Hacker

Know the enemy

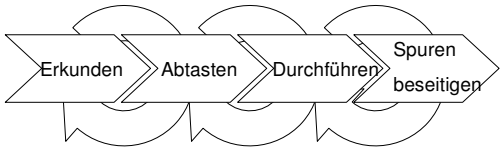
Motivation von Hackern

- Ehre und Lobpreisung durch Kollegen
- Nutzung fremder Ressourcen
- Erspähen von Informationen ggf. auch gegen Bezahlung
- Neugier
- Spieltrieb

Wer wird gehackt ?

- Jeder, der einen Server o.ä. an Netz betreibt,
- es ist keine Frage des OB sondern nur eine des WANN Mensch Opfer eines Versuchs wird
- Glauben Sie nicht ?
- Probieren sie es aus !

Vorgehen von Hackern



07.10.2004 4

Erkunden

- Stellenanzeigen
- „Vorsichtige„ Portscans
- Anrufe beim Admin
- Forschen in Newsgroups
- E-Mail an den Admin

07.10.2004 5

Abtasten

- Portscans mit OS Erkennung
- nmap
- languard
- telnet auf Port 80

07.10.2004 6

Durchführen

- Schwachstellen des erkannten OS ausnutzen
- Eigenen User einrichten
- User mit Root Rechten einrichten

Spuren vernichten

- Rootkit oder eingenudeltes Programm löschen
- ggf. Logdateien ändern
- Wenn möglich Trip Wire Daten ändern
- (Hoffentlich nicht)

Informationsquellen im Netz

- www.incidents.org
  - „Stand der Dinge“ in Sachen Angriffe z.Z.
  - Analysen über erfolgte Angriffe und Schwachstellen
- www.samspade.org
  - DNS, Whois, traceroute über Web Schnittstelle
- icat.nist.gov
  - Liste aller Schwachstellen zu einem Produkt
- www.iss.net - xforce
  - Alerts & Advisories zu Schwachstellen

CVE Nummern

- Jede bekannte Schwachstelle wird mit einer CVE Nummer (Common Vulnaribility Enumeration) versehen.
- Nach dieser Nummer lassen sich die Exploits aber auch die Gegenmassnahmen suchen und - i.d.R. - auch finden

Angriffe und deren Ziele

- Confidentiality
  - Ein solcher Angriff hat zur Folge, das sich das Vertrauensverhältnis gegenüber dem User - meist zu seinen Gunsten - geändert hat
  - Vertrauensstellung bei NT zwischen Hosts
  - Erweiterter Zugriff der User

Ziele

- Integrity
  - Backdoor Einbau d.h. verändern einiger Binaries durch eigene, creative Versionen
  - Folge: Angreifer loggt sich ein und kann durch Eingabe eines PW root Rechte erlangen

Ziele

- Availability
  - Die Erreichbarkeit eines Systems wird nachhaltig beeinträchtigt. Andere User sollen sich nicht mehr einloggen, mit dem Ziel selbst ungestört arbeiten zu können

Ziele

- Control
  - Erreichung der kompletten Kontrolle über den Server
  - Schliesst natürlich alle anderen Ziele ein ;-)

nmap

- Swiss Knife
- Portscanner der mit verschiedenen Optionen aus der Kommandozeile ausgeführt werden kann
- Doku siehe Paket

Nessus

- Open Source Security Scanner
- Benutzt nmap als Portscanner
- Findet Schwachstellen zu vorhandenen Betriebssystemen und Software
- Sehr laut
- Vorschläge zu Verbesserungen werden im HTML Format geliefert

07.10.2004

Dsniff

- Sniffer auf Netzwerkebene (ganz übles Teil!)
- Sucht gezielt nach Passwörtern in http, ftp und https Verbindungen
- Besteht aus vielen Tools mit denen der Netzwerkverkehr abgehört werden kann
- Doku siehe Paket

07.10.2004

ettercap

- Netzwerkanalyse
- Welche IP‘s befinden sich in einem Netzwerksegment
- Ermöglicht Man in the middle Attacks
- Kann ssh und https mitsniffen
- Passwort Collector für telnet, ssh usw...
- Doku siehe Paket

07.10.2004

Cheops

- Grafische Darstellung von Netzwerkverbindungen
- Komfortable Darstellung des vorhandenen Netzwerks
- Offene Ports werden dargestellt

07.10.2004

Tcpdump

- Netzwerkkarte in den Promiscous Mode
- Snifft unkomfortabel mit
- Die Mutter aller Sniffer

07.10.2004

ethereal

- Netzwerksniffer baut auf tcpdump auf
- Snifft gesamten Netzwerkverkehr mit
- Komfortable Darstellung der gewonnenen Ergebnisse

07.10.2004