# Testen von System- & Netzwerksicherheit


Seminar IT-Security HU Berlin 2004, Andreas Dittrich & Philipp Reinecke

# Gliederung

- Sicherheit im Allgemeinen
- Testbereiche
- Methodik und Standards
- Hilfsmittel im Speziellen
  - nessus
  - nmap
- Szenario im praktischen Teil

# Fragen zur Sicherheit

- Was ist sicher ?
  - vor was oder vor wem
  - in welchem Bedrohungsszenario
- Lässt sich Sicherheit realisieren ?
  - kontextbezogen
  - generell

# Fragen zur Sicherheit

- Lässt sich Sicherheit überhaupt testen ?
  - ein weites Feld...
  - wir zeigen einen Ansatz

# Testen von Sicherheit

- Externer Angriff
- Interne Sicherheitsprüfung
- Applikationsbezogene Sicherheitsprüfung
- WLAN/RAS-Prüfung
- Telefon & Sprachdienste
- Social Engineering

# Testen von Sicherheit

- Externer Angriff
  - fokussiert auf Internet-Server
  - 2 Phasen: Scan & Einbruch
- Interne Sicherheitsprüfung
- Applikationsbezogene Sicherheitsprüfung
- WLAN/RAS-Prüfung
- Telefon & Sprachdienste
- Social Engineering

# Testen von Sicherheit

- Externer Angriff
- Interne Sicherheitsprüfung
  - Test aus internen Netzsegmenten
    - Intranet, DMZ
- Applikationsbezogene Sicherheitsprüfung
- WLAN/RAS-Prüfung
- Telefon & Sprachdienste
- Social Engineering

# Testen von Sicherheit

- Externer Angriff
- Interne Sicherheitsprüfung
- Applikationsbezogene Sicherheitsprüfung
  - Suche nach Konfigurationsfehlern
  - losgelöst von der Netzinfrastruktur
- WLAN/RAS-Prüfung
- Telefon & Sprachdienste
- Social Engineering

# Testen von Sicherheit

- Externer Angriff
- Interne Sicherheitsprüfung
- Applikationsbezogene Sicherheitsprüfung
- WLAN/RAS-Prüfung
  - Sicherheit bei mobilem bzw. entferntem Arbeiten
  - Problem Wireless
- Telefon & Sprachdienste
- Social Engineering

# Testen von Sicherheit

- Externer Angriff
- Interne Sicherheitsprüfung
- Applikationsbezogene Sicherheitsprüfung
- WLAN/RAS-Prüfung
- Telefon & Sprachdienste
  - Angriffe auf äußere Einwahlpunkte
  - interne Telefonanlage
- Social Engineering

# Testen von Sicherheit

- Externer Angriff
- Interne Sicherheitsprüfung
- Applikationsbezogene Sicherheitsprüfung
- WLAN/RAS-Prüfung
- Telefon & Sprachdienste
- Social Engineering
  - „Psychologie des Hackens“

# Ansätze beim Testen

- Black Box
- Gray Box
- White/Crystal Box

# Ansätze beim Testen

- Black Box
  - nichts bekannt über das System
  - Testanfang dauert länger
  - „Security by Obscurity“
- Gray Box
- White/Crystal Box

# Ansätze beim Testen

- Black Box
- Gray Box
- White/Crystal Box
  - „Full Disclosure“

# Fragen zur Sicherheit

- Lässt sich Sicherheit testen ?
  - auf ein entsprechendes Szenario konzentriert nach bestem Wissen und Gewissen jein

# Methodik

- Standards
- Werkzeuge
- Rechtliches
- Report

# Methodik

- Standards
  - CHECK, OSSTMM, OWASP
- Werkzeuge
- Rechtliches
- Report

# Methodik

- Standards
- Werkzeuge
  - für jedes Szenario viele verschiedene
  - hier: nessus & nmap (dazu später)
- Rechtliches
- Report

# Methodik

- Standards
- Werkzeuge
- Rechtliches
  - Sensibilität von Daten
    - Datenschutz, Unternehmensgeheimnisse
  - Zerstörung von Daten/Systemen
    - vertraglich festzulegen
- Report

# Methodik

- Standards
- Werkzeuge
- Rechtliches
- Report
  - für wen wird der Report geschrieben ?

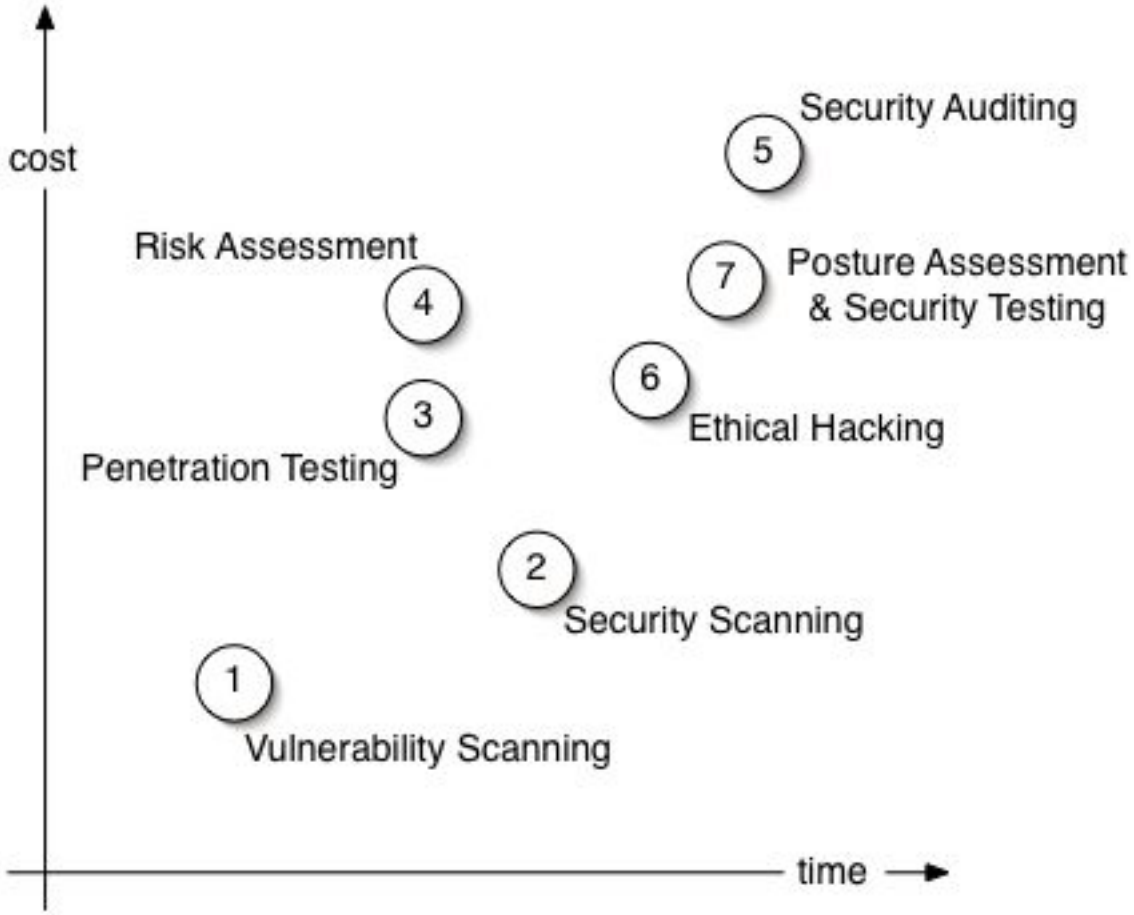
# Fragen zur Sicherheit

- Lässt sich Sicherheit testen ?
  - auf ein entsprechendes Szenario konzentriert nach bestem Wissen und Gewissen jein
  - Aufgabenbereich hochkomplex
    - Allgemeinwissen vonnöten
    - zusätzlich jede Menge Spezialistenarbeit
    - unsere Beschränkung auf ein Szenario

# Aus der Sicht der Wirtschaft

- Anforderungen
  - Erfahrung auf dem Gebiet
  - mehrere Standards
- Berater
  - Kaufmann und IT-Techniker
  - Arbeitgeber der Techniker

# Aus der Sicht der Wirtschaft



# Methodik

- Automatisierte Tests
- Manuelle Tests

# Automatisierte Tests

- Test der Systeme/Netze auf bekannte Schwachstellen
- Test der Netze auf Verstöße gegen Sicherheitsrichtlinien

# Automatisierte Tests

- Test der Systeme/Netze auf bekannte Schwachstellen
  - Welche Rechner sind sichtbar ?
  - Welche Services sind vorhanden ?
  - Gibt es (theoretische oder ausnutzbare) bekannte Sicherheitslücken darin ?
  - Sind Backdoors vorhanden ?
- Test der Netze auf Verstöße gegen Sicherheitsrichtlinien

# Automatisierte Tests

- Test der Systeme/Netze auf bekannte Schwachstellen
- Test der Netze auf Verstöße gegen Sicherheitsrichtlinien
  - Wie sieht das Netz tatsächlich aus?
  - Gibt es unbekannte Elemente?
    - Beispiel: Rogue Access Point
  - Existieren unbekannte Server?
    - Beispiel: eigene FTP-Server oder Windows-Freigaben

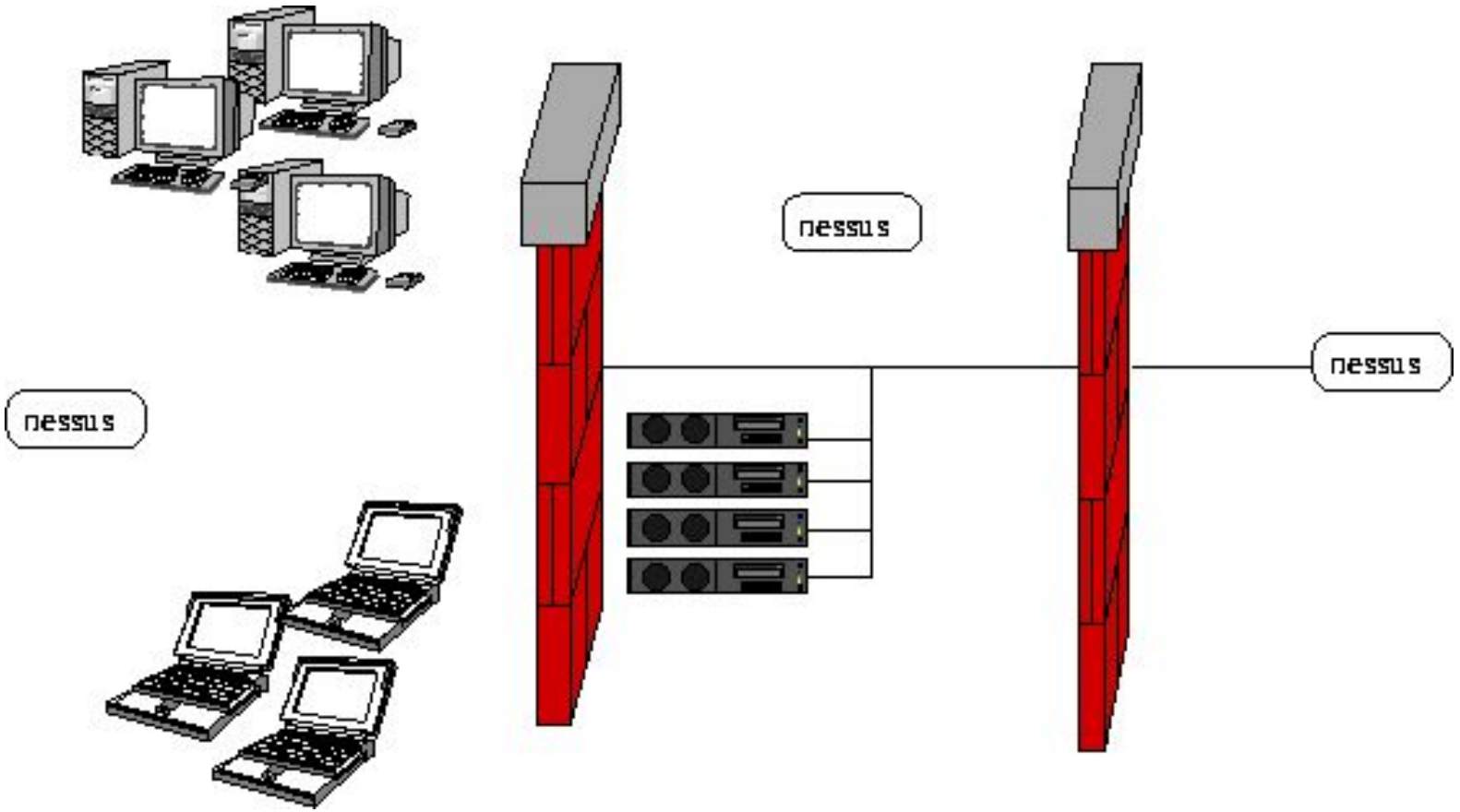
# Automatisierte Tests
# Beispiel Nessus

- im Nessus-Projekt unter Federführung von Renaud Deraison entwickelt
- Name bezeichnet unter anderem einen Zentaur der griechischen Mythologie und laut FAQ ein sicherheitsbesessenes Alien in „Ringworld“ von Larry Niven
- frei verfügbar, Leistungsumfang ähnlich kommerziellen Scannern

# Automatisierte Tests Beispiel Nessus

- Client-Server-Architektur
- Vorteile:
  - root-Rechte nur für Server
  - „Separation of concerns“ zwischen Administratoren von Teilnetzen
  - Server können an günstigen Orten plaziert werden
  - keine Beschränkung auf ein Betriebssystem
    - Bsp. NessusWX

# Nessus



# Nessus

- eigene Nutzer- und Rechteverwaltung:
  - `nessus-adduser, nessus-rmuser`
- Logins durch *Passwörter* oder Zertifikate gesichert
- verwendet SSL

# Nessus

- Anwendung:
  - Client starten, anmelden, Ziel angeben
  - Tests auswählen:
    - Sichere Tests: Prüfen nur passiv, beispielsweise anhand des Banners
    - Unsichere Tests: Versuchen, Lücken auszunutzen
  - Warten
  - Report lesen

# Nessus - NASL

- Wie werden Tests durchgeführt?
  - Tests sind Plugins, geschrieben in NASL:
    - Nessus Attack Scripting Language
  - NASL bietet Vorkehrungen gegen bösartige Server
    - bspw. Timeouts und Range-Checks
- Beispiel für sicheren Test ...

# Nessus - NASL

```
include("http_func.inc");

port = get_kb_item("Services/www");
if (!port) port = 80;
if(!get_port_state(port)) exit(0);

banner = get_http_banner(port: port);
if (!banner) exit(0);

serv = strstr(banner, "Server");
if(ereg(pattern:"^Server:.*Apache
(-AdvancedExtranetServer)\
   ?/2\.0\.([0-9][^0-9]|[0-3][0-9]|4[0-6])",
string:serv))
 {
   security_warning(port);
 }
```

# Automatisierte Tests

- Vorteile automatisierter Tests:
  - schnell, billig, gründlich
  - regelmäßig wiederholbar
- Nachteile automatisierter Tests:
  - Risiko der Beschädigung laufender Dienste und Systeme droht
  - fehlende Kreativität, nur bekannte Schwachstellen werden gefunden
  - auffällig
  - > Immer auch manuelle Tests nötig

# Manueller Test - Netzwerkscanner

- Aufgaben:
  - Netzwerkstruktur ergründen
  - laufende Dienste und deren Versionen herausfinden
  - Informationen über das Betriebssystem ermitteln, bspw. Name, Version und Uptime

# Manueller Test - Netzwerkscanner

- Aufgaben:
  - Netzwerkstruktur ergründen
    - `nmap 192.168.0.0/24`
  - laufende Dienste und Versionen dieser herausfinden
  - Informationen über das Betriebssystem ermitteln, bspw. Name, Version und Uptime

# Manueller Test - Netzwerkscanner

- Aufgaben:
  - Netzwerkstruktur ergründen
    - `nmap 192.168.0.0/24`
  - laufende Dienste und deren Versionen herausfinden
    - `nmap -sV 192.168.0.0/24`
  - Informationen über das Betriebssystem ermitteln, bspw. Name, Version und Uptime

# Manueller Test - Netzwerkscanner

- Aufgaben:
  - Netzwerkstruktur ergründen
    - `nmap 192.168.0.0/24`
  - laufende Dienste und deren Versionen herausfinden
    - `nmap -sV 192.168.0.0/24`
  - Informationen über das Betriebssystem ermitteln, bspw. Name, Version und Uptime
    - `nmap -O 192.168.0.0/24`

# Manueller Test - Netzwerkscanner

- Einige Tools
  - nessus http://www.nessus.org
  - SATAN (veraltet)
  - nmap http://www.insecure.org
  - p0f http://lcamtuf.coredump.cx/p0f.shtml
  - Metasploit Project http://metasploit.com/projects/Framework/downloads.html
  - John the Ripper http://www.openwall.com/john
  - telnet, netcat, Google, ...

# Manueller Test - Netzwerkscanner

- Hilfen:
  - WebAppTest CheatSheet:
    http://secguru.com/index.php/content/view/49
  - Reconnaissance CheatSheet:
    http://secguru.com/index.php/content/view/12

# Testen von System- & Netzwerksicherheit

## Fragen ?

# Quellen


- http://www.isecom.org/projects/osstmm.shtml
- http://www.securityfocus.com/infocus/1783
- http://www.penetration-testing.com/
- http://www.ee.oulu.fi/research/ouspg/sage/glossary/
- http://is-it-true.org/pt/
- http://www.cs.utk.edu/~dunigan/security.html
- http://www.deaddrop.org/security/Misc/penTestLinks.html
- http://www.linux-magazin.de/Artikel/ausgabe/2002/03/pentest/pentest.html
- http://www.insecure.org/nmap/nmap-fingerprinting-article.html