ERNW
Enno Rey Netzwerke

# Penetrationstests – Herausforderung Sicherheit

IIR Internet Security Forum

25.–27. September 2001

**Enno Rey & Michael Thumann**

# Agenda

- Definition & Abgrenzung
- Sinn & Zweck
- Konzepte & Methoden
- Durchführung
- Ausblick

# Definition

- Ein Penetrationstest ist der *zielgerichtete* Versuch, mit den Mitteln eines *Angreifers* und innerhalb einer gegebenen Zeitspanne *Lücken in der IT-Sicherheit* aufzudecken.

Zu klären ist also...

- das *Ziel*, etwa ein Teil der IT-Infrastruktur (z.B. Internet-Präsenz/-Anbindung, Einwahl-Segment), ein Geschäftsprozess (e.g. E-Business) oder die korrekte Implementierung von Maßnahmen (zur Prävention, Angriffs-Entdeckung, Reaktion darauf)
- der *Typus des Angreifers* (extern/intern, Hacker/Mitbewerber/Ex-Angestellter etc.)
- was eine *Lücke der IT-Sicherheit* darstellt (Verletzung der Security Policy, Non-conformity gemäß BS 7799, Beeinträchtigung eines Geschäftsprozesses u.ä.)

# Abgrenzung

Ein Penetrationstest unterscheidet sich von einem *Audit...*

- i.a. in der Methodik (Einsatz von Tools & Techniken vs. Prüfung von Policies & Procedures)
- in seinem Aussagewert (Snapshot vs. umfassend & Richtlinien-konform)
- in seinem Zweck

# Sinn & Zweck

- Dan Farmer & Wietse Venema [1993]: „Improving the Security of Your Site by Breaking Into it" www.fish.com/security/admin-guide-to-cracking.html

- Sicherheitsbewußtsein (insbesondere beim höheren Management) zu schaffen
- Den IT-Sicherheitsprozeß einzuleiten oder zu stützen
- Risiken einschätzen zu können
- Vorhandene Maßnahmen (von außen) zu bewerten & sie ggf. zu verbessern

# Weitere Merkmale

Penetration-Tests können weiterhin unterschieden werden nach...

- dem Kenntnisstand des Angreifers/Testers [mit/ohne Kenntnis bestimmter Informationen (etwa Pass-wörtern), mit/ohne Einsicht in Dokumente]; die häufigste Variante ist hier die *zero-knowledge attack*.
- dem Zeitpunkt der Durchführung [im Normalbetrieb, zu ungewöhnlichen Zeiten (Weihnachten), vor bzw. nach Änderungen der technischen, administrativen oder personalen Strukturen]

# Durchführung

Ein Pentest wird in mehreren Phasen durchgeführt:

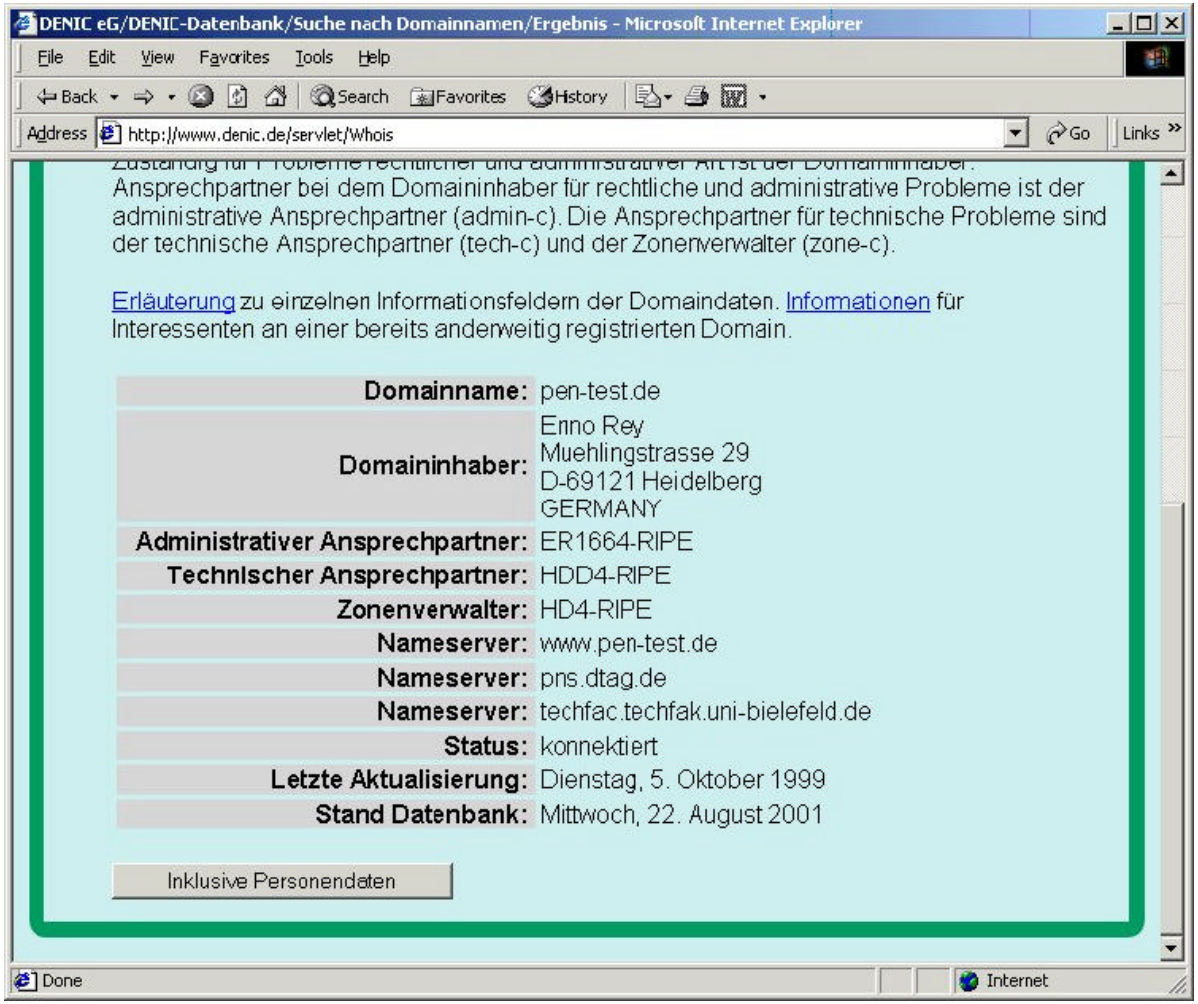
- Initiale Informationsgewinnung
- Detailliertere Untersuchung der Systeme
- Auflistung möglicher Sicherheitslücken
- Angriff nebst Privilegien-Erlangung & ‚Beweis‘
- Report
- Entfernen von Hinterlassenschaften (Tools, Logfiles)

# Initiale Informationsgewinnung

ERNW Enno Rey Netzwerke

- In dieser Phase werden möglichst viele, öffentlich zugängliche Informationen zusammengetragen, um erste Aussagen (etwa über die Infrastruktur) treffen zu können und das Ziel klarer eingrenzen zu können. Zu den Quellen zählen hier u.a.:
- whois-Informationen & öffentliche Datenbanken
- Struktur der Netzanbindung (*traceroute*, am besten mehrere)
- DNS-Informationen (idealerweise per Zonentransfer)
- Die Website des Ziels (möglichst umfassend, z.B. per *wget*)
- Eigene Logfiles mit Aktivität seitens des Ziels
- Mails, die vom/für‘s Ziel empfangen empfangen o. relayt wurden
- Postings an Newsgroups/Mailing-Lists durch Mitarbeiter des Ziels
- Homepages (oder Lebensläufe) von Mitarbeitern

# Initiale Informationsgewinnung



# Initiale Informationsgewinnung

```
C:\>tracert 195.145.236.252

Routenverfolgung zu 195.145.236.252 über maximal 30 Abschnitte

  1    60 ms    60 ms    80 ms  194.121.133.6
  2    60 ms    60 ms    80 ms  talos.ncc-mannheim.net [212.120.48.1]
  3    60 ms    60 ms    80 ms  S1-4-0.mhm2-c.mcbone.net [195.4.218.69]
  4   360 ms   100 ms    60 ms  L0.ffm2-c.mcbone.net [62.104.191.1]
  5   160 ms   160 ms   170 ms  G5-0.ffm4-gsr.mcbone.net [62.104.193.199]
  6   201 ms   210 ms   210 ms  L0.nbg2-gsr.mcbone.net [62.104.191.135]
  7   361 ms   330 ms   301 ms  L0.mch2-gsr.mcbone.net [62.104.191.134]
  8   170 ms    90 ms   120 ms  M-gw13.m.net.dtag.de [62.104.199.122]
  9    90 ms   110 ms    90 ms  MA-ag2.MA.NET.DTAG.DE [212.185.8.197]
 10   130 ms   140 ms   130 ms  016896-1-1-gw.MA.NET.DTAG.DE [62.225.84.205]
 11   120 ms   120 ms   100 ms  www.pen-test.de [195.145.236.252]
C:\>
```

```
[maint@mobile maint]$ dig axfr @195.145.236.252 pen-test.de

; <<>> DiG 8.2 <<>> axfr @195.145.236.252 pen-test.de
; (1 server found)
$ORIGIN pen-test.de.
@                   1H IN SOA www. Administrator. (
                                    3                   ; serial
                                    1H                  ; refresh
                                    10M                 ; retry
                                    1D                  ; expiry
                                    1H )                ; minimum

                    1H IN NS  www.
                    1H IN MX  10 mail
www                 1H IN A             195.145.236.252
@                   1H IN SOA www. Administrator. (
                                    3                   ; serial
                                    1H                  ; refresh
                                    10M                 ; retry
                                    1D                  ; expiry
                                    1H )                ; minimum

;; Received 5 answers (5 records).
;; FROM: mobile to SERVER: 195.145.236.252
;; WHEN: Wed Aug 22 12:18:01 2001
[maint@mobile maint]$ dig axfr @195.145.236.252 pen-test.de > pen-test.de.dns
[maint@mobile maint]$
```

# Initiale Informationsgewinnung

RE: [FW1] NT Printing through Firewall-1 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites History

Address http://www.firewall-1.org/2001-07/msg00362.html Go Links

```
Hi

I'm trying to set up my site so that an external site can print to my
internal printer.

I have set up an NT 4 machine on the DMZ that happily prints to the internal
printer (on a JetDirect box) via an internal NT 4 printserver.

The firewall is configured to allow any protocol (at present) through to the
DMZ print server.

The external site can ping the DMZ print server, and telnet to it.  But when
trying to print to it, it seems like only 72 bytes are sent and then
everything stops.

The firewall log shows one entry for each attempt viz:

14:47:17 accept firewall   >qe2 proto tcp src RemoteServer dst DMZServer
(Valid Address) service 9100 s_port 1223 len 48 rule 41 xlatesrc
RemoteServer xlatedst DMZServer xlatesport 1223 xlatedport 9100.

Can anyone give me any pointers please?


Regards,
Alan Baker

ISC Networks
Tel:     (Int +44) (0)1223 877068
Email:   mailto:Alan.Baker@europe.simoco.com
```

Done Internet

**Einladung?**

# Initiale Informationsgewinnung

[FW1] problem with snmp-fw1 daemon and snmpwalk query - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites History

Address http://www.firewall-1.org/2001-08/msg00141.html Go Links

- *From*: jrodriga@FW1-NOSPAMretevision.es
- *Date*: Mon, 6 Aug 2001 13:58:04 +0200
- *Sender*: owner-fw-1-mailinglist@FW1-NOSPAMlists.us.checkpoint.com

---

Hi to all,

when I use the snmpwalk command to ask to the snmp-fw1 agent (udp/260) from my snmp management console, it goes down and I have to restart it again. However, this doesn't happen with a snmpget query.

This is my CPFW1 version: Check Point VPN-1(TM) & FireWall-1(R) Version 4.1 Build 41814 [VPN + DES] SP3

Any idea about it?

Regards,

Josué.

La información incluida en el presente correo electrónico es CONFIDENCIAL,

Done Internet

?

# Detailliertere Untersuchung

ERNW Enno Rey Netzwerke

- Die in der ersten Phase ermittelten Ziele werden jetzt direkt geprüft („erster Feindkontakt“). Dabei werden avisierte Subnetze gescannt (etwa per *icmpenum*) und erreichbare Systeme auf offene Ports gescannt bzw. dem *OS-Fingerprinting* unterworfen.
- Einzelne Server (insbesondere Webserver) werden dann auf Versionsstände eingesetzter Dienste untersucht (per *banner grabbing* oder mithilfe dedizierter Scanner wie etwa *whisker).*
- In dieser Phase *können* Vulnerability-Scanner (sei es kommerzielle wie der *ISS* oder nicht-kommerzielle wie *Nessus*) zum Einsatz kommen. Es gibt jedoch gute Argumente dagegen:
- Der Pentest simuliert die Vorgehensweise eines Hackers (oder Mitbewerbers oder...). Sie alle arbeiten nicht mit solchen Tools.
- Vulnerability-Scanner sind in der Vorgehensweise viel zu *noisy* und im Ergebnis oft zu ungenau.

=> Fragen Sie bei Beauftragung eines Pentest nach den verwendeten Tools! Lautet die Antwort „Wir verwenden den ISS und einige andere Tools“, wird es wohl in erster Linie der ISS sein...

# Detailliertere Untersuchung

```
# nmap (V. 2.54BETA6) scan initiated Thu Feb  1 21:43:33 2001 as: nmap -sS -
    Ovv -p 1-1026 -oN /usr/local/data/nmap 195.145.236.252/30
Warning:  OS detection will be MUCH less reliable because we did not find at
    least 1 open and 1 closed TCP port
Interesting ports on www.pen-test.de(195.145.236.252):
(The 1024 ports scanned but not shown below are in state: filtered)
Port       State       Service
53/tcp     open        domain
80/tcp     open        http
443/tcp    open        https

TCP Sequence Prediction: Class=trivial time dependency
                         Difficulty=21 (Easy)

Sequence numbers: 1A6B7753 1A6B775A 1A6B776A 1A6B7771 1A6B77AB
Remote OS guesses: NT Server 4.0 SP4-SP5 running Checkpoint Firewall-1,
    Windows NT4 / Win95 / Win98
OS Fingerprint:
TSeq(Class=TD%gcd=1%SI=15)
T1(Resp=Y%DF=Y%W=2017%ACK=S++%Flags=AS%Ops=M)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=2017%ACK=S++%Flags=AS%Ops=M)
...
```

# Detailliertere Untersuchung

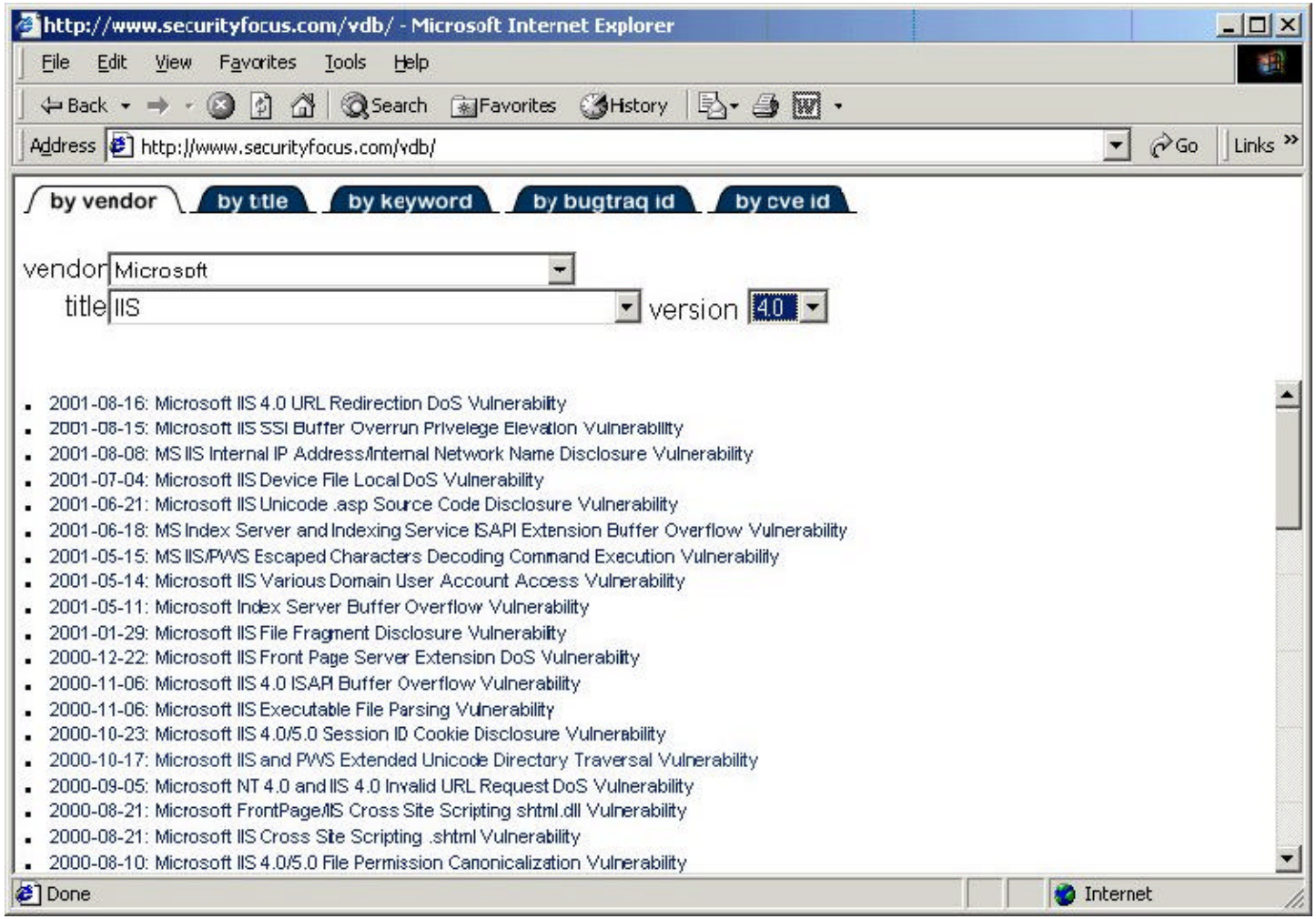
```
# whisker -inv -I 2 -M 1 -s /usr/local/src/whisker/SCAN.DB -h 195.145.236.252
      -- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net --
- Using IDS spoofing mode(s) 2

= - = - = - = - = - =
= Host: 195.145.236.252
= Server: Microsoft-IIS/4.0
- Appending ::\, %2E, or 0x81 to URLs may give script source
- Also try +.htr and %20%20.htw tricks
- Security settings on directories can be bypassed if you use 8.3 names

+ 200 OK: GET /msadc/Samples/selector/showcode.asp

+ 200 OK: GET /msadc/samples/adctest.asp

+ 200 OK: HEAD /msadc/msadcs.dll
- RDS.  See RDS advisory, RFP9902
- GIVE IT A REST, KIDS.

#
```

# Auflistung möglicher Sicherheitslücken

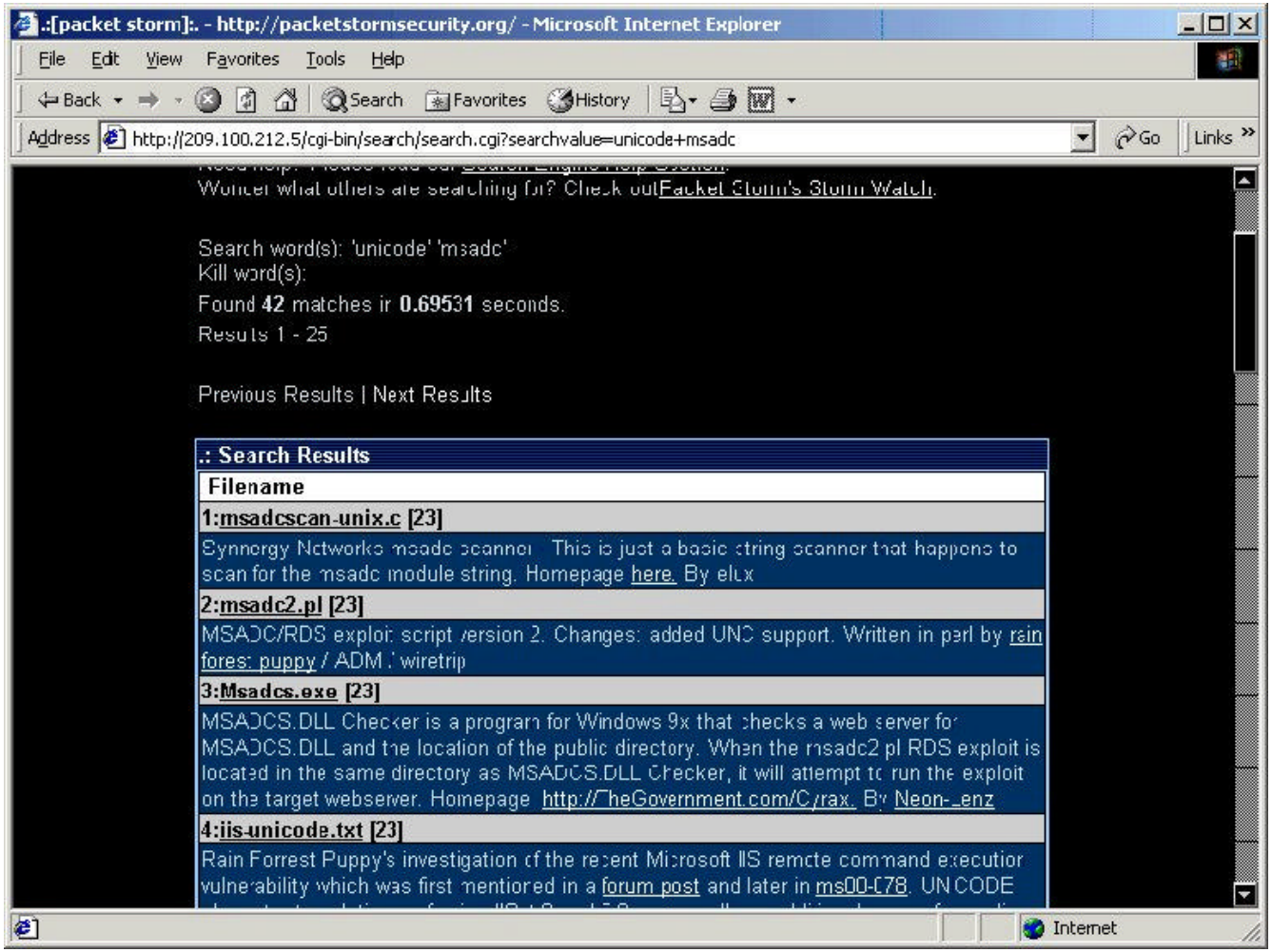
ERNW Enno Rey Netzwerke

- Anhand der (weitgehend automatisiert) gewonnenen Daten werden jetzt Profile potentiell angreifbarer Systeme erstellt.
- Einschlägige Foren (etwa *bugtraq*), Websites (Packet Storm, Technotronic, hack.co.za u.ä.) und Datenbanken sind hier die Informationsquellen.
- Darüber hinaus spielt das fach-spezifische Knowhow der/des Tester(s) eine entscheidende Rolle.
- Es müssen daher in das Test-Team entsprechende Köpfe eingebunden sein.
- => Prüfen Sie das!

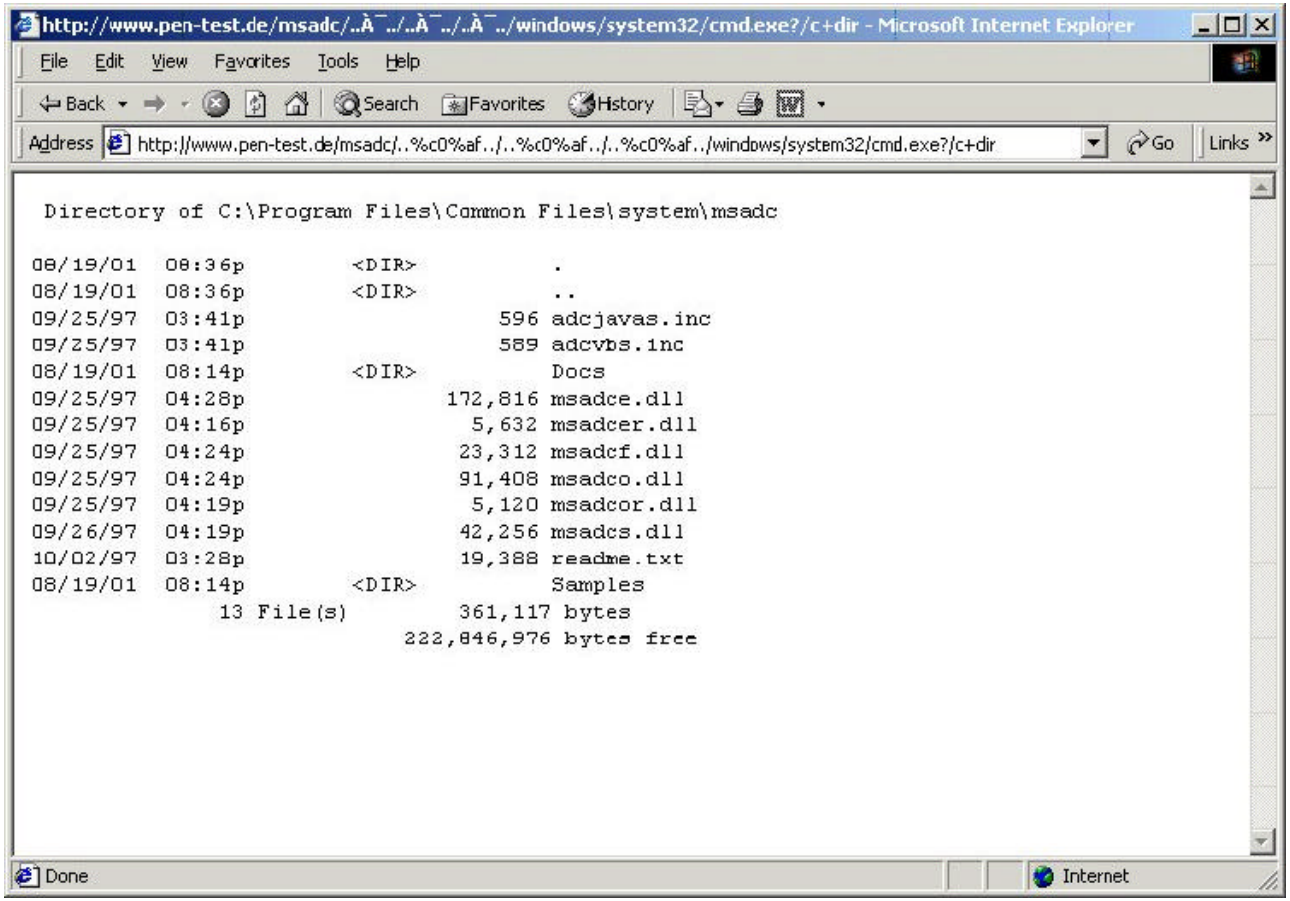
# Auflistung möglicher Sicherheitslücken



# Auflistung möglicher Sicherheitslücken

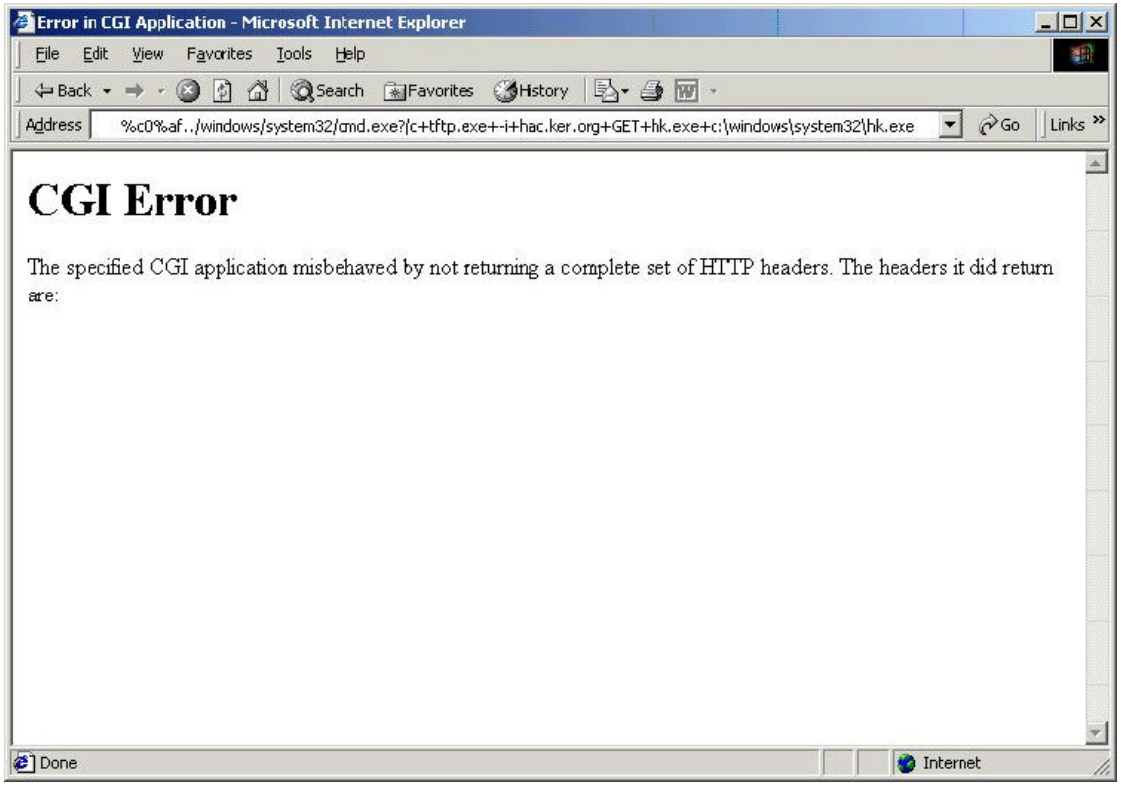


# Angriff & Privilegienerlangung




**Ausgenutzt wird die „Web Server Folder Traversal“-Lücke (MS00-078)**
**Fehler seitens des Opfers: Patch nicht installiert**

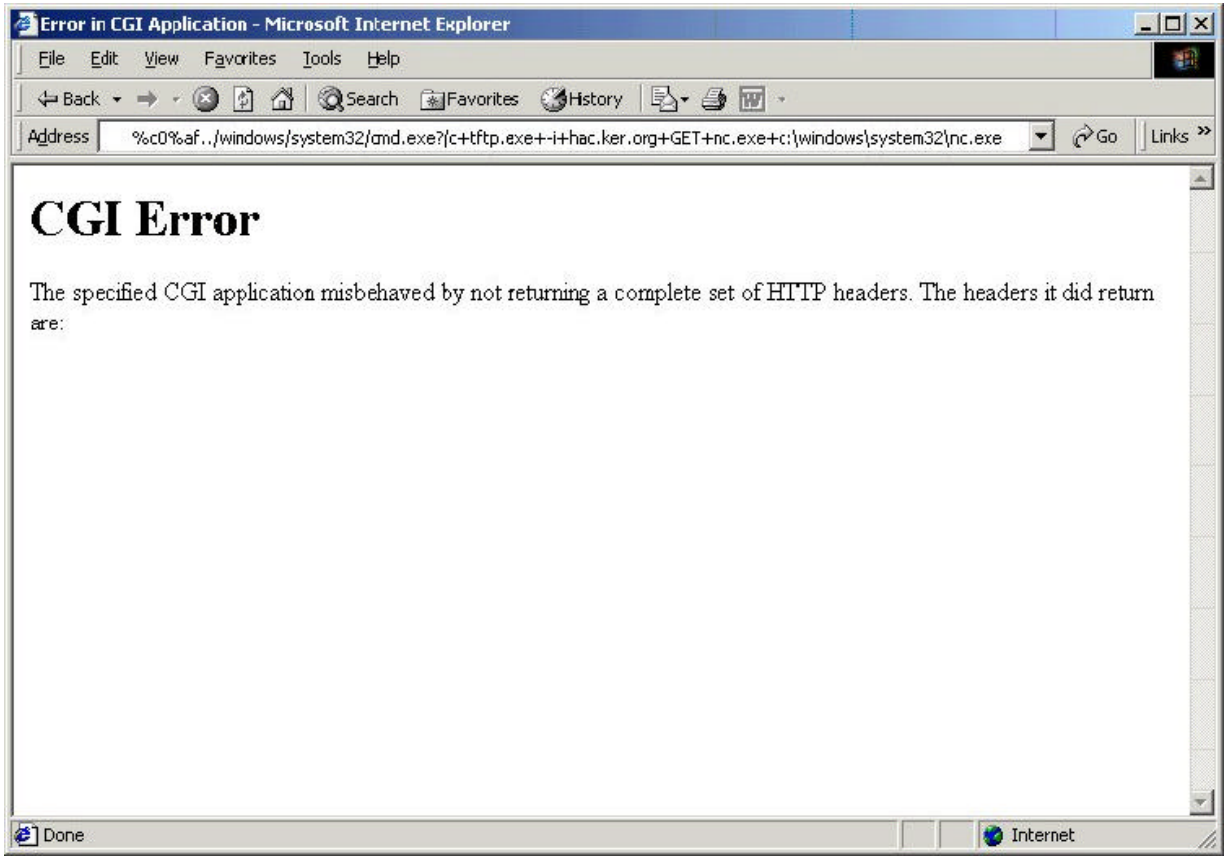
# Angriff & Privilegienerlangung




**Jetzt werden per TFTP zwei Tools (hk.exe, nc.exe) auf den Webserver kopiert**
**Fehler: DMZ wird als ‚trusted network' behandelt => Verbindung möglich**
**[Fehler wird insbesondere bei Einsatz der Cisco PIX gemacht, aber nicht nur...]**

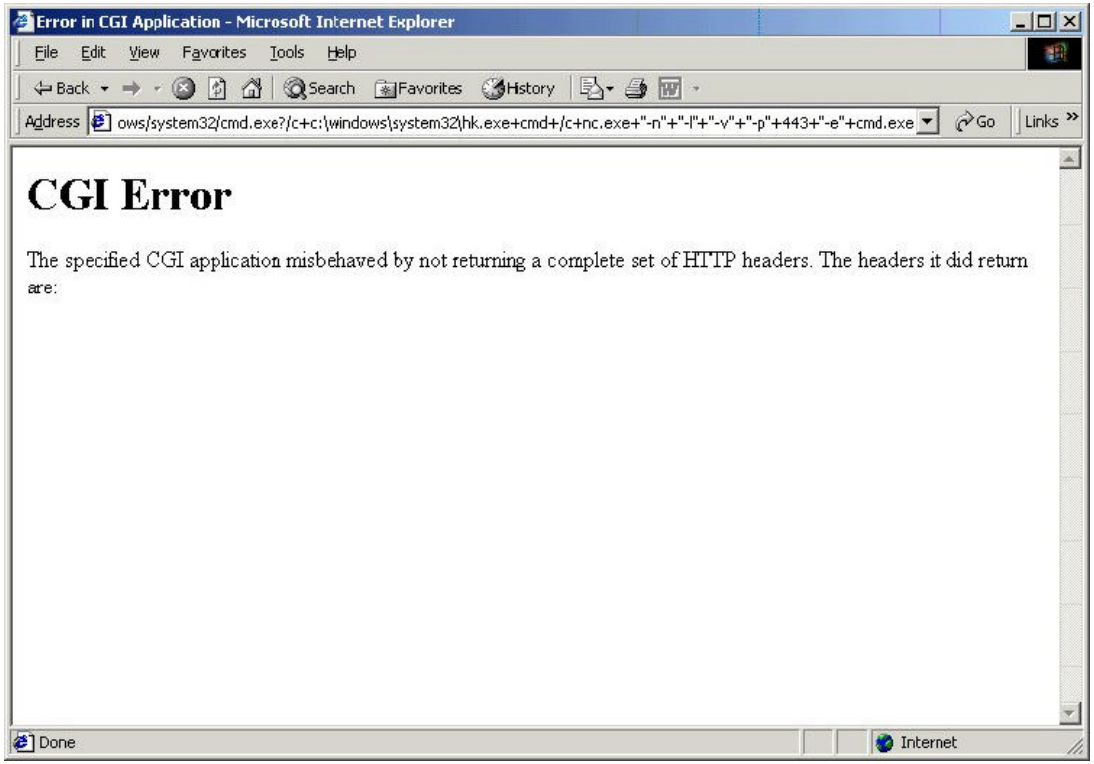
**hk.exe (www.nmrc.org/files/nt/hk-0.1.zip) verschafft *system*-Privilegien.**

# Angriff & Privilegienerlangung



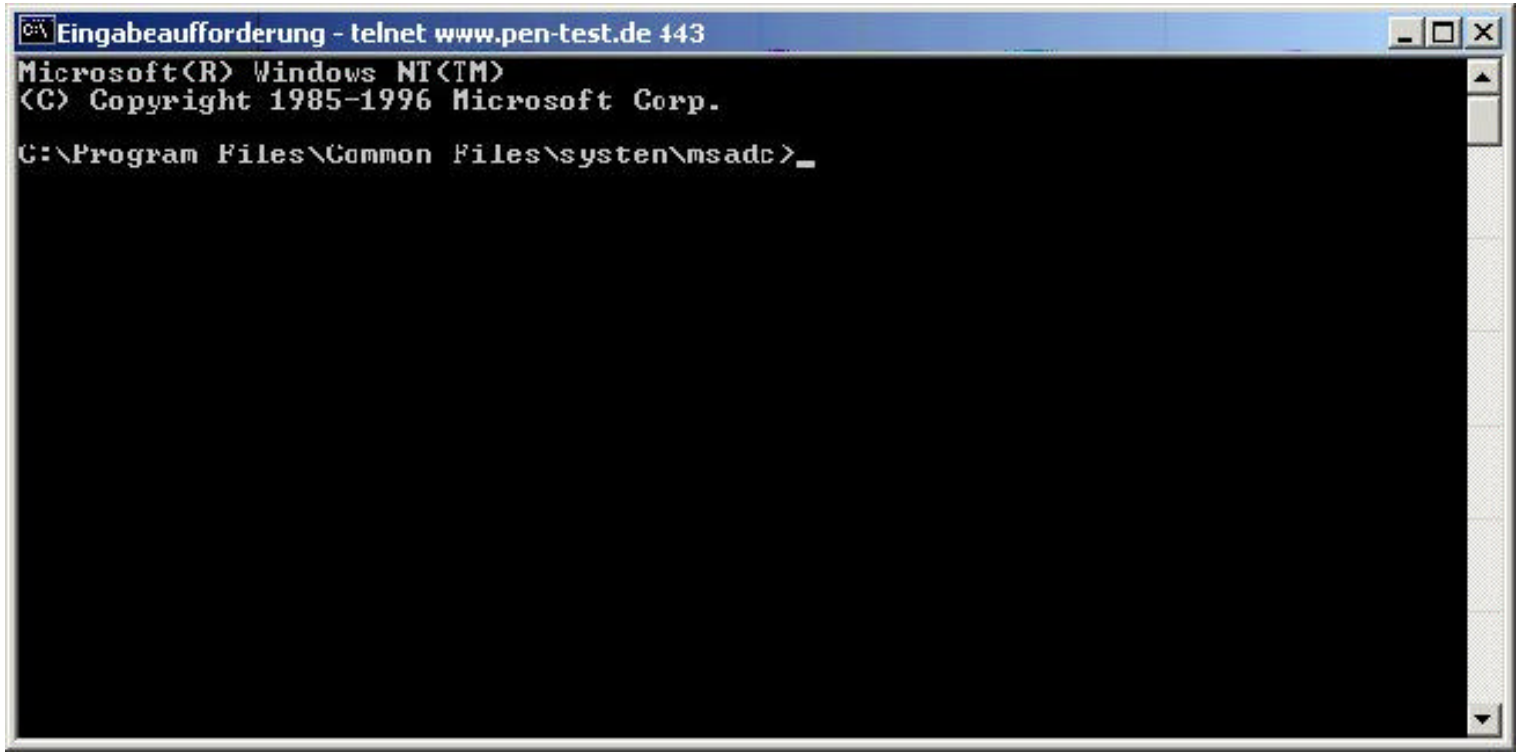

**netcat (www.l0pht.com/~weld/netcat/) ist das ‚Schweizer Taschenmesser' des Netzwerkers. Hier verwendet, um (Eingabe-) Daten zu transportieren...**

# Angriff & Privilegienerlangung




**Jetzt wird hk.exe verwendet, um netcat mit System-Rechten aufzurufen, das wiederum den Port 443 abhört und dort eine Shell (cmd.exe) bereithält, die natürlich ihrerseits diese Rechte hat...**
**Fehler: Post-SP6a-Fix nicht eingespielt, was hk.exe ermöglicht**
**Fehler: Port 443 wird v. der FW eingehend gestattet, obwohl kein SSL läuft**

# Angriff & Privilegienerlangung




**Ein telnet auf Port 443 ‚öffnet' diese Shell...**

# Angriff & Privilegienerlangung – Demonstration

ERNW Enno Rey Netzwerke

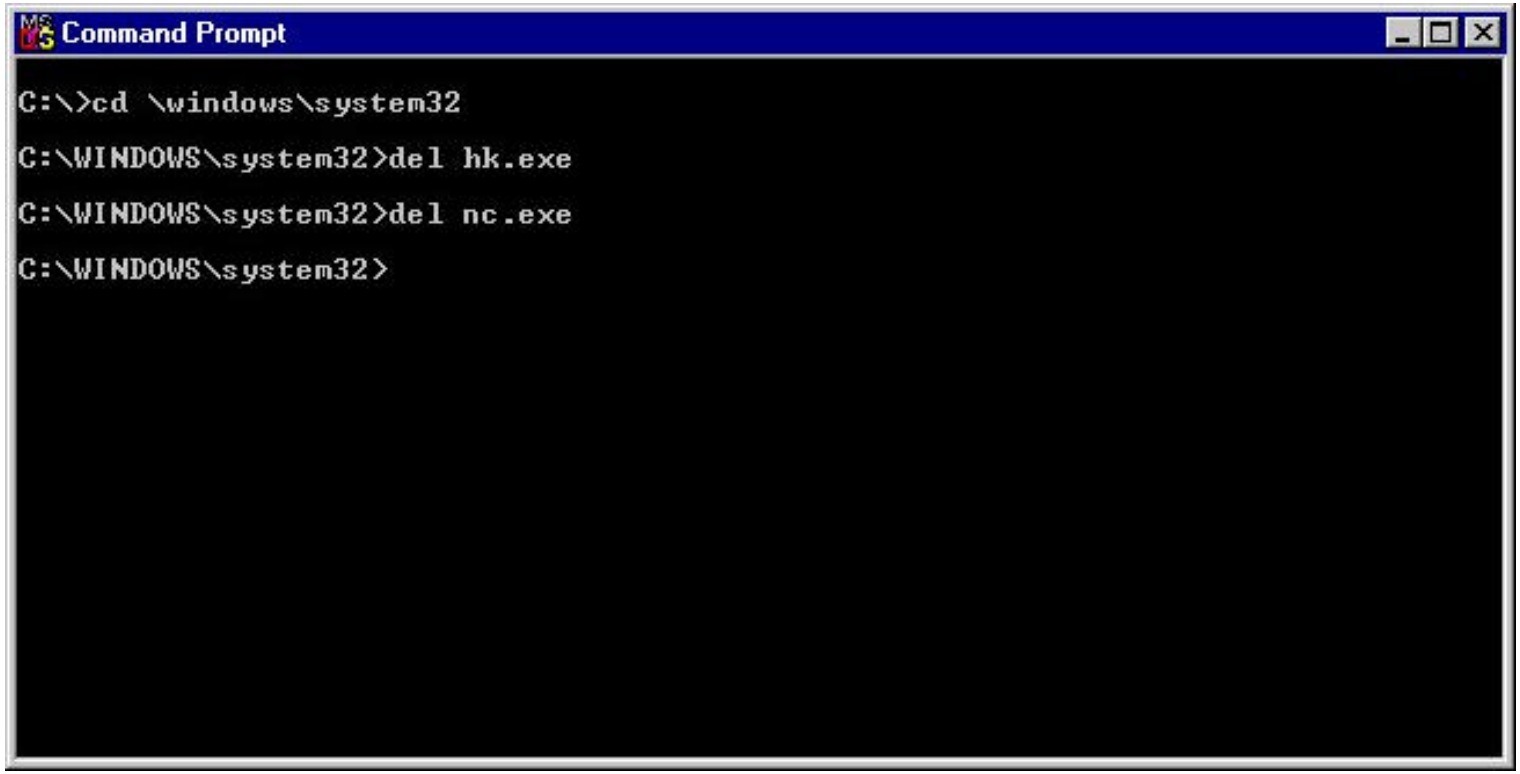
- Mithilfe dieser Shell können wir jetzt *alles* auf dem Zielsystem machen (*system*-Privilegien!), z.B.
- Eine modifizierte Zonendatei (die ja schon aus Phase 1 vorliegt) mit verändertem MX-Record auf dieses System laden, dann...
- den DNS-Dienst neu starten (net stop & start)...
- Wo werden denn jetzt wohl alle Mails an pen-test.de landen?

# Der Report

Der Report enthält:

- Eine genaue Beschreibung des Ziels des Pentests und der angewandten Verfahren
- Die konkrete Vorgehensweise in nachvollziehbarer und reproduzierbarer Form
- Eine (für Nicht-Techniker...) lesbare, abstrahierte Auswertung der Ergebnisse
- Richtlinien & Empfehlungen
- Die detaillierte Darstellung aller Testergebnisse

# Das Aufräumen



# Ausblick

- Penetrationstests werden sich (wie eben auch Angriffe) immer mehr auf die Applikationsebene bewegen.
- Weg von der Überprüfung der TK-Strukturen (etwa mit Wardialern) und auch weg von der Prüfung Netz/IP-Infrastruktur.
- Penetrationstests werden zukünftig VPN/IPsec-Knowhow erfordern.

# Danksagung & weitere Quellen

ERNW Enno Rey Netzwerke

- Weitere Quellen:
- Mailingliste *pen-test*: www.securityfocus.com/frames/?content=/forums/pen-test/intro.html
- Präsentation auf der *Black Hat* zu automatisierten Pentests:
- www.blackhat.com/presentations/bh-usa-01/IvanAcre/bh-usa-01-Ivan-Arce.ppt
- Dieser Präsentation verdanken wir wichtige Anregungen! Danke!

# Fragen

- Fragen?

# Danke

- Danke für Ihre Aufmerksamkeit!