External to DA, the OS X Way

Contents

Introductions

- Alex Rymdeko-Harvey is a previous US Army Solider that recently transitioned and currently works at the Adaptive Threat Division at Veris Group as a Penetration Tester and Red Teamer. Alex has a wide range of skills and experience from offensive and defensive operations taking place in today's security surface.

- Steve Borosh is a long-time security enthusiast. Prior: U.S. Army Infantry Combat Veteran and private security contractor. Currently working as a Penetration Tester, Red Teamer and Instructor with Veris Group's Adaptive Threat Division. Steve enjoys bug hunting, building useful security tools and teaching.

Overview

- Typical penetration tests cover Windows / Linux
- Assessments become mundane
- Client approaches with a large OS X user-base
- Use common methodologies with new tools and techniques adapted for OS X
- Utilize EmPyre, a Remote Access Trojan based of of the Empire framework

Adversarial Use

- WireLurker (Trojanized applications, Infects connected ios devices)
- XcodeGhost (Infected xcode package in China)
- Hacking Team (Remote Code Systems compromise platform)
- OceanLotus (Flash Dropper, Download Mach-O binary)
- KeRanger (Ransomware, Infected transmission package)

The Scenario

- A client requests an external penetration test against their corporate infrastructure.
- Phishing with payloads may be conducted with email addresses harvested from publicly available sources.
- 90% of users utilize OS X with several developers using Windows

Scenario: Goals

- Phish OS X users
- Elevate local privileges
- Move Laterally if needed
- Gain control of the Active Directory domain

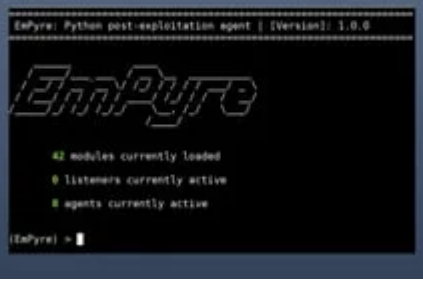
Tradecraft Preparation

- Planning and Preparation
  - Right tools for the job
  - Live off the land
    - pbpaste
    - screencapture
  - Native vs Non-Native
- Methodology
  - Reconnaissance
  - Exploitation (gain access)
  - Situational Awareness
  - Escalate Privileges
  - Establish Persistence
  - Lateral Movement

Challenges

- Limited information on operating in OS X environments
- No open-sourced asynchronous Remote Access Trojan (RAT)
- Lateral Spread
  - OS X/Linux
  - Windows
- Less phishing payloads available
  - No OLE
  - Less executable types

The Agent: EmPyre



The Agent: EmPyre

- Remote Access Trojan (RAT)
- Python (core developed by @harmj0y) based on the Empire project
- Asynchronous / C2
- Secure Diffie-Hellman exchange communications
- Post-Exploitation modules
- OS X/Linux
- Launcher detects Little Snitch

The Agent: EmPyre

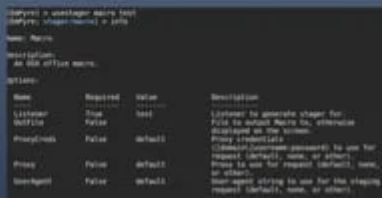
- The Diffie Hellman implementation is from Mark Loiseau's project at https://github.com/lowazo/pyDHE, licensed under version 3.0 of the GNU General Public License.
- The AES implementation is adapted from Richard Moore's project at https://github.com/ricmoo/pyaes, licensed under the MIT license.

Phishing

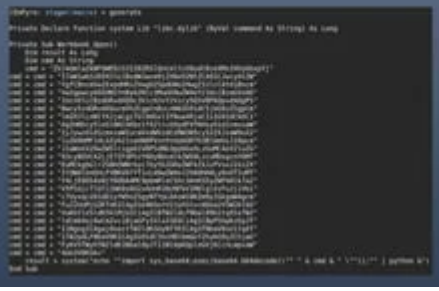
- Previous Tradecraft
  - Browser Exploits
  - Java Payloads
  - OLE Documents
  - Macro Payloads

Phishing: Payload Generation

- 2015-7007 HTML Applescript launcher
- OS X Microsoft Office Macro
  - Supports 2011
  - 2016 = "Sandbox"



Payload Generation



Situational Awareness: Host

- Previous Tradecraft
  - PowerShell
    - WMI
    - PowerUp
  - Cobalt Strike Beacon modules
  - Meterpreter modules
- The core of knowing your land
  - How do we priv-esc?

Situational Awareness: Host

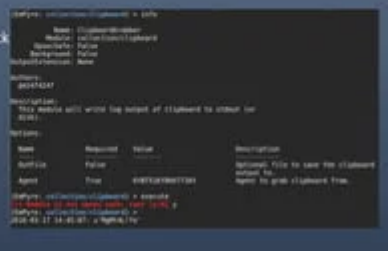
- Keylog
- Keychain Dump
- Clipboard Monitoring
- Scrape Messages
- Hash Dump
- Browser Dump

Situational Awareness: Keylogging

- Elevated Context
- Vital portion of our tradecraft
  - post exploitation

Situational Awareness: Clipboard Monitoring

- Non-Native method
  - Native pbpaste may be signatured by Carbon Black
- Out to file



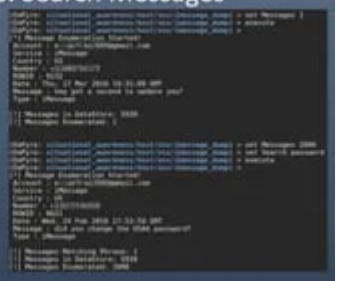
Situational Awareness: Keychain Dump

- Cleartext Keychain Dump
- Versions Prior to OS X El Capitan

Inspired / Adapted from Juuso: https://github.com/juuso/keychaindump

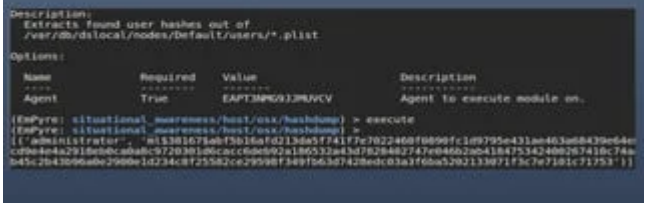
Situational Awareness: Search Messages

- Scrapes Message.app DB
  - iMessage, Jabber, Google Talk, Yahoo, AIM
- Enumerate X messages
  - Account
  - Service
  - Number
  - message



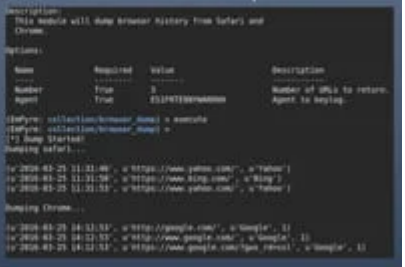
Situational Awareness: Hashdump

- Local Hashes
- Hashcat format ready!



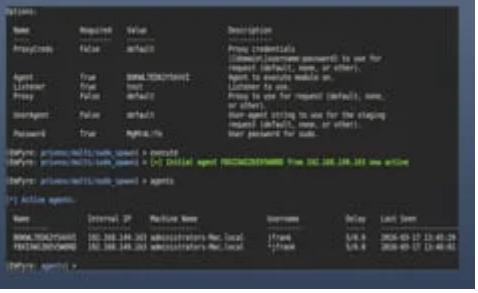
Situational Awareness: Browser Dump

- Dump Chrome
- Dump Safari
- Specify length of output



Privilege Escalation

- Sudo Spawn



Persistence

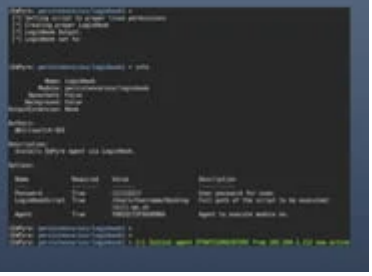
- Previous Tradecraft
  - Windows
    - Registry
    - Startup Folders
    - WMI
    - DLL Hijack
    - Net user /add
  - Linux
    - Crontab
    - adduser

Persistence

- Login Hooks
  - Login persistence
- Crontab
  - Hourly persistence
- LaunchDaemon
  - Reboot persistence
- DyLib Hijacking
  - Application start persistence

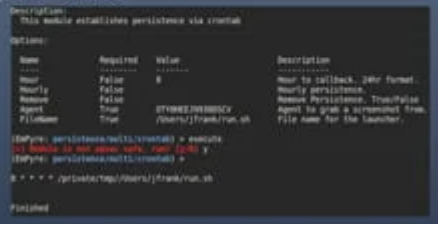
Persistence: Login Hook - User Context Persistence

- Mac Login Hooks
  - Bash / Applescript execution
  - Accessible to all users
- Uses "Defaults" tool
  - Sets com.apple.loginwindow LoginHook



Persistence: Crontab

- Set persistence by time
- Requires file on disk



Persistence: Launch Daemon

- Requires Sudo
- Spawns on reboot
- Spawns on agent loss

Persistence: Dylib Hijacking

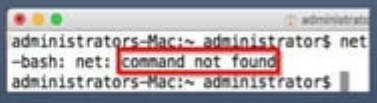
- Hijack Scanner Module
- Based on @patrickwardle research

Persistence: Dylib Hijacking

- Hijacked Xcode

Situational Awareness: Network

- Previous Tradecraft
  - Arp
  - Nmap
  - Net Commands
  - EyeWitness
  - PowerView



Situational Awareness: Network

- Group Policy Preferences
- Active Directory Queries
- Port Scanning
- Web Discovery

Situational Awareness: Active Directory Modules

- situational_awareness/network/active_directory/get_computers
- situational_awareness/network/active_directory/get_domaincontrollers
- situational_awareness/network/active_directory/get_fileservers
- situational_awareness/network/active_directory/get_groupmembers
- situational_awareness/network/active_directory/get_groupmemberships
- situational_awareness/network/active_directory/get_groups
- situational_awareness/network/active_directory/get_ous
- situational_awareness/network/active_directory/get_userinformation
- situational_awareness/network/active_directory/get_users

Situational Awareness: GPP

- Group Policy Preferences
  - Pulls "Encrypted" passwords from SYSVOL
  - MS14-025

```
(EmPyre: privesc/windows/get_gpppasswords) > execute
(EmPyre: privesc/windows/get_gpppasswords) >

Searching for Passwords...This may take some time

newName="SuperAdmin"
cpassword="1yNtWiKZ0cr9sFbwshKvvv56Mxuy6Nt2j90aX5F3K3c"
userName="Administrator (built-in)"

Unmount successful for /Volumes/sysvol/

Finished
```

https://raw.githubusercontent.com/leonteale/pentestpackage/master/Gpprefdecrypt.py

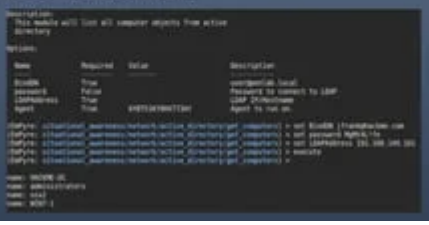
Situational Awareness: Finding the Domain Controller

```
(EmPyre: [redacted]) > shell nslookup -type=any _ldap._tcp.dc._msdcs.hackme.com
(EmPyre: [redacted]) >
Server:         192.168.149.161
Address:        192.168.149.161#53

_ldap._tcp.dc._msdcs.hackme.com service = 0 100 389 hackme-dc.hackme.com.
```

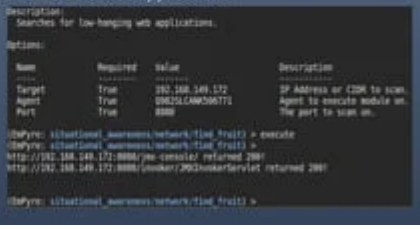
Situational Awareness: LDAP Queries

- Utilizes LDAP queries to pull objects such as computers, users, groups and more from Active Directory.



Situational Awareness: Web Services

- find_fruit module
- Checks for possible vulnerable web applications
  - Tomcat
  - jboss
  - idrac
  - Apache Axis2
  - etc..

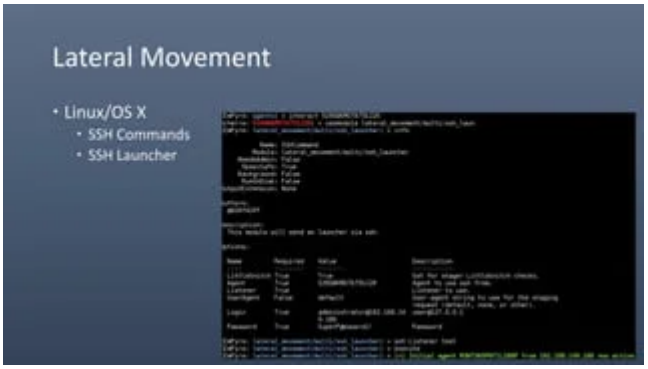


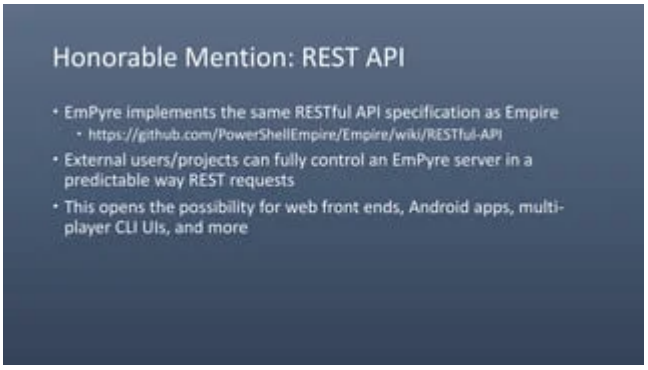
Lateral Movement

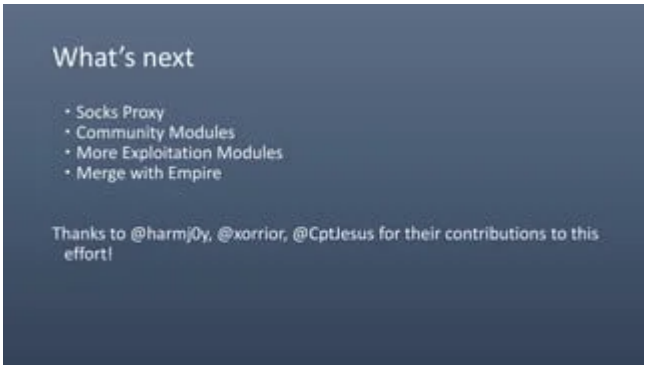
- Previous Tradecraft
  - Linux
    - SSH
    - Telnet
    - Exploitation
  - Windows
    - PSEXEC
    - WMI
    - Exploitation
    - RDP

Lateral Movement

- Windows
  - Pivot to "Empire"
  - Exploit Web Services







More Related Content

PDF

Introduction to red team operations

PPTX

Sticky Keys to the Kingdom

PDF

Addios!

PDF

Internal Pentest: from z3r0 to h3r0

PDF

Defcon 22-wesley-mc grew-instrumenting-point-of-sale-malware

PDF

Security events in 2014

PPTX

Outlook and Exchange for the bad guys

PPTX

[CB16] Invoke-Obfuscation: PowerShell obFUsk8tion Techniques & How To (Try To...

What's hot

PDF

Lateral Movement: How attackers quietly traverse your Network

PPTX

BSIDES-PR Keynote Hunting for Bad Guys

PDF

Defcon 22-zoltan-balazs-bypass-firewalls-application-whiteli

PDF

Malware collection and analysis

PDF

Anatomy of a Cloud Hack

PDF

Fruit vs Zombies: Defeat Non-jailbroken iOS Malware by Claud Xiao

PPTX

Invoke-Obfuscation DerbyCon 2016

PPTX

Pentest Apocalypse - SANSFIRE 2016 Edition

PPTX

[CB16] Facebook Malware: Tag Me If You Can by Ido Naor & Dani Goland

PDF

Web security for developers

PDF

hackcon2013-Dirty Little Secrets They Didn't Teach You In Pentesting Class v2

PDF

Defcon 22-philip-young-from-root-to-special-hacking-ibm-main

PPTX

Injection flaw teaser

PPTX

Offensive Python for Pentesting

PPT

Malware Analysis Made Simple

PPT

BSides Philly Finding a Company's BreakPoint

PDF

TeelTech - Advancing Mobile Device Forensics (online version)

PPTX

Lateral Movement - Phreaknik 2016

PDF

Attack All the Layers - What's Working in Penetration Testing

PDF

Attacker's Perspective of Active Directory

Similar to External to DA, the OS X Way

PDF

Building an EmPyre with Python

PPTX

InOffensive Security_cybersecurity2.pptx

PDF

Advanced Threats and Lateral Movement Detection

PDF

The Dirty Little Secrets They Didn’t Teach You In Pentesting Class

PPTX

Disruptionware-TRustedCISO103020v0.7.pptx

PDF

Who Should Use Powershell? You Should Use Powershell!

PDF

The Supporting Role of Antivirus Evasion while Persisting

PPTX

Bridging the Gap: Lessons in Adversarial Tradecraft

PDF

PHDays 2018 Threat Hunting Hands-On Lab

PDF

Getting Bear-y Cozy with PowerShell

PDF

Metasploit

PPTX

Red Team Apocalypse

PPTX

computer security principles and practice chapter 8

PPTX

Lannguyen-Detecting Cyber Attacks

PDF

DEF CON 27 - workshop - RICHARD GOLD - mind the gap

PPTX

Bridging the Gap

PPT

Bsides-Philly-2016-Finding-A-Companys-BreakPoint

DOCX

ARMITAGE-THE CYBER ATTACK MANAGEMENT

PPTX

DC612 Day - Hands on Penetration Testing 101

PDF

Try {stuff} Catch {hopefully not} - Evading Detection & Covering Tracks

External to DA, the OS X Way

- 1.

  External to DA, the OS X Way Operating in an OS X-heavy environment

- 2.

  Contents Introduction Overview Tradecraft Preparation Challenges The Agent Phishing Situational Awareness: Host Enumeration Privilege Escalation Persistence Situational Awareness: Network and User Enumeration Lateral Movement

- 3.

  Introductions Alex Rymdeko-Harvey is a previous US Army Solider that recently transitioned and currently works at the Adaptive Threat Division at Veris Group as a Penetration Tester and Red Teamer.

Alex has a wide range of skills and experience from offensive and defensive operations taking place in today's security surface. Steve Borosh is a long-time security enthusiast. Prior: U.S. Army Infantry Combat Veteran and private security contractor. Currently working as a Penetration Tester, Red Teamer and Instructor with Veris Group’s Adaptive Threat Division. Steve enjoys bug hunting, building useful security tools and teaching.

- 4.

  Overview • Typical penetrationtests cover Windows / Linux • Assessments become mundane • Client approaches with a large OS X user-base • Use common methodologies with new tools and techniques adapted for OS X • Utilize EmPyre, a Remote Access Trojan based of of the Empire framework

- 5.

  Adversarial Use • WireLurker(Trojanized applications, Infects connected ios devices) • XcodeGhost (Infected xcode package in China) • Hacking Team (Remote Code Systems compromise platform) • OceanLotus (Flash Dropper, Download Mach-O binary) • KeRanger (Ransomware, Infected transmission package)

- 6.

  The Scenario • Aclient requests an external penetration test against their corporate infrastructure. • Phishing with payloads may be conducted with email addresses harvested from publicly available sources. • 90% of users utilize OS X with several developers using Windows

- 7.

  Scenario: Goals • PhishOS X users • Elevate local privileges • Move Laterally if needed • Gain control of the Active Directory domain

- 8.

  Tradecraft Preparation • Planningand Preparation • Right tools for the job • Live off the land • pbpaste • screencapture • Native vs Non-Native • Methodology • Reconnaissance • Exploitation (gain access) • Sitiuational Awareness • Escalate Privileges • Establish Persistence • Lateral Movement Gain Access Situational Awareness Escalate Privileges Establish Persistence Lateral Movement

- 9.

  Challenges Limited informationon operating in OS X environments No open-sourced asynchronous Remote Access Trojan (RAT) Lateral Spread OS X/Linux Windows Less phishing payloads available No OLE Less executable types

- 10.
- 11.

The Agent: EmPyre Remote Access Trojan (RAT) Python (core developed by @harmj0y) based on the Empire project Asynchronous / C2 Secure Diffie-Hellman exchange communications Post-Exploitation modules OS X/Linux Launcher detects Little Snitch

- 12.

The Agent: EmPyre The Diffie Hellman implementation is from Mark Loiseau's project at https://github.com/lowazo/pyDHE, licensed under version 3.0 of the GNU General Public License. The AES implementation is adapted from Richard Moore's project at https://github.com/ricmoo/pyaes, licensed under the MIT license.

- 13.
- 14.

Phishing: Payload Generation 2015-7007 HTML Applescript launcher OS X Microsoft Office Macro Supports 2011 2016 = “Sandbox”

- 15.
- 16.

Situational Awareness: Host Previous Tradecraft PowerShell WMI PowerUp Cobalt Strike Beacon modules Meterpreter modules The core of knowing your land How do we priv-esc?

- 17.

Situational Awareness: Host Keylog Keychain Dump Clipboard Monitoring Scrape Messages Hash Dump Browser Dump

- 18.
- 19.
- 20.

Situational Awareness: KeychainDump Cleartext Keychain Dump Versions Prior to OS X El Capitan Inspired / Adapted from Juuso: https://github.com/juuso /keychaindump

- 21.

Situational Awareness: SearchMessages Scrapes Message.app DB iMessage, Jabber, Google Talk, Yahoo, AIM Enumerate X messages Account Service Number message

- 22.
- 23.
- 24.
- 25.
- 26.

Persistence Login Hooks Login persistence Crontab Hourly persistence LaunchDaemon Reboot persistence DyLib Hijacking Application start persistence

- 27.

Persistence: Login Hook- User Context Persistence Mac Login Hooks Bash / Applescript execution Accessible to all users Uses “Defaults” tool Sets com.apple.loginwindow LoginHook

- 28.
- 29.
- 30.
- 31.
- 32.
- 33.
- 34.

Situational Awareness: ActiveDirectory Modules
situational_awareness/network/active_directory/get_computers
situational_awareness/network/active_directory/get_domaincontrollers
situational_awareness/network/active_directory/get_fileservers
situational_awareness/network/active_directory/get_groupmembers
situational_awareness/network/active_directory/get_groupmemberships
situational_awareness/network/active_directory/get_groups
situational_awareness/network/active_directory/get_ous
situational_awareness/network/active_directory/get_userinformation
situational_awareness/network/active_directory/get_users

- 35.

Situational Awareness: GPP Group Policy Preferences Pulls “Encrypted” passwords from SYSVOL MS14-025 https://raw.githubusercontent.com/leonteale/pentestpackage/master/Gpprefdecrypt.py

- 36.
- 37.

Situational Awareness: LDAPQueries Utilizes LDAP queries to pull objects such as computers, users, groups and more from Active Directory.

- 38.

Situational Awareness: WebServices find_fruit module Checks for possible vulnerable web applications Tomcat jboss idrac Apache Axis2 etc..

- 39.

Lateral Movement PreviousTradecraft Linux SSH Telnet Exploitation Windows PSEXEC WMI Exploitation RDP

- 40.
- 41.
- 43.

  Honorable Mention: RESTAPI EmPyre implements the same RESTful API specification as Empire https://github.com/PowerShellEmpire/Empire/wiki/RESTful-API External users/projects can fully control an EmPyre server in a predictable way REST requests This opens the possibility for web front ends, Android apps, multi- player CLI UIs, and more

- 44.

  What's next SocksProxy Community Modules More Exploitation Modules Merge with Empire Thanks to @harmj0y, @xorrior, @CptJesus for their contributions to this effort!

Editor's Notes

- #3 Steve starts talking
- #4 Introduce ourselves
- #5 As a Penetration Tester or Red Teamer, the path to Domain Administrator in many environments may seem all too easy or "cookie cutter" these days. But what happens when you engage a high-security client with an OS X-heavy environment? Do you turn down the engagement or accept the challenge and up your game? This talk explores such a scenario and how testers can utilize various tools, techniques, and lessons-learned to successfully perform a complete assessment in an OS X domain-joined environment. We will cover a custom-built OS X/Linux agent and its associated tradecraft, from gaining initial access, to post-exploitation, lateral spread, persistence, and domain compromise.
- #9 Keep in mind, methodologies stay the same for OS X, tradecraft may change. Explain such as "How do we gain access in OS X"? SSH/Phishing.
- #10 Different operating systems present their own lateral spread challenges. (linux: no smb, wmi, powershell) (Windows: no ssh, OS X doesnt have net commands)
- #11 Alex Start Familiar interface for Empire users.
- #15 Currently ,we have two payloads for phishing.
- #17 Talk about tradecraft as a whole, This is post exploitation enumeration
- #18 Keychain Dump - No el Capitan YET
- #19 Currently saves to target in an unencrypted format.
- #22 Talk about how messages are stored unencrypted in a database
- #24 Currently, only dumps history. Useful for hunting internal web services.
- #29 Steve Starts
- #35 Utilizes "ldapsearch" for AD enumeration
- #37 In order to perform LDAP queries we'll need to start off by finding the domain controller that we are going to bind our LDAP queries to. One quick solution is a single nslookup query.
- #40 During most penetration tests, you may find yourself moving from host to host using common techniques such as PSEXEC, WMI or RDP. Operating in an OS X environment presents challenges as these methods may not be available.
