yeyintminthuhtut / Awesome-Red-Teaming

List of Awesome Red Teaming Resources

cobalt-strike phishing redteaming redteam empire uac

62 commits 1 branch 0 releases 3 contributors MIT

Branch: master New pull request Find file Clone or download

yeyintminthuhtut Merge pull request #4 from santosomar/patch-1 ... Latest commit e599e5f 9 hours ago

LICENSE	Initial commit	8 months ago

README.md

Awesome Red Teaming

List of Awesome Red Team / Red Teaming Resources

This list is for anyone wishing to learn about Red Teaming but do not have a starting point.

Anyway, this is a living resources and will update regularly with latest Adversarial Tactics and Techniques based on Mitre ATT&CK

You can help by sending Pull Requests to add more information.

Table of Contents

- Collection
- Exfiltration
- Command and Control
- Embedded and Peripheral Devices Hacking
- Misc
- Ebooks
- Training
- Certification

↑ Initial Access

- How To: Empire's Cross Platform Office Macro
- Phishing with PowerPoint
- PHISHING WITH EMPIRE
- Bash Bunny
- OWASP Presentation of Social Engineering - OWASP
- USB Drop Attacks: The Danger of "Lost And Found" Thumb Drives
- Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter - Defcon 23
- Cobalt Strike - Spear Phishing documentation
- Cobalt Strike Blog - What's the go-to phishing technique or exploit?
- Spear phishing with Cobalt Strike - Raphael Mudge
- EMAIL RECONNAISSANCE AND PHISHING TEMPLATE GENERATION MADE SIMPLE
- Phishing for access
- Excel macros with PowerShell

- PowerPoint and Custom Actions
- Macro-less Code Exec in MSWord
- Multi-Platform Macro Phishing Payloads
- Abusing Microsoft Word Features for Phishing: “subDoc”
- Phishing Against Protected View
- POWERSHELL EMPIRE STAGERS 1: PHISHING WITH AN OFFICE MACRO AND EVADING AVS
- The PlugBot: Hardware Botnet Research Project
- Luckystrike: An Evil Office Document Generator
- The Absurdly Underestimated Dangers of CSV Injection
- Macroless DOC malware that avoids detection with Yara rule
- Phishing between the app whitelists
- Executing Metasploit & Empire Payloads from MS Office Document Properties (part 1 of 2)
- Executing Metasploit & Empire Payloads from MS Office Document Properties (part 2 of 2)
- Social Engineer Portal
- 7 Best social Engineering attack
- Using Social Engineering Tactics For Big Data Espionage - RSA Conference Europe 2012
- USING THE DDE ATTACK WITH POWERSHELL EMPIRE
- Phishing on Twitter - POT
- Microsoft Office – NTLM Hashes via Frameset
- Defense-In-Depth write-up
- Spear Phishing 101

↑ Execution

- Research on CMSTP.exe,
- Windows oneliners to download remote payload and execute arbitrary code
- Executing Commands and Bypassing AppLocker with PowerShell Diagnostic Scripts
- WSH Injection: A Case Study

↑ Persistence

- A View of Persistence
- hiding registry keys with psreflect
- Persistence using RunOnceEx – Hidden from Autoruns.exe
- Persistence using GlobalFlags in Image File Execution Options – Hidden from Autoruns.exe
- Putting data in Alternate data streams and how to execute it – part 2
- WMI Persistence with Cobalt Strike
- Leveraging INF-SCT Fetch & Execute Techniques For Bypass, Evasion, & Persistence
- Leveraging INF-SCT Fetch & Execute Techniques For Bypass, Evasion, & Persistence (Part 2)
- Vshadow: Abusing the Volume Shadow Service for Evasion, Persistence, and Active Directory Database Extraction

↑ Privilege Escalation

User Account Control Bypass

- First entry: Welcome and fileless UAC bypass,
- Exploiting Environment Variables in Scheduled Tasks for UAC Bypass,
- Reading Your Way Around UAC in 3 parts: Part 1. Part 2. Part 3.
- Bypassing UAC using App Paths,

- "Fileless" UAC Bypass using sdclt.exe,
- UAC Bypass or story about three escalations,
- "Fileless" UAC Bypass Using eventvwr.exe and Registry Hijacking,
- Bypassing UAC on Windows 10 using Disk Cleanup,
- Using IARPUninstallStringLauncher COM interface to bypass UAC,
- Fileless UAC Bypass using sdclt
- Eventvwr File-less UAC Bypass CNA
- Windows 7 UAC whitelist

Escalation

- Windows Privilege Escalation Checklist
- From Patch Tuesday to DA
- A Path for Privilege Escalation

↑ Defense Evasion

- Window 10 Device Guard Bypass
- App Locker ByPass List
- Window Signed Binary
- Bypass Application Whitelisting Script Protections - Regsvr32.exe & COM Scriptlets (.sct files)
- Bypassing Application Whitelisting using MSBuild.exe - Device Guard Example and Mitigations
- Empire without powershell
- Powershell without Powershell to bypass app whitelist
- MS Signed mimikatz in just 3 steps

- Hiding your process from sysinternals
- code signing certificate cloning attacks and defenses
- userland api monitoring and code injection detection
- In memory evasion
- Bypassing AMSI via COM Server Hijacking
- process doppelganging
- Week of Evading Microsoft ATA - Announcement and Day 1 to Day 5
- VEIL-EVASION AES ENCRYPTED HTTPKEY REQUEST: SAND-BOX EVASION
- Putting data in Alternate data streams and how to execute it
- AppLocker – Case study – How insecure is it really? – Part 1
- AppLocker – Case study – How insecure is it really? – Part 2
- Harden Windows with AppLocker – based on Case study part 2
- Harden Windows with AppLocker – based on Case study part 2
- Office 365 Safe links bypass
- Windows Defender Attack Surface Reduction Rules bypass
- Bypassing Device guard UMCI using CHM – CVE-2017-8625
- Bypassing Application Whitelisting with BGInfo
- Cloning and Hosting Evil Captive Portals using a Wifi PineApple
- https://bohops.com/2018/01/23/loading-alternate-data-stream-ads-dll-cpl-binaries-to-bypass-applocker/
- Executing Commands and Bypassing AppLocker with PowerShell Diagnostic Scripts

↑ Credential Access

- Windows Access Tokens and Alternate credentials

- Bringing the hashes home with reGeorg & Empire
- Intercepting passwords with Empire and winning
- Local Administrator Password Solution (LAPS) Part 1
- Local Administrator Password Solution (LAPS) Part 2
- USING A SCF FILE TO GATHER HASHES
- Remote Hash Extraction On Demand Via Host Security Descriptor Modification
- Offensive Encrypted Data Storage
- Practical guide to NTLM Relaying
- Dump Clear-Text Passwords for All Admins in the Domain Using Mimikatz DCSync

↑ Discovery

- Red Team Operating in a Modern Environment
- My First Go with BloodHound
- Introducing BloodHound
- A Red Teamer's Guide to GPOs and OUs
- Automated Derivative Administrator Search
- A Pentester's Guide to Group Scoping
- Local Group Enumeration
- The PowerView PowerUsage Series #1 - Mass User Profile Enumeration
- The PowerView PowerUsage Series #2 – Mapping Computer Shortnames With the Global Catalog
- The PowerView PowerUsage Series #3 – Enumerating GPO edit rights in a foreign domain
- The PowerView PowerUsage Series #4 – Finding cross-trust ACEs
- Aggressor PowerView

- Lay of the Land with BloodHound
- Scanning for Active Directory Privileges & Privileged Accounts
- Microsoft LAPS Security & Active Directory LAPS Configuration Recon
- Trust Direction: An Enabler for Active Directory Enumeration and Trust Exploitation

↑ Lateral Movement

- A Citrx Story
- Jumping Network Segregation with RDP
- Pass hash pass ticket no pain
- Abusing DNSAdmins privilege for escalation in Active Directory
- Using SQL Server for attacking a Forest Trust
- Extending BloodHound for Red Teamers
- OPSEC Considerations for beacon commands
- My First Go with BloodHound
- Kerberos Party Tricks: Weaponizing Kerberos Protocol Flaws
- Lateral movement using excel application and dcom
- Lay of the Land with BloodHound
- The Most Dangerous User Right You (Probably) Have Never Heard Of
- Agentless Post Exploitation
- A Guide to Attacking Domain Trusts
- Pass-the-Hash Is Dead: Long Live LocalAccountTokenFilterPolicy
- Targeted Kerberoasting
- Kerberoasting Without Mimikatz

- Abusing GPO Permissions
- Abusing Active Directory Permissions with PowerView
- Roasting AS-REPs
- Getting the goods with CrackMapExec: Part 1
- Getting the goods with CrackMapExec: Part 2
- DiskShadow: The Return of VSS Evasion, Persistence, and Active Directory Database Extraction
- Abusing Exported Functions and Exposed DCOM Interfaces for Pass-Thru Command Execution and Lateral Movement
- a guide to attacking domain trusts
- Outlook Home Page – Another Ruler Vector
- Outlook Forms and Shells

↑ Collection

- Accessing clipboard from the lock screen in Windows 10 Part 1
- Accessing clipboard from the lock screen in Windows 10 Part 2

↑ Exfiltration

- DNS Data exfiltration—What is this and How to use?
- DNS Tunnelling
- sg1: swiss army knife for data encryption, exfiltration & covert communication
- Data Exfiltration over DNS Request Covert Channel: DNSExfiltrator
- DET (extensible) Data Exfiltration Toolkit

↑ Command and Control

Domain Fronting

- Empre Domain Fronting
- Escape and Evasion Egressing Restricted Networks - Tom Steele and Chris Patten
- Finding Frontable Domain
- TOR Fronting – Utilising Hidden Services for Privacy
- Simple domain fronting PoC with GAE C2 server
- Domain Fronting Via Cloudfront Alternate Domains
- Finding Domain frontable Azure domains - thoth / Fionnbharr (@a_profligate)
- Google Groups: Blog post on finding 2000+ Azure domains using Censys
- Red Team Insights on HTTPS Domain Fronting Google Hosts Using Cobalt Strike
- SSL Domain Fronting 101
- How I Identified 93k Domain-Frontable CloudFront Domains
- Validated CloudFront SSL Domains
- CloudFront Hijacking
- CloudFrunt GitHub Repo

Connection Proxy

- Redirecting Cobalt Strike DNS Beacons
- Apache2Mod Rewrite Setup
- Cobalt Strike HTTP C2 Redirectors with Apache mod_rewrite
- High-reputation Redirectors and Domain Fronting
- Cloud-based Redirectors for Distributed Hacking

- Combatting Incident Responders with Apache mod_rewrite
- Operating System Based Redirection with Apache mod_rewrite
- Invalid URI Redirection with Apache mod_rewrite
- Strengthen Your Phishing with Apache mod_rewrite and Mobile User Redirection
- mod_rewrite rule to evade vendor sandboxes
- Expire Phishing Links with Apache RewriteMap
- Serving random payloads with NGINX
- Mod_Rewrite Automatic Setup
- Hybrid Cobalt Strike Redirectors
- Expand Your Horizon Red Team – Modern SAAS C2
- RTOps: Automating Redirector Deployment With Ansible

Web Services

- C2 with Dropbox
- C2 with gmail
- C2 with twitter
- Office 365 for Cobalt Strike C2
- Red Team Insights on HTTPS Domain Fronting Google Hosts Using Cobalt Strike
- A stealthy Python based Windows backdoor that uses Github as a C&C server
- External C2 (Third-Party Command and Control)
- Cobalt Strike over external C2 – beacon home in the most obscure ways
- External C2 for Cobalt Strike
- External C2 framework for Cobalt Strike
- External C2 framework - GitHub Repo

- Hiding in the Cloud: Cobalt Strike Beacon C2 using Amazon APIs
- Exploring Cobalt Strike's ExternalC2 framework

Application Layer Protocol

- C2 WebSocket
- C2 WMI
- C2 Website
- C2 Image
- C2 Javascript
- C2 WebInterface
- C2 with DNS
- C2 with https
- C2 with webdav
- Introducing Merlin—A cross-platform post-exploitation HTTP/2 Command & Control Tool
- InternetExplorer.Application for C2

Infrastructure

- Automated Red Team Infrastructure Deployment with Terraform - Part 1
- Automated Red Team Infrastructure Deployment with Terraform - Part 2
- Red Team Infrastructure - AWS Encrypted EBS
- 6 RED TEAM INFRASTRUCTURE TIPS
- How to Build a C2 Infrastructure with Digital Ocean – Part 1
- Infrastructure for Ongoing Red Team Operations
- Attack Infrastructure Log Aggregation and Monitoring

- Randomized Malleable C2 Profiles Made Easy
- Migrating Your infrastructure
- ICMP C2
- Using WebDAV features as a covert channel
- Safe Red Team Infrastructure
- EGRESSING BLUECOAT WITH COBALTSTIKE & LET'S ENCRYPT
- Command and Control Using Active Directory
- A Vision for Distributed Red Team Operations
- Designing Effective Covert Red Team Attack Infrastructure
- Serving Random Payloads with Apache mod_rewrite
- Mail Servers Made Easy
- Securing your Empire C2 with Apache mod_rewrite
- Automating Gophish Releases With Ansible and Docker
- How to Write Malleable C2 Profiles for Cobalt Strike
- How to Make Communication Profiles for Empire
- A Brave New World: Malleable C2
- Malleable Command and Control

↑ Embedded and Peripheral Devices Hacking

- Gettting in with the Proxmark3 & ProxBrute
- Practical Guide to RFID Badge copying
- Contents of a Physical Pentester Backpack
- MagSpoof - credit card/magstripe spoofer

- Wireless Keyboard Sniffer
- RFID Hacking with The Proxmark 3
- Swiss Army Knife for RFID
- Exploring NFC Attack Surface
- Outsmarting smartcards
- Reverse engineering HID iClass Master keys
- Android Open Pwn Project (AOPP)

↑ Misc

- Red Tips of Vysec
- Cobalt Strike Tips for 2016 ccde red teams
- Models for Red Team Operations
- Planning a Red Team exercise
- Raphael Mudge - Dirty Red Team tricks
- introducing the adversary resilience methodology part 1
- introducing the adversary resilience methodology part 2
- Responsible red team
- Red Teaming for Pacific Rim CCDC 2017
- How I Prepared to Red Team at PRCCDC 2015
- Red Teaming for Pacific Rim CCDC 2016
- Responsible Red Teams

↑ Ebooks

- Next Generation Red Teaming
- Targeted Cyber Attack
- Advanced Penetration Testing: Hacking the World's Most Secure Networks
- Social Engineers' Playbook Pretical Pretexting

↑ Training (Free)

- Tradecraft - a course on red team operations
- Advanced Threat Tactics Course & Notes

↑ Certification

- CREST Certified Simulated Attack Specialist
- CREST Certified Simulated Attack Manager
- SEC564: Red Team Operations and Threat Emulation
- ELearn Security Penetration Testing eXtreme