

CITRIX AND TERMINAL SERVICES

**IAN VITEK
IXSECURITY**

FIRST WORDS

The new tools and this presentation
will be available for download at:
<http://www.cqure.net/itools01.html>

CITRIX AND TERMINAL SERVICES

- ▶ **What is Terminal Services**
- ▶ **How to abuse Terminal Services**
- ▶ **Scanning for non-public published applications. Tool: citrix-pa-scan**
- ▶ **Connecting to non-public published applications. Tool: citrix-pa-proxy**
- ▶ **Demonstration**
- ▶ **Statistics from a large scan**

WHAT IS TERMINAL SERVICES

- ▶ MS Terminal Services, Citrix, Tarantella and similar
- ▶ Remote multi-user desktop similar to Unix X
- ▶ Like "Sitting locally on a PC but over a network"
- ▶ Citrix can publish a specific application

HOW TO ABUSE TERMINAL SERVICES

- ▶ Several users are using different desktops on the same server
- ▶ Elevation of rights
- ▶ Breaking out from the given environment
- ▶ Some published applications are executable without a password

PUBLISHED APPLICATIONS

Normal scan:

- ▶ Where to find published applications
 - ▶ nmap for port 1494/tcp
 - ▶ Google for:
citrix demo password
nfuse demo password
- ▶ Use the Citrix client to enumerate published applications

PUBLISHED APPLICATIONS

Dump from normal PA enumerate:

CLIENT:32771 -> 193.11.12.13:1604

20 00 01 30 02 FD A8 E3 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

193.11.12.13:1604 -> CLIENT:32771

30 00 01 31 02 FD A8 E3 02 00 06 44 C1 0B 0C 0D
00 00 00 00 00 00 00 00 00 00 00 00 02 00 06 44
C1 0B 0C 0D 00 00 00 00 00 00 00 00 00 00 00 00

CLIENT:32771 -> 193.11.12.13:1604

2C 00 02 32 02 FD A8 E3 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 21 00 02 00
01 00 00 00 00 00 00 00 00 00 00 00 00

193.11.12.13:1604 -> CLIENT:32771

Published Applications

PUBLISHED APPLICATIONS

Non public Master Browser scan:

- ▶ Citrix servers can have non public Master Browsers (NAT or similar)
- ▶ Citrix client will try to connect to the Master Browser. This will fail.
- ▶ nmap for port 1494/tcp
- ▶ Use citrix-pa-scan to enumerate published applications

PUBLISHED APPLICATIONS

Dump non public Master Browser:

CLIENT:32771 -> 193.11.12.13:1604

20 00 01 30 02 FD A8 E3 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

193.11.12.13:1604 -> CLIENT:32771

30 00 01 31 02 FD A8 E3 02 00 06 44 0A 0B 0C 0D
00 00 00 00 00 00 00 00 00 00 00 00 02 00 06 44
0A 0B 0C 0D 00 00 00 00 00 00 00 00 00 00 00 00

CLIENT:32771 -> 10.11.12.13:1604

2C 00 02 32 02 FD A8 E3 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 21 00 02 00
01 00 00 00 00 00 00 00 00 00 00 00 00

No connection!

PUBLISHED APPLICATIONS

Citrix-pa-scan will just send third
packet to the Citrix server:

CLIENT:32771 -> 193.11.12.13:1604

```
2C 00 02 32 02 FD A8 E3 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 21 00 02 00
01 00 00 00 00 00 00 00 00 00 00 00 00
```

193.11.12.13:1604 -> CLIENT:32771

Published Applications

CONNECTING

Connecting to a published application with a non public Master Browser is "impossible" with the Citrix client

- ▶ Master Browser spoof and application server spoof is needed
- ▶ Can be done with citrix-pa-proxy
- ▶ Can be done with pas

CLIENT:32771 -> 193.11.12.13:1604

20 00 01 30 02 FD A8 E3 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

193.11.12.13:1604 -> CLIENT:32771

30 00 01 31 02 FD A8 E3 02 00 06 44 0A 0B 0C 0D
00 00 00 00 00 00 00 00 00 00 00 00 02 00 06 44
0A 0B 0C 0D 00 00 00 00 00 00 00 00 00 00 00 00

CLIENT:32771 -> 193.11.12.13:1604

4A 00 03 34 02 FD A8 E3 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 28 00 02 00
36 00 01 00 00 00 00 00 43 00 44 00 2D 00 52 00
4F 00 4D 00 00 00 01 00 04 00 74 00 72 00 61 00
70 00 70 00 65 00 72 00 00 00

193.11.12.13:1604 -> CLIENT:32771

3E 00 02 35 02 FD A8 E3 02 00 06 44 0A 0B 0C 0D
00 00 00 00 00 00 00 00 00 00 00 00 02 00 18 00
26 00 01 00 00 00 01 00 AF 02 02 00 06 44 0A 0B
0C 0D 00 00 00 00 00 00 00 00 00 00 00 00

PAS

You could directly connect to a published application with an ica file. The script pas will:

- ▶ Step through the output from citrix-pa-scan and create ica files
- ▶ Launch the ica file and record the result
- ▶ Fastest way to check hundreds of published applications

SUMMARY TOOLS

Citrix-pa-scan S1

C -----> S1 # Get PA!

C <----- S1 # One or more packets of PA

SUMMARY TOOLS

Citrix-pa-proxy S1

(Non public Master Browser is S2)

```
C -----> Pr # Master Browser?
Pr -----> S1 # Master Browser?
Pr <--- S2 --- S1 # Master Browser is S2!
C <--- Pr --- Pr # Master Browser is Proxy!
C -----> Pr # Run PA!
Pr -----> S1 # Run PA!
Pr <--- S2 --- S1 # Welcome at S2!
C <--- S1 --- Pr # Welcome at S1!
C -----> S1 # 1494/tcp Here we go!
```

DEMONSTRATION

- ▶ nmap scan
- ▶ citrix-pa-scan
- ▶ Connection with citrix-pa-proxy
- ▶ Connection with pas
- ▶ Break out from the given environment

STATISTICS

- ▶ Statistics from a larger scan
 - ▶ How many open 1494/tcp is out there?
 - ▶ How many have public published applications?
 - ▶ How many have non public published applications?
 - ▶ How many of the published applications is not password protected?

STATISTICS

How it was made:

- ▶ Several of millions IP addresses was tested
- ▶ Very short timeout values (140 ms)
- ▶ Server farms makes statistical errors

STATISTICS

- ▶ 42% of the servers had
server IP == Master Browser
(No proxy needed)
 - ▶ 44% of these servers had no
published application
- ▶ 58% of the servers had
server IP != Master Browser
(Proxy needed)
 - ▶ 37% of these servers had no
published application

PA STATISTICS

Servers that doesn't need a proxy and had published applications:

- ▶ Average: 12 PA/server
- ▶ 5% of PA; anonymous and vulnerable (20% of servers)
- ▶ <1% of PA; anonymous (2% of servers)
- ▶ 92% of PA required login
- ▶ 3% of PA gave unexpected error

PA STATISTICS

Servers that need a proxy and had published applications:

- ▶ Average: 16 PA/server
- ▶ 2% of PA; anonymous and vulnerable (10% of servers)
- ▶ <1% of PA; anonymous (1% of servers)
- ▶ 96% of PA required login
- ▶ 2% of PA gave unexpected error

PROTECTION?

- ▶ Do not publish applications
 - ▶ Firewall when needed
 - ▶ VPN
- ▶ Prevent attackers to break out from given environment
 - ▶ Strong ACL
 - ▶ Regedt32
 - ▶ Appsense
 - ▶ SecureEXE

THE END?

Just scratching the surface.

Just a quick published application protocol research.

Terminal server vulnerabilities?

EOF

The new tools and this presentation
will be available for download at:
<http://www.cqure.net/itools01.html>

ian.vitek@ixsecurity.com

+46-70-229 39 17