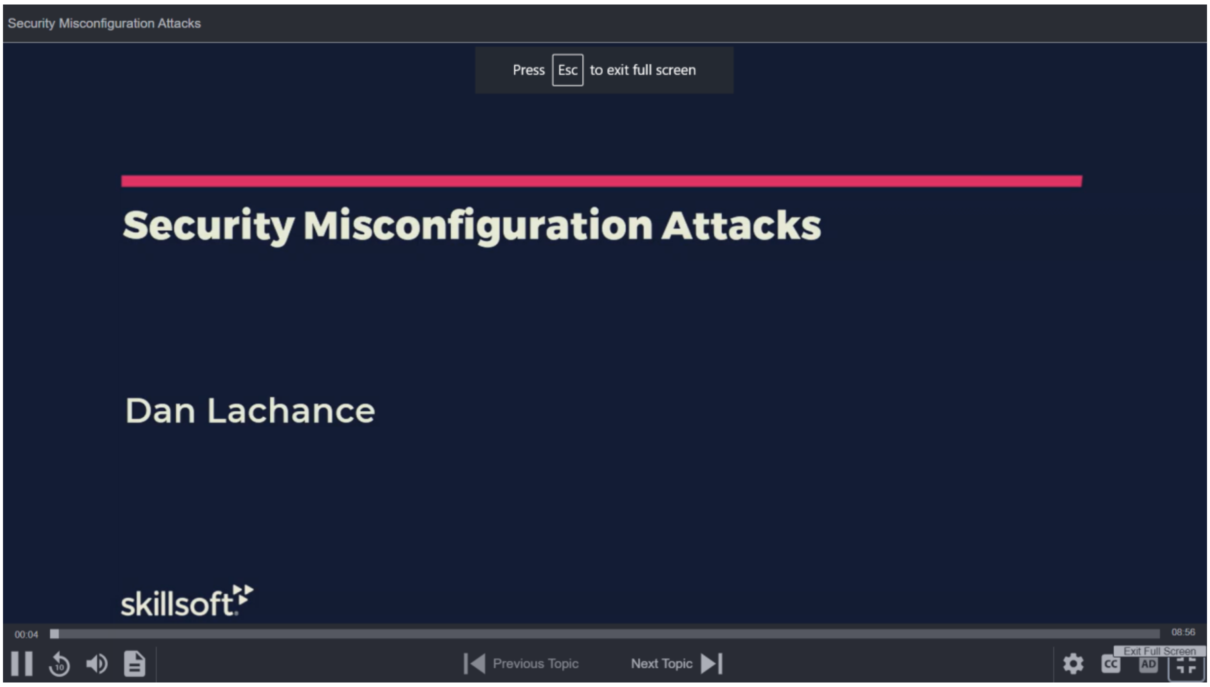


Security Misconfiguration Attacks

Press Esc to exit full screen

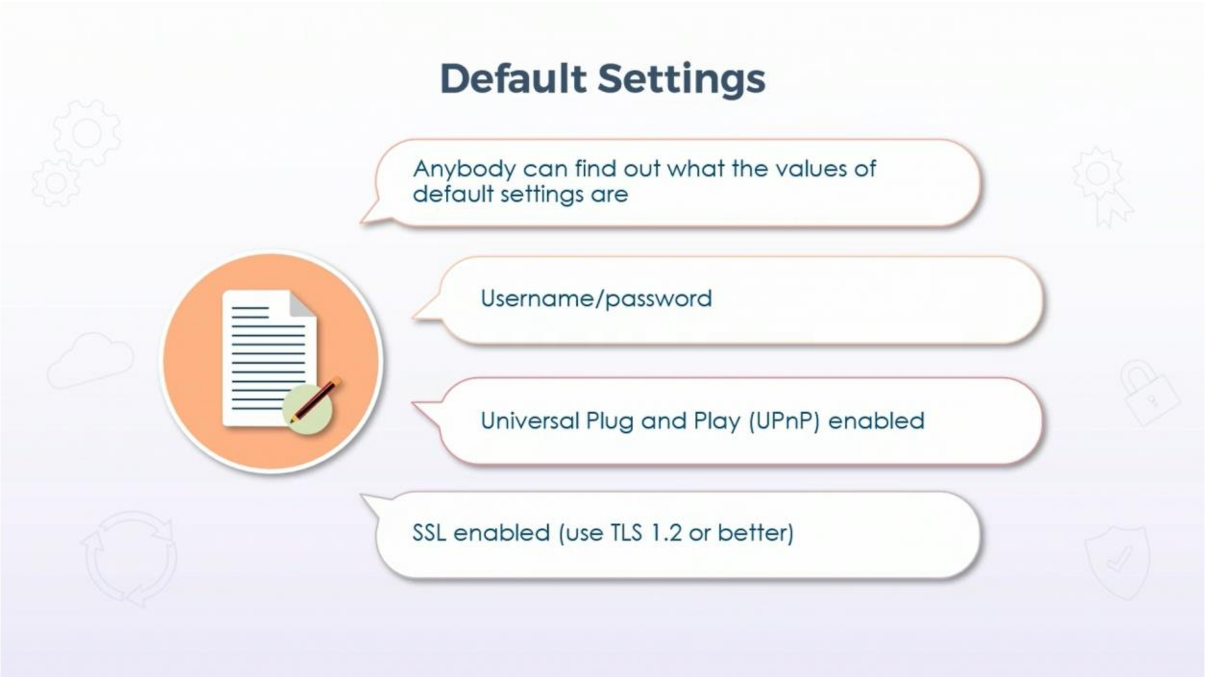
Security Misconfiguration Attacks

Dan Lachance

Security Misconfiguration Attacks

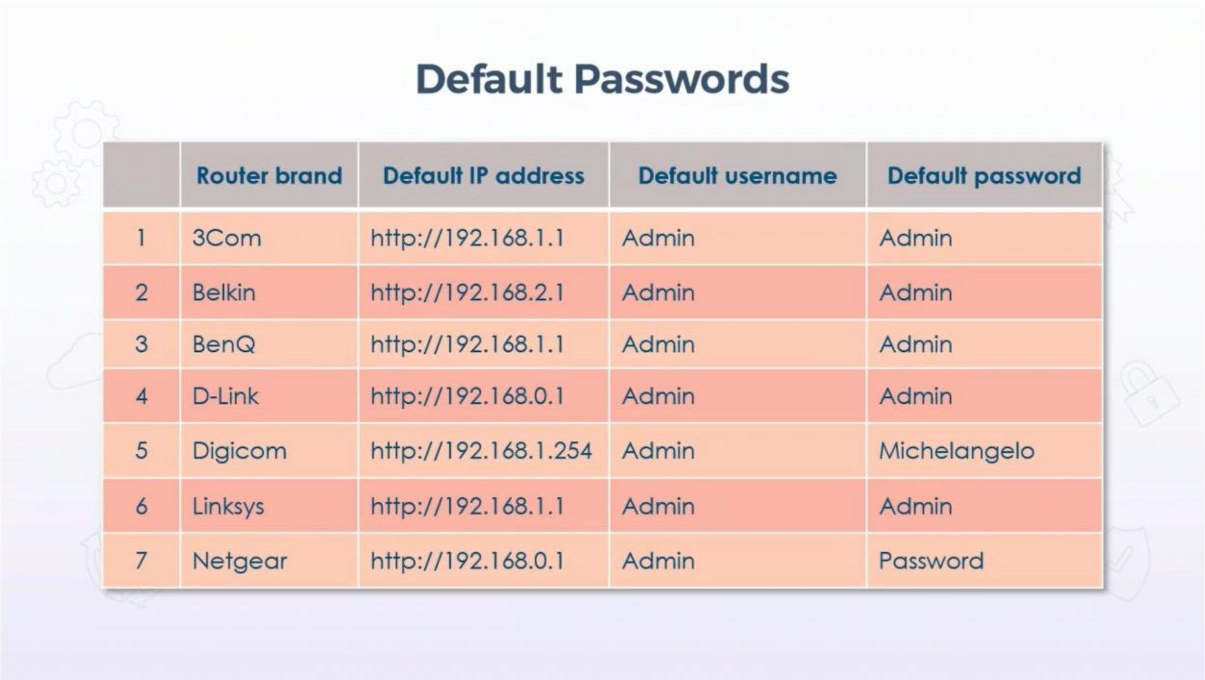
Security Misconfiguration Attacks

- IT solution design/planning
- IT solution deployment
- IT solution management



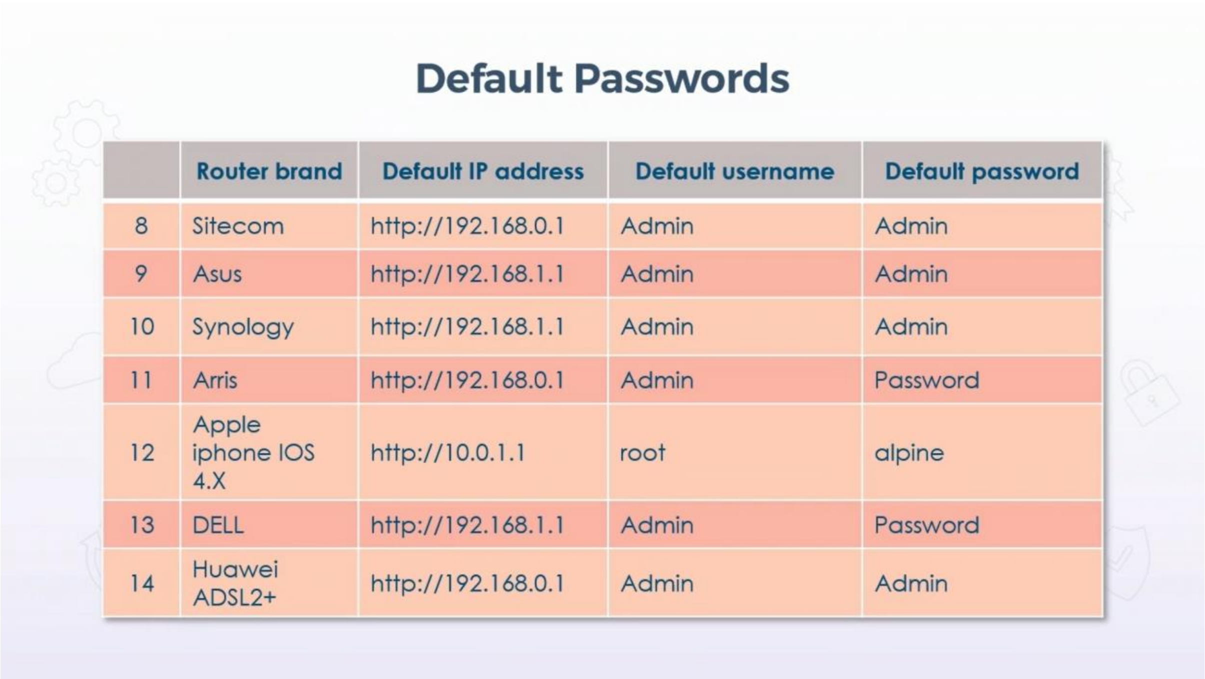
Default Settings

- Anybody can find out what the values of default settings are
- Username/password
- Universal Plug and Play (UPnP) enabled
- SSL enabled (use TLS 1.2 or better)



Default Passwords

	Router brand	Default IP address	Default username	Default password
1	3Com	http://192.168.1.1	Admin	Admin
2	Belkin	http://192.168.2.1	Admin	Admin
3	BenQ	http://192.168.1.1	Admin	Admin
4	D-Link	http://192.168.0.1	Admin	Admin
5	Digicom	http://192.168.1.254	Admin	Michelangelo
6	Linksys	http://192.168.1.1	Admin	Admin
7	Netgear	http://192.168.0.1	Admin	Password



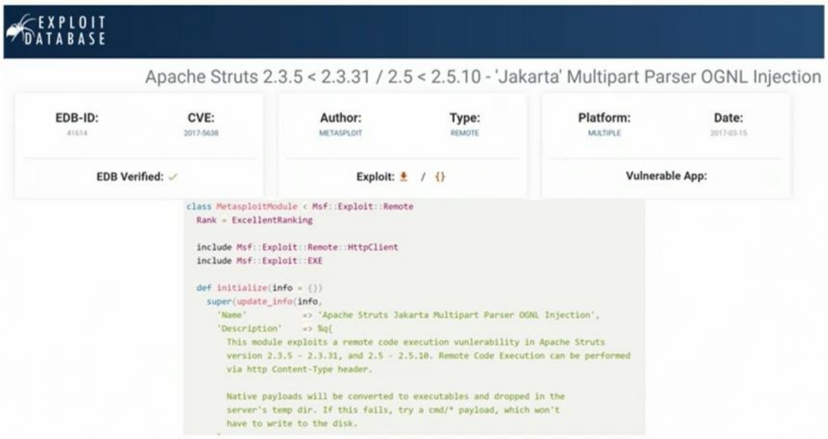
Default Passwords

	Router brand	Default IP address	Default username	Default password
8	Sitecom	http://192.168.0.1	Admin	Admin
9	Asus	http://192.168.1.1	Admin	Admin
10	Synology	http://192.168.1.1	Admin	Admin
11	Arris	http://192.168.0.1	Admin	Password
12	Apple iphone IOS 4.X	http://10.0.1.1	root	alpine
13	DELL	http://192.168.1.1	Admin	Password
14	Huawei ADSL2+	http://192.168.0.1	Admin	Admin

Missing Patches

Device and app inventory is required

Apache Struts Missing Updates - Equifax Hack 2017



EXPLOIT DATABASE

Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - 'Jakarta' Multipart Parser OGNL Injection

EDB-ID: 41614

CVE: 2017-5638

Author: METASPLOIT

Type: REMOTE

Platform: MULTIPLE

Date: 2017-03-15

EDB Verified: ✓

Exploit: ⬇ / {}

Vulnerable App:

```
class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::HttpClient
  include Msf::Exploit::EXE

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'Apache Struts Jakarta Multipart Parser OGNL Injection',
      'Description'    => %q{
        This module exploits a remote code execution vunlerability in Apache Struts
        version 2.3.5 - 2.3.31, and 2.5 - 2.5.10. Remote Code Execution can be performed
        via http Content-Type header.

        Native payloads will be converted to executables and dropped in the
        server's temp dir. If this fails, try a cmd/* payload, which won't
        have to write to the disk.
```

HTTP Strict Transport Policy (HSTS)

Server informs clients via response header that HTTPS is required

Forces HTTP to HTTPS redirect via HTTP 301:Permanent redirect

Web app requires a valid PKI certificate

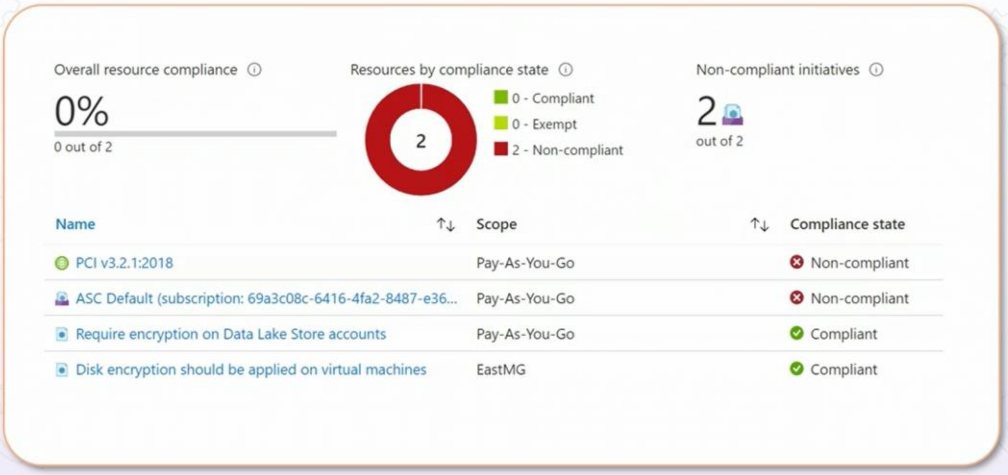
Mitigating Security Misconfigurations

Depends on planning, baselines, and inventory

Web Application Firewall (WAF)

- Designed to look for web application attacks
- Can prevent and report on potential web application security violations

Identifying Non-compliant Configurations



Overall resource compliance ⓘ

0%

0 out of 2

Resources by compliance state ⓘ

2

🟩 0 - Compliant

🟩 0 - Exempt

🟥 2 - Non-compliant

Non-compliant initiatives ⓘ

2

out of 2

Name ↑↓	Scope ↑↓	Compliance state
PCI v3.2.1:2018	Pay-As-You-Go	✖ Non-compliant
ASC Default (subscription: 69a3c08c-6416-4fa2-8487-e36...	Pay-As-You-Go	✖ Non-compliant
Require encryption on Data Lake Store accounts	Pay-As-You-Go	✓ Compliant
Disk encryption should be applied on virtual machines	EastMG	✓ Compliant

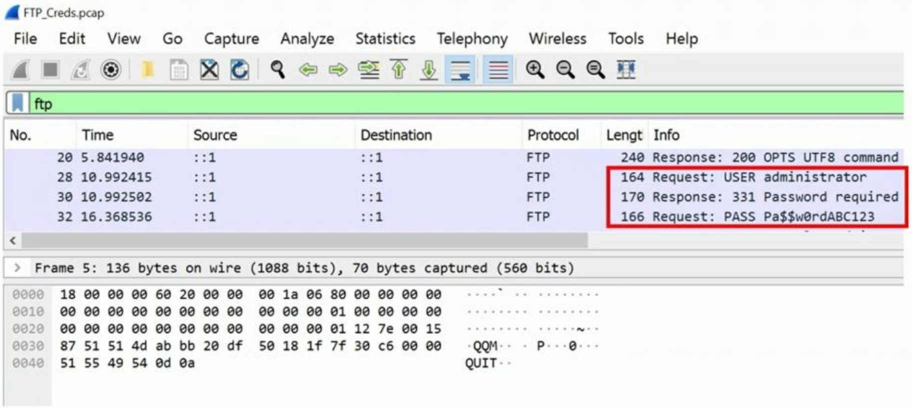
Mitigating Security Misconfigurations

Use different admin credentials among all systems

Disable unused services

Do not expose services directly to the Internet unless required

Data Transmission without Encryption



ftp

```
No.     Time        Source      Destination   Protocol  Lengt Info
     20 5.841940    ::1         ::1           FTP         240 Response: 200 OPTS UTF8 command
     28 10.992415   ::1         ::1           FTP         164 Request: USER administrator
     30 10.992502   ::1         ::1           FTP         170 Response: 331 Password required
     32 16.368536   ::1         ::1           FTP         166 Request: PASS Pa$$w0rdABC123
```

```
> Frame 5: 136 bytes on wire (1088 bits), 70 bytes captured (560 bits)
```

```
0000  18 00 00 00 60 20 00 00  00 1a 06 80 00 00 00 00   ····` ·· ········
0010  00 00 00 00 00 00 00 00  00 00 00 01 00 00 00 00   ········ ········
0020  00 00 00 00 00 00 00 00  00 00 00 01 12 7e 00 15   ········ ·····~··
0030  87 51 51 4d ab bb 20 df  50 18 1f 7f 30 c6 00 00   ·QQM·· · P···0···
0040  51 55 49 54 0d 0a                                  QUIT··
```

Periodic Automated Configuration Review