

External to DA, the OS X Way

Archived: 2026-04-05 16:28:55 UTC

More Related Content

Introduction to red team operations

Sticky Keys to the Kingdom

Internal Pentest: from z3r0 to h3r0

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

Outlook and Exchange for the bad guys

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

What's hot

Lateral Movement: How attackers quietly traverse your Network

BSIDES-PR Keynote Hunting for Bad Guys

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

Malware collection and analysis

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

Invoke-Obfuscation DerbyCon 2016

Pentest Apocalypse - SANSFIRE 2016 Edition

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

Web security for developers

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

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

Offensive Python for Pentesting

Malware Analysis Made Simple

BSides Philly Finding a Company's BreakPoint

TeelTech - Advancing Mobile Device Forensics (online version)

Lateral Movement - Phreaknik 2016

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

Attacker's Perspective of Active Directory

Similar to External to DA, the OS X Way

Building an EmPyre with Python

InOffensive Security_cybersecurity2.pptx

Advanced Threats and Lateral Movement Detection

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

Disruptionware-TRustedCISO103020v0.7.pptx

Who Should Use Powershell? You Should Use Powershell!

The Supporting Role of Antivirus Evasion while Persisting

Bridging the Gap: Lessons in Adversarial Tradecraft

PHDays 2018 Threat Hunting Hands-On Lab

Getting Bear-y Cozy with PowerShell

computer security principles and practice chapter 8

Lannguyen-Detecting Cyber Attacks

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

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

ARMITAGE-THE CYBER ATTACK MANAGEMENT

DC612 Day - Hands on Penetration Testing 101

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 Soldier 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 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

- 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](#) • 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

- 7.

[Scenario: Goals](#) • [Phish](#) OS X users • Elevate local privileges • Move Laterally if needed • Gain control of the Active Directory domain

- 8.

[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 Gain Access Situational Awareness Escalate Privileges Establish Persistence Lateral Movement

- 9.

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

- 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: Keychain Dump Cleartext Keychain Dump Versions Prior to OS X El Capitan Inspired / Adapted from Juuso: <https://github.com/juuso/keychaindump>

- 21.

Situational Awareness: Search Messages 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](#) [Previous](#) Tradecraft 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](#) [Socks](#) Proxy 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. 

Source: <https://www.slideshare.net/slideshow/external-to-da-the-os-x-way/62021418>