerabilities, Responsible disclosure, hvad kan man som firma gøre for at sikre at man får gode rapporter ind, bl.a. oprette abuse@ email :-D
- **7. Web application hacking**
  Tag udgangspunkt i juice shop måske, oversigter over sårbarheder i Web, OWASP
- **8. Metasploit**
  Forklare hvad Metasploit er og kan. Herunder afvikling af test og udvikling af shell code - at man ikke selv skal skrive, fordi det er inkluderet
- **9. SSL/TLS Secure Sockets Layer / Transport Layer Security**
  Web sikkerhed - krypteringsdelen, hvorfor, hvordan man tester, hvordan man fixer, hvordan skal web protokoller sikres i 2019
- **10. Kali Linux**
  Hvad er Kali Linux, hvad er fordelen ved Kali Linux, hvordan kommer man igang med Kali, osv.

Bemærk der er IKKE keywords inde i eksamenslokalet

Course Description

From: STUDIEORDNING Diplomuddannelse i it-sikkerhed August 2018

Indhold:
Den studerende lærer om hvordan en penetration test udføres, samt kan indhente oplysninger om de seneste sårbarheder, og kan benytte sig af de relevante værktøjer til dette formål.

Viden
Den studerende viden om og forståelse for:

- Etiske samt kontraktuelle forhold omkring en penetrationstest.
- Standardiseringorganisationers og myndigheders krav til og om penetrationstesting

Færdigheder
Tage højde for sikkerhedsaspekter ved at:

- Anvende relevante metoder ved udførsel af en penetrationstest
- Udarbejde en angrebsplan ud fra indsamlede oplysninger om et mål
- Finde sårbarheder i et givet system
- Dokumentere og rapportere fundne sårbarheder

Kompetencer Den studerende kan:

- Planlægge en penetration test, samt eksekvere den både ved brug af værktøjer og manuelt

Final word is the Studieordning which can be downloaded from

`https://kompetence.kea.dk/uddannelser/it-digitalt/diplom-i-it-sikkerhed`

`Studieordning_for_Diplomuddannelsen_i_IT-sikkerhed_Aug_2018.pdf`