Privilege Escalation & Post-Exploitation

Table of Contents

- DLL Stuff
- OS X Privilege Escalation
- General Post Exploitation
- Linux Post Exploitation
- OS X Post Exploitation
- Windows Post Exploitation
- ActiveDirectory
- Kerberos
- Office Macros
- Email/Exchange
- Grabbing Goodies
- Gaining Awareness
- Persistence Techniques
- Linux Persistence Techniques
- OS X Persistence
- Pivoting & Lateral movement
- Avoiding/Bypassing Anti-Virus/Whitelisting/Sandboxes/etc
- Containers & Docker
- Payloads
- Code Injection
- Papers

Sort

- Add code injection stuff to post-exploitation Windows
    - Add linux/windows/os x to code injection section
- Add linux post exploitation/persistence stuff
- Add stuff to powershell without powershell section
- Battle Of SKM And IUM How Windows 10 Rewrites OS Architecture - Alex Ionescu - BHUSA2015
    - Slides
- Brutal
    - Brutal is a toolkit to quickly create various payload,powershell attack , virus attack and launch listener for a Human Interface Device
- Oneliner-izer
    - Convert any Python file into a single line of code which has the same functionality.
- Malicious Installer Plugins - specterops
- Using Parameters with InstallUtil
- Leveraging INF-SCT Fetch & Execute Techniques For Bypass, Evasion, & Persistence (Part 1)
- Leveraging INF-SCT Fetch & Execute Techniques For Bypass, Evasion, & Persistence (Part 2)
- DAMP
    - The Discretionary ACL Modification Project: Persistence Through Host-based Security Descriptor Modification. This project contains several files that implement host-based security descriptor "backdoors" that facilitate the abuse of

various remotely accessible services for arbitrary trustees/security principals. tl;dr - this grants users/groups (local, domain, or 'well-known' like 'Everyone') of an attacker's choosing the ability to perform specific administrative actions on a modified host without needing membership in the local administrators group.

end Sort

Hardware-based Privilege Escalation

- **Writeups**
  - Windows DMA Attacks : Gaining SYSTEM shells using a generic patch
  - Where there's a JTAG, there's a way: Obtaining full system access via USB
  - Snagging creds from locked machines - mubix
  - Bash Bunny QuickCreds – Grab Creds from Locked Machines
  - PoisonTap
    - Exploits locked/password protected computers over USB, drops persistent WebSocket-based backdoor, exposes internal router, and siphons cookies using Raspberry Pi Zero & Node.js.
  - **Rowhammer**
    - Exploiting the DRAM rowhammer bug to gain kernel privileges
    - Row hammer - Wikipedia
    - Another Flip in the Wall of Rowhammer Defenses
    - rowhammer.js
      - Rowhammer.js - A Remote Software-Induced Fault Attack in JavaScript
    - Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript
    - Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors

        - Abstract. Memory isolation is a key property of a reliable and secure computing system — an access to one memory ad- dress should not have unintended side e ects on data stored in other addresses. However, as DRAM process technology scales down to smaller dimensions, it becomes more diffcult to prevent DRAM cells from electrically interacting with each other. In this paper, we expose the vulnerability of commodity DRAM chips to disturbance errors. By reading from the same address in DRAM, we show that it is possible to corrupt data in nearby addresses. More specifically, activating the same row in DRAM corrupts data in nearby rows. We demonstrate this phenomenon on Intel and AMD systems using a malicious program that generates many DRAM accesses. We induce errors in most DRAM modules (110 out of 129) from three major DRAM manufacturers. From this we conclude that many deployed systems are likely to be at risk. We identify the root cause of disturbance errors as the repeated toggling of a DRAM row's wordline, which stresses inter-cell coupling e ects that accelerate charge leakage from nearby rows. We provide an extensive characterization study of disturbance errors and their behavior using an FPGA-based testing plat- form. Among our key findings, we show that (i) it takes as few as 139K accesses to induce an error and (ii) up to one in every 1.7K cells is susceptible to errors. After examining var- ious potential ways of addressing the problem, we propose a low-overhead solution to prevent the errors.

- **Tools**
    - Inception
        - Inception is a physical memory manipulation and hacking tool exploiting PCI-based DMA. The tool can attack over FireWire, Thunderbolt, ExpressCard, PC Card and any other PCI/PCIe HW interfaces.
    - PCILeech
        - PCILeech uses PCIe hardware devices to read and write from the target system memory. This is achieved by using DMA over PCIe. No drivers are needed on the target system.
    - physmem
        - physmem is a physical memory inspection tool and local privilege escalation targeting macOS up through 10.12.1. It exploits either CVE-2016-1825 or CVE-2016-7617 depending on the deployment target. These two vulnerabilities are nearly identical, and exploitation can be done exactly the same. They were patched in OS X El Capitan 10.11.5 and macOS Sierra 10.12.2, respectively.

    - rowhammer-test
        - Program for testing for the DRAM "rowhammer" problem
    - Tools for "Another Flip in the Wall"

Linux Privilege Escalation

- **101**
    - Windows / Linux Local Privilege Escalation Workshop
- **Blogposts/Writeups**
    - Dangerous Sudoers Entries – Series, 5 parts
    - No one expect command execution!
    - Attack and Defend: Linux Privilege Escalation Techniques of 2016
    - Back To The Future: Unix Wildcards Gone Wild - Leon Juranic
    - Using the docker command to root the host (totally not a security issue)
        - It is possible to do a few more things more with docker besides working with containers, such as creating a root shell on the host, overwriting system configuration files, reading restricted stuff, etc.
- **Talks/Videos**
    - Chw00t: Breaking Unixes' Chroot Solutions
- **Tools**
    - Linux_Exploit_Suggester
        - Linux Exploit Suggester; based on operating system release number. This program run without arguments will perform a 'uname -r' to grab the Linux Operating Systems release version, and return a suggestive list of possible exploits. Nothing fancy, so a patched/back-ported patch may fool this script. Additionally possible to provide '-k' flag to manually enter the Kernel Version/Operating System Release Version.
    - Basic Linux Privilege Escalation - g0tmi1k

        - Not so much a script as a resource, g0tmi1k's blog post here has led to so many privilege escalations on Linux system's it's not funny. Would definitely recommend trying out everything on this post for enumerating systems.
    - LinEnum
        - This tool is great at running through a heap of things you should check on a Linux system in the post exploit process. This include file permissions, cron jobs if visible, weak credentials etc. The first thing I run on a newly compromised system.
    - LinuxPrivChecker
        - This is a great tool for once again checking a lot of standard things like file permissions etc. The real gem of this script is the recommended privilege escalation exploits given at the conclusion of the script. This is a great starting point for escalation.
    - Unix Privilege Escalation Checker
        - Unix-privesc-checker is a script that runs on Unix systems (tested on Solaris 9, HPUX 11, Various Linuxes, FreeBSD 6.2). It tries to find misconfigurations that could allow local unprivileged users to escalate privileges to other users or to access local apps (e.g. databases). It is written as a single shell script so it can be easily uploaded and run (as opposed to un-tarred, compiled and installed). It can run either as a normal user or as root (obviously it does a better job when running as root because it can read more files).
    - EvilAbigail
        - Initrd encrypted root fs attack
    - Triple-Fetch-Kernel-Creds
        - Attempt to steal kernelcredentials from launchd + task_t pointer (Based on: CVE-2017-7047)
    - LinEnum
    - linux-exploit-suggester
        - Linux privilege escalation auditing tool
    - linuxprivchecker.py --- A Linux Privilege Escalation Checker for Python 2.7 and 3.x
        - This script is intended to be executed locally on a Linux machine, with a Python version of 2.7 or 3.x, to enumerate basic system info and search for common privilege escalation vectors. Currently at version 2. - Fork

of the ever popular scrip that added support for Python3

- systemd (systemd-tmpfiles) < 236 - 'fs.protected_hardlinks=0' Local Privilege Escalation

---

Windows Privilege Escalation

- **Blogposts/Writeups**
  - **101**
    - Windows Privilege Escalation Fundamentals
    - Windows Privilege Escalation Methods for Pentesters
    - Common Windows Privilege Escalation Vectors
    - Windows Privilege Escalation Cheat Sheet/Tricks
    - Windows / Linux Local Privilege Escalation Workshop
  - **Specific Techniques**
    - **Group Policy Preferences**
      - Exploiting Windows 2008 Group Policy Preferences
    - **Intel SYSRET**
      - Windows Kernel Intel x64 SYSRET Vulnerability + Code Signing Bypass Bonus
      - Windows Kernel Intel x64 SYSRET Vulnerability Exploit + Kernel Code Signing Bypass Bonus
    - **Logic**
      - Introduction to Logical Privilege Escalation on Windows - James Forshaw
      - Windows Logical EoP Workbook
      - Abusing Token Privileges For EoP
        - This repository contains all code and a Phrack-style paper on research into abusing token privileges for escalation of privilege. Please feel free to ping us with questions, ideas, insults, or bugs.
    - PentestLab Windows PrivEsc Writeup List

        - Hot Potato
        - Always Install Elevated
        - Unquoted Service Path
        - Token Manipulation
        - Secondary Logon Handle
        - Insecure Registry Permissions
        - Intel SYSRET
        - Weak Service Permissions
- **NTLM-related**
    - Windows: DCOM DCE/RPC Local NTLM Reflection Elevation of Privilege
    - Windows: Local WebDAV NTLM Reflection Elevation of Privilege
    - **Hot Potato**
        - Hot Potato
            - Hot Potato (aka: Potato) takes advantage of known issues in Windows to gain local privilege escalation in default configurations, namely NTLM relay (specifically HTTP->SMB relay) and NBNS spoofing.
        - SmashedPotato
- **Tokens**
    - Abusing Token Privileges For LPE - drone/breenmachine
    - The Art of Becoming TrustedInstaller
        - There's many ways of getting the TI token other than these 3 techniques. For example as Vincent Yiu pointed out on Twitter if you've got easy access to a system token, say using Metasploit's getsystem command you can impersonate system and then open the TI token, it's just IMO less easy :-). If you get a system token with SeTcbPrivilege you can also call LogonUserExExW or LsaLogonUser where you can specify an set of additional groups to apply to a service token. Finally if you get a system

token with SeCreateTokenPrivilege (say from LSASS.exe if it's not running PPL) you can craft an arbitrary token using the NtCreateToken system call.

- Rotten Potato – Privilege Escalation from Service Accounts to SYSTEM - @breenmachine
- Windows: DCOM DCE/RPC Local NTLM Reflection Elevation of Privilege
- Social Engineering The Windows Kernel: Finding And Exploiting Token Handling Vulnerabilities - James Forshaw
- Social Engineering The Windows Kernel: Finding And Exploiting Token Handling Vulnerabilities - James Forshaw - BHUSA2015
  - One successful technique in social engineering is pretending to be someone or something you're not and hoping the security guard who's forgotten their reading glasses doesn't look too closely at your fake ID. Of course there's no hyperopic guard in the Windows OS, but we do have an ID card, the Access Token which proves our identity to the system and let's us access secured resources. The Windows kernel provides simple capabilities to identify fake Access Tokens, but sometimes the kernel or other kernel-mode drivers are too busy to use them correctly. If a fake token isn't spotted during a privileged operation local elevation of privilege or information disclosure vulnerabilities can be the result. This could allow an attacker to break out of an application sandbox, elevate to administrator privileges, or even compromise the kernel itself. This presentation is about finding and then exploiting the incorrect handling of tokens in the Windows kernel as well as first and third party drivers. Examples of serious vulnerabilities, such as CVE-2015-0002 and CVE-2015-0062 will be presented. It will provide clear exploitable patterns so that you can do your own security reviews for these issues. Finally, I'll discuss some of the ways of exploiting these types of vulnerabilities to elevate local privileges.
- token_manipulation
  - Bypass User Account Control by manipulating tokens (can bypass AlwaysNotify)
- **Rotten Potato**
  - Rotten Potato – Privilege Escalation from Service Accounts to SYSTEM - foxglove security

        - Rotten Potato Privilege Escalation from Service Accounts to SYSTEM - Stephen Breen Chris Mallz - Derbycon6
        - RottenPotatoNG
            - New version of RottenPotato as a C++ DLL and standalone C++ binary - no need for meterpreter or other tools.
    - **Obtaining System Privileges**
        - The “SYSTEM” challenge
        - Writeup of achieving system from limited user privs.
        - All roads lead to SYSTEM
        - Alternative methods of becoming SYSTEM - XPN
    - **Writeups**
        - Analyzing local privilege escalations in win32k
            - This paper analyzes three vulnerabilities that were found in win32k.sys that allow kernel-mode code execution. The win32k.sys driver is a major component of the GUI subsystem in the Windows operating system. These vulnerabilities have been reported by the author and patched in MS08-025. The first vulnerability is a kernel pool overflow with an old communication mechanism called the Dynamic Data Exchange (DDE) protocol. The second vulnerability involves improper use of the ProbeForWrite function within string management functions. The third vulnerability concerns how win32k handles system menu functions. Their discovery and exploitation are covered.
        - Some forum posts on Win Priv Esc
        - Post Exploitation Using netNTLM Downgrade attacks - Fishnet/Archive.org
        - Old Privilege Escalation Techniques
        - How to own any windows network with group policy hijacking attacks
        - Windows 7 ‘Startup Repair’ Authentication Bypass
        - Windows Privilege Escalation Methods for Pentesters - pentest.blog
        - Windows Privilege Escalation Guide - sploitspren(2018)

        - Nice methodology/walk through of Windows PrivEsc methods and tactics
    - Linux Vulnerabilities Windows Exploits: Escalating Privileges with WSL - BlueHat IL 2018 - Saar Amar
        - Slides
    - Escalating Privileges with CylancePROTECT - atredis
- **Talks/Videos**
    - Hacking windows through the Windows API; delves into windows api, how it can break itself
    - Sedating the Watchdog Abusing Security Products to Bypass Windows Protections - Tomer Bit - BSidesSF
    - Black hat talk on Windows Privilege Escalation
    - Level Up! - Practical Windows Privilege Escalation
    - Extreme Privelege Escalataion on Windows8 UEFI Systems
        - Slides
        - Summary by stormehh from reddit: “In this whitepaper (and accompanying Defcon/Blackhat presentations), the authors demonstrate vulnerabilities in the UEFI "Runtime Service" interface accessible by a privileged userland process on Windows 8. This paper steps through the exploitation process in great detail and demonstrates the ability to obtain code execution in SMM and maintain persistence by means of overwriting SPI flash”
    - The Travelling Pentester: Diaries of the Shortest Path to Compromise
    - Windows Privilege Escalation - Riyaz Walikar
- **Tools**
    - Windows Exploit Suggester
        - [Blogpost]https://blog.gdssecurity.com/labs/2014/7/11/introducing-windows-exploit-suggester.html
        - This tool compares a targets patch levels against the Microsoft vulnerability database in order to detect potential missing patches on the target. It also notifies the user if there are public exploits and Metasploit modules available for the missing bulletins.
    - PowerUp
        - Windows Privilege Escalation through Powershell

    - ElevateKit
        - The Elevate Kit demonstrates how to use third-party privilege escalation attacks with Cobalt Strike's Beacon payload.
    - kernelpop
        - kernel privilege escalation enumeration and exploitation framework
    - BeRoot
    - Pompem
        - Pompem is an open source tool, designed to automate the search for Exploits and Vulnerability in the most important databases. Developed in Python, has a system of advanced search, that help the work of pentesters and ethical hackers. In the current version, it performs searches in PacketStorm security, CXSecurity, ZeroDay, Vulners, National Vulnerability Database, WPScan Vulnerability Database
    - AccessChk
        - As a part of ensuring that they've created a secure environment Windows administrators often need to know what kind of accesses specific users or groups have to resources including files, directories, Registry keys, global objects and Windows services. AccessChk quickly answers these questions with an intuitive interface and output.
    - AutoDane at BSides Cape Town
    - Auto DANE
        - Auto DANE attempts to automate the process of exploiting, pivoting and escalating privileges on windows domains.
    - lonelypotato
        - Modified version of RottenPotatoNG C++
        - Blogpost
    - psgetsystem
        - getsystem via parent process using ps1 & embeded c#
- **Misc Privilege Escalation**

    - dtappgather-poc.sh
        - Exploit PoC reverse engineered from EXTREMEPARR which provides local root on Solaris 7 - 11 (x86 & SPARC). Uses a environment variable of setuid binary dtappgather to manipulate file permissions and create a user owned directory anywhere on the system (as root). Can then add a shared object to locale folder and run setuid binaries with an untrusted library file.
    - Privilege Escalation Using Keepnote
    - #AVGater: Getting Local Admin by Abusing the Anti-Virus Quarantine
    - VMware Escape Exploit
        - VMware Escape Exploit before VMware WorkStation 12.5.5

Powershell Things

- **101**
- **Educational**
    - Get-Help: An Intro to PowerShell and How to Use it for Evil - Jared Haight
    - Brosec
        - Brosec is a terminal based reference utility designed to help us infosec bros and broettes with usefuPowershelll (yet sometimes complex) payloads and commands that are often used during work as infosec practitioners. An example of one of Brosec's most popular use cases is the ability to generate on the fly reverse shells (python, perl, powershell, etc) that get copied to the clipboard.
    - Introducing PowerShell into your Arsenal with PS>Attack - Jared Haight
        - Introducing PS Attack, a portable PowerShell attack toolkit - Jared Haight
    - PowerShell Secrets and Tactics Ben0xA
    - Egress Testing using PowerShell
- **Articles/Blogposts/Presentations/Talks/Writeups**

    - Client Side attacks using Powershell
    - Accessing the Windows API in PowerShell via internal .NET methods and reflection
        - It is possible to invoke Windows API function calls via internal .NET native method wrappers in PowerShell without requiring P/Invoke or C# compilation. How is this useful for an attacker? You can call any Windows API function (exported or non-exported) entirely in memory. For those familiar with Metasploit internals, think of this as an analogue to railgun.
    - PSReflect
        - Easily define in-memory enums, structs, and Win32 functions in PowerShell
- **Command and Control**
    - Empire
        - Empire is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent. It is the merge of the previous PowerShell Empire and Python EmPyre projects. The framework offers cryptologically-secure communications and a flexible architecture. On the PowerShell side, Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework. PowerShell Empire premiered at BSidesLV in 2015 and Python EmPyre premeiered at HackMiami 2016.
    - Koadic
        - Koadic, or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. The major difference is that Koadic does most of its operations using Windows Script Host (a.k.a. JScript/VBScript), with compatibility in the core to support a default installation of Windows 2000 with no service packs (and potentially even versions of NT4) all the way through Windows 10.
    - Babadook
        - Connection-less Powershell Persistent and Resilient Backdoor
- **Active Directory**
    - Offensive Active Directory with Powershell

- Attacking ADFS Endpoints with PowerShell
- Find AD users with empty password using PowerShell
- LDAPDomainDump
  - In an Active Directory domain, a lot of interesting information can be retrieved via LDAP by any authenticated user (or machine). This makes LDAP an interesting protocol for gathering information in the recon phase of a pentest of an internal network. A problem is that data from LDAP often is not available in an easy to read format. ldapdomaindump is a tool which aims to solve this problem, by collecting and parsing information available via LDAP and outputting it in a human readable HTML format, as well as machine readable json and csv/tsv/greppable files.
- ACLight
  - The tool queries the Active Directory (AD) for its objects' ACLs and then filters and analyzes the sensitive permissions of each one. The result is a list of domain privileged accounts in the network (from the advanced ACLs perspective of the AD). You can run the scan with just any regular user (could be non-privileged user) and it automatically scans all the domains of the scanned network forest.
- MailSniper
  - MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.). It can be used as a non-administrative user to search their own email, or by an Exchange administrator to search the mailboxes of every user in a domain. MailSniper also includes additional modules for password spraying, enumerating users/domains, gathering the Global Address List from OWA and EWS, and checking mailbox permissions for every Exchange user at an organization.
- I hunt sys admins 2.0
- Invoke-TheHash
  - Invoke-TheHash contains PowerShell functions for performing pass the hash WMI and SMB tasks. WMI and SMB services are accessed through .NET TCPClient connections. Authentication is performed by passing an NTLM hash into the NTLMv2 authentication protocol. Local administrator privilege is not required client-side.
- LAPSToolkit

        - Tool to audit and attack LAPS environments
    - Wireless_Query
        - Query Active Directory for Workstations and then Pull their Wireless Network Passwords. This tool is designed to pull a list of machines from AD and then use psexec to pull their wireless network passwords. This should be run with either a DOMAIN or WORKSTATION Admin account.
    - Grouper
        - Grouper is a slightly wobbly PowerShell module designed for pentesters and redteamers (although probably also useful for sysadmins) which sifts through the (usually very noisy) XML output from the Get-GPOReport cmdlet (part of Microsoft's Group Policy module) and identifies all the settings defined in Group Policy Objects (GPOs) that might prove useful to someone trying to do something fun/evil.
- **AV Bypass Stuff**
    - Invoke-Obfuscation
        - Invoke-Obfuscation is a PowerShell v2.0+ compatible PowerShell command and script obfuscator.
        - Presentation
        - Invoke-Obfuscation: PowerShell obFUsk8tion Techniques & How To (Try To) D""e `Tec` T 'Th'+'em'
    - Pulling Back the Curtains on EncodedCommand PowerShell Attacks
    - Invoke-CradleCrafter: Moar PowerShell obFUsk8tion by Daniel Bohannon
    - Invoke-CradleCrafter v1.1
- **Bypass Powershell Restrictions**
    - **Articles/Videos**
        - AMSI: How Windows 10 Plans to Stop Script-Based Attacks and How Well It Does It - Blogpost
        - AMSI: How Windows 10 Plans to Stop Script-Based Attaacks and How Well It Does It - BH US16
        - 15 Ways to Bypass the PowerShell Execution Policy15 Ways to bypass
        - AMSI Bypass With a Null Character
            - Patched Feb2018
        - PSAmsi - An offensive PowerShell module for interacting with the Anti-Malware Scan Interface in Windows 10

        - Bypassing AMSI via COM Server Hijacking
        - PowerShell ScriptBlock Logging Bypass
        - Powershell without Powershell to bypass app whitelist
        - Empire without PowerShell.exe
        - Exploiting PowerShell Code Injection Vulnerabilities to Bypass Constrained Language Mode
        - PSShell
            - PSShell is an application written in C# that does not rely on powershell.exe but runs powershell commands and functions within a powershell runspace environment (.NET). It doesn't need to be "installed" so it's very portable.
    - **Tools**
        - DigitalSignature-Hijack.ps1
            - Hijack Digital Signatures – PowerShell Script - pentestlab
        - PoCSubjectInterfacePackage
            - A proof-of-concept subject interface package (SIP) used to demonstrate digital signature subversion attacks.
        - PSAmsi
            - PSAmsi is a tool for auditing and defeating AMSI signatures.
        - nps - Not PowerShell
            - Execute powershell without powershell.exe
        - nps_payload
            - This script will generate payloads for basic intrusion detection avoidance. It utilizes publicly demonstrated techniques from several different sources.
        - PowerShdll
            - Run PowerShell with rundll32. Bypass software restrictions.
        - p0wnedShell

        - p0wnedShell is an offensive PowerShell host application written in C# that does not rely on powershell.exe but runs powershell commands and functions within a powershell runspace environment (.NET).
    - UnmanagedPowerShell
    - PowerOPS: PowerShell for Offensive Operations
        - PowerOPS Github page
        - PowerOPS is an application written in C# that does not rely on powershell.exe but runs PowerShell commands and functions within a powershell runspace environment (.NET). It intends to include multiple offensive PowerShell modules to make the process of Post Exploitation easier.
    - PowerLine
        - Presentation
    - Bat Armor
        - Bypass PowerShell execution policy by encoding ps script into bat file.
- **Bypass Logging**
    - A Critique of Logging Capabilities in PowerShell v6
        - Introduces 'PowerShell Upgrade Attack'
    - Bypass for PowerShell ScriptBlock Warning Logging of Suspicious Commands - cobbr.io
    - PowerShell ScriptBlock Logging Bypass - cobbr.io
- **Frameworks**
    - Empire
    - Powersploit
    - Nishang
        - Nishang is a framework and collection of scripts and payloads which enables usage of PowerShell for offensive security, penetration testing and red teaming. Nishang is useful during all phases of penetration testing.
- **Dumping/Grabbing Creds**
    - PShell Script: Extract All GPO Set Passwords From Domain

        - This script parses the domain's Policies folder looking for Group.xml files. These files contain either a username change, password setting, or both. This gives you the raw data for local accounts and/or passwords enforced using Group Policy Preferences. Microsoft chose to use a static AES key for encrypting this password. How awesome is that!
    - mimikittenz
        - A post-exploitation powershell tool for extracting juicy info from memory.
    - Inveigh
        - Inveigh is a PowerShell LLMNR/mDNS/NBNS spoofer and man-in-the-middle tool designed to assist penetration testers/red teamers that find themselves limited to a Windows system.
    - PowerMemory
        - Exploit the credentials present in files and memory. PowerMemory levers Microsoft signed binaries to hack Microsoft operating systems.
    - Dump-Clear-Text-Password-after-KB2871997-installed
        - Auto start Wdigest Auth,Lock Screen,Detect User Logon and get clear password.
    - SessionGopher
        - SessionGopher is a PowerShell tool that finds and decrypts saved session information for remote access tools. It has WMI functionality built in so it can be run remotely. Its best use case is to identify systems that may connect to Unix systems, jump boxes, or point-of-sale terminals. SessionGopher works by querying the HKEY_USERS hive for all users who have logged onto a domain-joined box at some point. It extracts PuTTY, WinSCP, SuperPuTTY, FileZilla, and RDP saved session information. It automatically extracts and decrypts WinSCP, FileZilla, and SuperPuTTY saved passwords. When run in Thorough mode, it also searches all drives for PuTTY private key files (.ppk) and extracts all relevant private key information, including the key itself, as well as for Remote Desktop (.rdp) and RSA (.sdtid) files.
    - Invoke-WCMDump
        - PowerShell script to dump Windows credentials from the Credential Manager. Invoke-WCMDump enumerates Windows credentials in the Credential Manager and then extracts available information about each one.

Passwords are retrieved for "Generic" type credentials, but can not be retrived by the same method for "Domain" type credentials. Credentials are only returned for the current user. Does not require admin privileges!

    - MimiDbg
        - PowerShell oneliner to retrieve wdigest passwords from the memory
    - mimikittenz
        - mimikittenz is a post-exploitation powershell tool that utilizes the Windows function ReadProcessMemory() in order to extract plain-text passwords from various target processes.
- **Grabbing Useful files**
    - BrowserGatherer
        - Fileless Extraction of Sensitive Browser Information with PowerShell
    - SessionGopher
        - SessionGopher is a PowerShell tool that uses WMI to extract saved session information for remote access tools such as WinSCP, PuTTY, SuperPuTTY, FileZilla, and Microsoft Remote Desktop. It can be run remotely or locally.
    - CC_Checker
        - CC_Checker cracks credit card hashes with PowerShell.
    - BrowserGather
        - Fileless Extraction of Sensitive Browser Information with PowerShell. This project will include various cmdlets for extracting credential, history, and cookie/session data from the top 3 most popular web browsers (Chrome, Firefox, and IE). The goal is to perform this extraction entirely in-memory, without touching the disk of the victim. Currently Chrome credential and cookie extraction is supported.
- **Malicious X (Document/Macro/whatever) Generation**
    - psWar.py
    - Code that quickly generates a deployable .war for a PowerShell one-liner
- **Priv Esc / Post Ex Scripts**
    - PowerUp

        - PowerUp is a powershell tool to assist with local privilege escalation on Windows systems. It contains several methods to identify and abuse vulnerable services, as well as DLL hijacking opportunities, vulnerable registry settings, and escalation opportunities.
    - Sherlock
        - PowerShell script to quickly find missing software patches for local privilege escalation vulnerabilities.
    - JSRat-Py
        - implementation of JSRat.ps1 in Python so you can now run the attack server from any OS instead of being limited to a Windows OS with Powershell enabled
    - ps1-toolkit
        - This is a set of PowerShell scripts that are used by many penetration testers released by multiple leading professionals. This is simply a collection of scripts that are prepared and obfuscated to reduce level of detectability and to slow down incident response from understanding the actions performed by an attacker.
- **Recon**
    - Invoke-ProcessScan
        - Gives context to a system. Uses EQGRP shadow broker leaked list to give some descriptions to processes.
    - Veil-PowerView
        - Veil-PowerView is a powershell tool to gain network situational awareness on Windows domains. It contains a set of pure-powershell replacements for various windows `net *` commands, which utilize powershell AD hooks and underlying Win32 API functions to perform useful Windows domain functionality.
    - PowerShell-AD-Recon
        - AD PowerShell Recon Scripts
- **Running Powershell without PowerShell**
    - PowerLessShell
        - PowerLessShell rely on MSBuild.exe to remotely execute PowerShell scripts and commands without spawning powershell.exe. You can also execute raw shellcode using the same approach.
- **Miscellaneous Useful Things**

- Invoke-DCOM.ps1
- PowerShell and Token Impersonation
- Harness
  - Harness is remote access payload with the ability to provide a remote interactive PowerShell interface from a Windows system to virtually any TCP socket. The primary goal of the Harness Project is to provide a remote interface with the same capabilities and overall feel of the native PowerShell executable bundled with the Windows OS.
- DPAPI Primer for Pentesters - webstersprodigy
- **Utilities**
  - 7Zip4Powershell
    - Powershell module for creating and extracting 7-Zip archives
- **Servers**
  - Dirty Powershell Webserver
  - Pode
    - Pode is a PowerShell framework that runs HTTP/TCP listeners on a specific port, allowing you to host REST APIs, Web Pages and SMTP/TCP servers via PowerShell. It also allows you to render dynamic HTML using PSHTML files.
- Invoke-VNC
  - Powershell VNC injector
- Invoke-BSOD
  - A PowerShell script to induce a Blue Screen of Death (BSOD) without admin privileges. Also enumerates Windows crash dump settings. This is a standalone script, it does not depend on any other files.
- Invoke-SocksProxy
  - Creates a Socks proxy using powershell.

DLL Stuff

DLL Stuff * Creating a Windows DLL with Visual Basic * Calling DLL Functions from Visual Basic Applications - msdn

- **DLL Hijacking**
  - Dynamic-Link Library Hijacking
  - Crash Course in DLL Hijacking
  - VB.NET Tutorial - Create a DLL / Class Library
- **DLL Injection**
  - DLL Injection and Hooking
  - Windows DLL Injection Basics
  - Crash Course in DLL Hijacking
  - Windows DLL Injection Basics - OpenSecurityTraining
  - An Improved Reflective DLL Injection Technique - Dan Staples
  - Reflective DLL Injection with PowerShell - clymb3r
  - Delivering custom payloads with Metasploit using DLL injection - blog.cobalstrike
- **DLL Tools**
  - rattler
    - Rattler is a tool that automates the identification of DLL's which can be used for DLL preloading attacks.
  - injectAllTheThings
    - Single Visual Studio project implementing multiple DLL injection techniques (actually 7 different techniques) that work both for 32 and 64 bits. Each technique has its own source code file to make it easy way to read and understand.
- **Group Policy Preferences trick**
  - 1
  - 2

    - 3
- **Other**
    - Pazuzu
        - Pazuzu is a Python script that allows you to embed a binary within a precompiled DLL which uses reflective DLL injection. The goal is that you can run your own binary directly from memory. This can be useful in various scenarios.

Privilege Escalation - OS X

- **Writeups**
    - Hidden backdoor API to root privileges in Apple OS X
    - Works on 10.7 -> 10.10.2
    - Mac OS X local privilege escalation (IOBluetoothFamily)
    - Privilege Escalation on OS X below 10.0
    - Hacking Mac With EmPyre
    - macOS Code Signing In Depth
    - Privilege escalation on OS X – without exploits - n00py.io
    - Why `<blank>` Gets You Root
    - osascript: for local phishing
    - abusing the local upgrade process to bypass SIP - Objective-see
    - Native Mac OS X Application / Mach-O Backdoors for Pentesters
    - Attacking OSX for fun and profit tool set limiations frustration and table flipping Dan Tentler - ShowMeCon
    - IOHIDeous
- **Tools**
    - BigPhish

        - This issue has been resolved by Apple in MacOS Sierra by enabling tty_tickets by default. NOTE: All other MacOS operation system (El Capitan, Yosemite, Mavericks etc...) still remain vulnerable to this exploit.
    - osxinj
        - Another dylib injector. Uses a bootstrapping module since mach_inject doesn't fully emulate library loading and crashes when loading complex modules.
    - kcap
        - This program simply uses screen captures and programmatically generated key and mouse events to locally and graphically man-in-the-middle an OS X password prompt to escalate privileges.
    - Platypus
        - Platypus is a Mac OS X developer tool that creates native Mac applications from interpreted scripts such as shell scripts or Perl, Ruby and Python programs. This is done by wrapping the script in an application bundle along with a native executable binary that runs the script.

General Post Exploitation

- Adversarial Post Ex - Lessons from the Pros
- portia
    - Portia aims to automate a number of techniques commonly performed on internal network penetration tests after a low privileged account has been compromised.
- Meta-Post Exploitation - Using Old, Lost, Forgotten Knowledge
- dvcs-ripper
    - Rip web accessible (distributed) version control systems: SVN, GIT, Mercurial/hg, bzr, ... It can rip repositories even when directory browsing is turned off.
- Shellpaste
    - Tiny snippet of code that pulls ASCII shellcode from pastebin and executes it. The purpose of this is to have a minimal amount of benign code so AV doesn't freak out, then it pulls down the evil stuff. People have been doing this

kind of stuff for years so I take no credit for the concept. That being said, this code (or similar code) works surprisingly often during pentests when conventional malware fails.

- JVM Post-Exploitation One-Liners
- Meltdown PoC for Reading Google Chrome Passwords

Post-Exploitation Linux

- **101**linpost
- **Articles/Blogposts/Writeups**
  - More on Using Bash's Built-in /dev/tcp File (TCP/IP)
- **Tools**
  - nullinux
    - nullinux is an internal penetration testing tool for Linux that can be used to enumerate OS information, domain information, shares, directories, and users through SMB. If no username and password are provided, nullinux will attempt to connect to the target using an SMB null session. Unlike many of the enumeration tools out there already, nullinux can enumerate multiple targets at once and when finished, creates a users.txt file of all users found on the host(s). This file is formatted for direct implementation and further exploitation.This program assumes Python 2.7, and the smbclient package is installed on the machine. Run the setup.sh script to check if these packages are installed.

Post-Exploitation OS X

- **Educational**
  - The ‘app’ you can’t trash: how SIP is broken in High Sierra
- **Grabbing Goodies**

    - Mac OS X Keychain Forensic Tool
        - The chainbreaker can extract user credential in a Keychain file with Master Key or user password in forensically sound manner. Master Key candidates can be extracted from volafox or volatility keychaindump module. Supports: Snow Leopard, Lion, Mountain Lion, Mavericks, Yosemite, El Capitan, (High) Sierra
- **Recon**
    - Orchard
        - Live off the land for macOS. This program allows users to do Active Directory enumeration via macOS' JXA (JavaScript for Automation) code. This is the newest version of AppleScript, and thus has very poor documentation on the web.
- **Persistence**
    - EvilOSX
        - A pure python, post-exploitation, RAT (Remote Administration Tool) for macOS / OSX.
    - p0st-ex
        - Post-exploitation scripts for OS X persistence and privesc
    - Running and disguising programs through XCode shims on OS X

Post-Exploitation Windows

- **101**
    - Windows - Application Shims
    - Windows CMD Reference - ms
- **Articles/Blogposts/Writeups**
    - Dumping user passwords in plaintext on Windows 8.1 and Server 2012
    - Post-Exploitation on Windows using ActiveX Controls

    - Windows Driver and Service enumeration with Python
    - LAPS - Part 1 - Rastamouse
        - The purpose of this post, is to put together a more complete end-to-end process for mapping out the LAPS configuration in a domain.
    - [LAPS - Part 2 - Rastamouse])(https://rastamouse.me/2018/03/laps---part-2/)
        - In this part, we'll look at various ways LAPS can be abused for persistence purposes.
    - DSCompromised: A Windows DSC Attack Framework - Matt Hastings, Ryan Kazanciyan - BH Asia16

- **Code Injection**

    - DLL Injection - Pentestlab
    - Process-Hollowing
        - Great explanation of Process Hollowing
    - atom-bombing
        - Here's a new code injection technique, dubbed AtomBombing, which exploits Windows atom tables and Async Procedure Calls (APC). Currently, this technique goes undetected by common security solutions that focus on preventing infiltration.
        - ATOMBOMBING: BRAND NEW CODE INJECTION FOR WINDOWs
    - DoubleAgent
        - DoubleAgent is a new Zero-Day technique for injecting code and maintaining persistence on a machine (i.e. auto-run).
        - Technical Writeup
    - Syringe
        - Syringe is a general purpose DLL and code injection utility for 32 and 64-bit Windows. It is capable of executing raw shellcode as well as injecting shellcode or a DLL directly into running processes.

- **Tools**

    - Windows DACL Enum Project
        - A collection of tools to enumerate and analyse Windows DACLs
    - WMI Shell Tool
        - The WMI shell tool that we have developed allows us to execute commands and get their output using only the WMI infrastructure, without any help from other services, like the SMB server. With the wmi-shell tool we can execute commands, upload files and recover Windows passwords remotely using only the WMI service available on port 135.
    - WMIcmd
        - A command shell wrapper using only WMI for Microsoft Windows
    - Portia
        - Portia aims to automate a number of techniques commonly performed on internal network penetration tests after a low privileged account has been compromised. Portia performs privilege escalation as well as lateral movement automatically in the network
    - NetRipper
        - NetRipper is a post exploitation tool targeting Windows systems which uses API hooking in order to intercept network traffic and encryption related functions from a low privileged user, being able to capture both plain-text traffic and encrypted traffic before encryption/after decryption.

Active Directory

- **101**
    - What is Active Directory Domain Services and how does it work?
- **General**
    - Offensive Active Directory with Powershell
    - Abusing Active Directory in Post-Exploitation

        - Windows APIs are often a blackbox with poor documentation, taking input and spewing output with little visibility on what actually happens in the background. By reverse engineering (and abusing) some of these seemingly benign APIs, we can effectively manipulate Windows into performing stealthy custom attacks using previously unknown persistent and injection techniques. In this talk, we'll get Windows to play with itself nonstop while revealing 0day persistence, previously unknown DLL injection techniques, and Windows API tips and tricks. To top it all off, a custom HTTP beaconing backdoor will be released leveraging the newly released persistence and injection techniques. So much Windows abuse, so little time.
    - Accessing Internal Fileshares through Exchange ActiveSync
    - Pen Testing Active Directory Series
    - Beyond the MCSE: Red Teaming Active Directory
    - Red vs Blue: Modern Active Directory Attacks & Defense - Defcon23
    - Red Vs. Blue: Modern Active Directory Attacks, Detection, And Protection - BHUSA15
    - Abusing Active Directory in Post Exploitation - Carlos Perez - Derbycon 4
    - Setting up Samba as a Domain Member
    - ATA Suspicious Activity Playbook - technet.ms
    - DCShadow explained: A technical deep dive into the latest AD attack technique - Luc Delsalle
    - Skeleton Key Malware Analysis - SecureWorks
- **Specific Vulnerabilities**
    - Practically Exploiting MS15-014 and MS15-011 - MWR
    - MS15-011 - Microsoft Windows Group Policy real exploitation via a SMB MiTM attack - coresecurity
- **Getting(Hunting) Domain User(s)**
    - Active Directory Control Paths
        - Control paths in Active Directory are an aggregation of "control relations" between entities of the domain (users, computers, groups, GPO, containers, etc.) which can be visualized as graphs (such as above) and whose purpose is to answer questions like "Who can get 'Domain Admins' privileges ?" or "What resources can a user control ?" and even "Who can read the CEO's emails ?".

    - Exchange-AD-Privesc
        - This repository provides a few techniques and scripts regarding the impact of Microsoft Exchange deployment on Active Directory security. This is a side project of AD-Control-Paths, an AD permissions auditing project to which I recently added some Exchange-related modules.
    - hunter
        - (I)user hunter using WinAPI calls only
    - icebreaker
        - Automates network attacks against Active Directory to deliver you piping hot plaintext credentials when you're inside the network but outside of the Active Directory environment. Performs 5 different network attacks for plaintext credentials as well as hashes. Autocracks hashes found with JohnTheRipper and the top 10 million most common passwords.
- **Getting(Hunting) Domain Admin(s)**
    - 5 Ways to Find Systems Running Domain Admin Processes
    - Attack Methods for Gaining Domain Admin Rights in Active Directory
    - Nodal Analysis of Domain Trusts – Maximizing the Win!
    - Derivative Local Admin
    - Faster Domain Escalation using LDAP
    - Abusing DNSAdmins privilege for escalation in Active Directory
    - How Attackers Dump Active Directory Database Credentials
    - “I Hunt Sys Admins”
    - I Hunt Sysadmins 2.0 - slides
        - It covers various ways to hunt for users in Windows domains, including using PowerView.
    - Requiem For An Admin, Walter Legowski (@SadProcessor) - BSides Amsterdam 2017
        - Orchestrating BloodHound and Empire for Automated AD Post-Exploitation. Lateral Movement and Privilege Escalation are two of the main steps in the Active Directory attacker kill- chain. Applying the 'assume breach' mentality, more and more companies are asking for red-teaming type of assessments, and security researcher

have therefor developed a wide range of open-source tools to assist them during these engagements. Out of these, two have quickly gained a solid reputation: PowerShell Empire and BloodHound (Both by @Harmj0y & ex-ATD Crew). In this Session, I will be presenting DogStrike, a new tool (PowerShell Modules) made to interface Empire & BloodHound, allowing penetration testers to merge their Empire infrastructure into the bloodhound graph database. Doing so allows the operator to request a bloodhound path that is 'Agent Aware', and makes it possible to automate the entire kill chain, from initial foothold to DA - or any desired part of an attacker's routine. Presentation will be demo-driven. Code for the module will be made public after the presentation. Automation of Active Directory post-exploitation is going to happen sooner than you might think. (Other tools are being released with the same goal). Is it a good thing? Is it a bad thing? If I do not run out of time, I would like to finish the presentation by opening the discussion with the audience and see what the consequences of automated post- exploitation could mean, from the red, the blue or any other point of view... : DeathStar by @Byt3Bl33d3r | GoFetch by @TalTheMaor.

    - Gaining Domain Admin from Outside Active Directory - markitzeroday

- **Group Policy**
    - Get-GPTrashFire
        - Identifiying and Abusing Vulnerable Configuraitons in MS AD Group Policy
- **MS SQL Server** * Hacking SQL Server on Scale with PowerShell - Secure360 2017 * Using SQL Server for attacking a Forest Trust
- **Pass-the-`*`**
    - **Hash**
        - For this kind of attack and related ones, check out the Network Attacks page, under Pass-the-Hash.
        - Windows Credential Guard & Mimikatz - nviso
    - **Ticket**
        - How To Pass the Ticket Through SSH Tunnels
        - Pass-the-ticket - ldapwiki
        - **Silver**

        - Sneaky Active Directory Persistence #16: Computer Accounts & Domain Controller Silver Tickets - adsecurity
        - Impersonating Service Accounts with Silver Tickets - stealthbits
        - Mimikatz 2.0 - Silver Ticket Walkthrough
    - **Golden**
        - mimikatz - golden ticket
        - Golden Ticket - ldapwiki
        - Advanced Targeted Attack. PoC Golden Ticket Attack - BSides Tampa 17
        - Complete Domain Compromise with Golden Tickets - stealthbits
        - Pass-the-(Golden)-Ticket with WMIC
- **Recon**
    - **Articles/Blogposts/Presentations/Talks/Writeups**
        - Automating the Empire with the Death Star: getting Domain Admin with a push of a button
        - Active Directory Pentest Recon Part 1: SPN Scanning aka Mining Kerberos Service Principal Names
    - **Tools**
        - Invoke-HostRecon
            - This function runs a number of checks on a system to help provide situational awareness to a penetration tester during the reconnaissance phase. It gathers information about the local system, users, and domain information. It does not use any 'net', 'ipconfig', 'whoami', 'netstat', or other system commands to help avoid detection.
        - HostEnum
            - A PowerShell v2.0 compatible script comprised of multiple system enumeration / situational awareness techniques collected over time. If system is a member of a Windows domain, it can also perform limited domain enumeration with the -Domain switch. However, domain enumeration is significantly limited with the intention that PowerView or BoodHound could also be used.
        - ADRecon

        - ADRecon is a tool which extracts various artifacts (as highlighted below) out of an AD environment in a specially formatted Microsoft Excel report that includes summary views with metrics to facilitate analysis. The report can provide a holistic picture of the current state of the target AD environment. It can be run from any workstation that is connected to the environment, even hosts that are not domain members. Furthermore, the tool can be executed in the context of a non-privileged (i.e. standard domain user) accounts. Fine Grained Password Policy, LAPS and BitLocker may require Privileged user accounts. The tool will use Microsoft Remote Server Administration Tools (RSAT) if available, otherwise it will communicate with the Domain Controller using LDAP.
    - DeathStar
        - DeathStar is a Python script that uses Empire's RESTful API to automate gaining Domain Admin rights in Active Directory environments using a variety of techinques.
    - AdEnumerator
        - Active Directory enumeration from non-domain system. Powershell script
    - pywerview
        - A (partial) Python rewriting of PowerSploit's PowerView
    - BloodHound
        - BloodHound is a single page Javascript web application, built on top of Linkurious, compiled with Electron, with a Neo4j database fed by a PowerShell ingestor. BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify. Defenders can use BloodHound to identify and eliminate those same attack paths. Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an Active Directory environment.
        - My First Go with BloodHound
        - Lay of the Land with BloodHound
        - ANGRYPUPPY
            - Bloodhound Attack Path Execution for Cobalt Strike

        - GoFetch
            - GoFetch is a tool to automatically exercise an attack plan generated by the BloodHound application. GoFetch first loads a path of local admin users and computers generated by BloodHound and converts it to its own attack plan format. Once the attack plan is ready, GoFetch advances towards the destination according to plan step by step, by successively applying remote code execution techniques and compromising credentials with Mimikatz.
        - DogWhisperer - BloodHound Cypher Cheat Sheet (v2)
        - Extending BloodHound: Track and Visualize Your Compromise
            - Customizing BloodHound's UI and taking advantage of Custom Queries to document a compromise, find collateral spread of owned nodes, and visualize deltas in privilege gains.
        - DomainTrustExplorer
            - Python script for analyis of the "Trust.csv" file generated by Veil PowerView. Provides graph based analysis and output.
    - NtdsAudit
        - NtdsAudit is an application to assist in auditing Active Directory databases. It provides some useful statistics relating to accounts and passwords. It can also be used to dump password hashes for later cracking.
    - Orchard
        - Live off the land for macOS. This program allows users to do Active Directory enumeration via macOS' JXA (JavaScript for Automation) code. This is the newest version of AppleScript, and thus has very poor documentation on the web.
- **Skeleton Key**
    - Active Directory Domain Controller Skeleton Key Malware & Mimikatz - ADSecurity
    - Skeleton Key Malware Analysis - SecureWorks
- **Miscellaneous Tools**
    - Windows Vault Password Dumper

        - The following code shows how to use native undocumented functions of Windows Vault API to enumerate and extract credentials stored by Microsoft Windows Vault. The code has been successfully tested on Windows7 and Windows8 operating systems.
    - knit_brute.sh
        - A quick tool to bruteforce an AD user's password by requesting TGTs from the Domain Controller with 'kinit'
    - LyncSniper
        - A tool for penetration testing Skype for Business and Lync deployments
        - Blogpost/Writeup
    - LyncSmash
        - a collection of tools to enumerate and attack self-hosted Skype for Business and Microsoft Lync installations
        - Talk
        - Slides

Office Macros

Office Macros

- **101**
    - Getting Started with VBA in Office
- **General**
    - DLL Tricks with VBA to Improve Offensive Macro Capability
- **Tools**
    - MacroShop
        - Collection of scripts to aid in delivering payloads via Office Macros.
    - Generate-Macro

        - This Powershell script will generate a malicious Microsoft Office document with a specified payload and persistence method.
    - wePWNise
        - WePWNise generates architecture independent VBA code to be used in Office documents or templates and automates bypassing application control and exploit mitigation software

---

Email/Microsoft Exchange

Microsoft Exchange

- **101**
- **General**
    - Outlook and Exchange for the Bad Guys Nick Landers
    - #OLEOutlook - bypass almost every Corporate security control with a point'n'click GUI
    - Ruler Pivoting Through Exchange - Etienne Stalmans - TR17
- **Tools**
    - MailSniper
        - MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.). It can be used as a non-administrative user to search their own email, or by an administrator to search the mailboxes of every user in a domain.
    - Ruler
        - Ruler is a tool that allows you to interact with Exchange servers remotely, through either the MAPI/HTTP or RPC/HTTP protocol. The main aim is abuse the client-side Outlook features and gain a shell remotely.

Grabbing Goodies

- **Dumping Passwords**
  - CredCrack
    - CredCrack is a fast and stealthy credential harvester. It exfiltrates credentials recusively in memory and in the clear. Upon completion, CredCrack will parse and output the credentials while identifying any domain administrators obtained. CredCrack also comes with the ability to list and enumerate share access and yes, it is threaded! CredCrack has been tested and runs with the tools found natively in Kali Linux. CredCrack solely relies on having PowerSploit's "Invoke-Mimikatz.ps1" under the /var/www directory.
  - LaZagne
    - The LaZagne project is an open source application used to retrieve lots of passwords stored on a local computer. Each software stores its passwords using different techniques (plaintext, APIs, custom algorithms, databases, etc.). This tool has been developed for the purpose of finding these passwords for the most commonly-used software.
  - KeeThief
    - Methods for attacking KeePass 2.X databases, including extracting of encryption key material from memory.
  - pysecdump
    - pysecdump is a python tool to extract various credentials and secrets from running Windows systems. It currently extracts:
    - LM and NT hashes (SYSKEY protected); Cached domain passwords; LSA secrets; Secrets from Credential Manager (only some)
  - 3snake
    - Targeting rooted servers, reads memory from sshd and sudo system calls that handle password based authentication. Doesn't write any memory to the traced processes. Spawns a new process for every sshd and sudo command that is run. Listens for the proc event using netlink sockets to get candidate processes to trace. When it receives an sshd or sudo process ptrace is attached and traces read and write system calls, extracting strings related to password based authentication.

    - Internal Monologue Attack: Retrieving NTLM Hashes without Touching LSASS
- **Pillaging valuable Files/Logs/Items**
    - skype log viewer
        - Download and View Skype History Without Skype This program allows you to view all of your skype chat logs and then easily export them as text files. It correctly organizes them by conversation, and makes sure that group conversations do not get jumbled with one on one chats.
    - Pillaging .pst Files
    - swap_digger
        - swap_digger is a bash script used to automate Linux swap analysis for post-exploitation or forensics purpose. It automates swap extraction and searches for Linux user credentials, Web form credentials, Web form emails, HTTP basic authentication, WiFi SSID and keys, etc.
    - net-creds
        - Thoroughly sniff passwords and hashes from an interface or pcap file. Concatenates fragmented packets and does not rely on ports for service identification.
    - PCredz
        - This tool extracts Credit card numbers, NTLM(DCE-RPC, HTTP, SQL, LDAP, etc), Kerberos (AS-REQ Pre-Auth etype 23), HTTP Basic, SNMP, POP, SMTP, FTP, IMAP, etc from a pcap file or from a live interface.
- **Writeups**
    - Post exploitation trick - Phish users for creds on domains, from their own box
    - Dumping Windows Credentials
    - Unofficial Guide to Mimikatz
    - Capturing Windows 7 Credentials at Logon Using Custom Credential Provider
        - The quick lowdown: I wrote a DLL capable of logging the credentials entered at logon for Windows Vista, 7 and future versions which you can download at http://www.leetsys.com/programs/credentialprovider/cp.zip. The credentials are logged to a file located at c:\cplog.txt. Simply copy the dll to the system32 directory and run the included register.reg script to create the necessary registry settings.

    - Dump Windows password hashes efficiently - Part 1
    - Dumping hashes from Active Directory for cracking
    - NTDSXtract - Active Directory Forensics Framework
        - This framework was developed by the author in order to provide the community with a solution to extract forensically important information from the main database of Microsoft Active Directory (NTDS.DIT).
    - No one expect command execution!
    - Digging passwords in Linux swap
- **Tools**
    - You Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger
        - Keyloggers are a prominent class of malware that harvests sensitive data by recording any typed in information. Key- logger implementations strive to hide their presence using rootkit-like techniques to evade detection by antivirus and other system protections. In this paper, we present a new approach for implementing a stealthy keylogger: we explore the possibility of leveraging the graphics card as an alterna- tive environment for hosting the operation of a keylogger. The key idea behind our approach is to monitor the system's keyboard buffer directly from the GPU via DMA, without any hooks or modifications in the kernel's code and data structures besides the page table. The evaluation of our pro- totype implementation shows that a GPU-based keylogger can effectively record all user keystrokes, store them in the memory space of the GPU, and even analyze the recorded data in-place, with negligible runtime overhead.
    - SearchForCC
        - A collection of open source/common tools/scripts to perform a system memory dump and/or process memory dump on Windows-based PoS systems and search for unencrypted credit card track data.
    - KeeFarce
        - Extracts passwords from a KeePass 2.x database, directly from memory.
    - KeeThief
        - Methods for attacking KeePass 2.X databases, including extracting of encryption key material from memory.
    - **Linux**

        - mimipenguin
            - A tool to dump the login password from the current linux user
    - **Windows**
        - mimikatz
            - Mimikatz Overview, Defenses and Detection
            - Mimikatz Logs and Netcat
        - quarkspwdump
            - Dump various types of Windows credentials without injecting in any process.
        - SessionGopher
            - SessionGopher is a PowerShell tool that uses WMI to extract saved session information for remote access tools such as WinSCP, PuTTY, SuperPuTTY, FileZilla, and Microsoft Remote Desktop. It can be run remotely or locally.

Gaining Awareness/Situational Awareness

Situational Awareness

- **Active Directory**
    - Domain Trusts: Why You Should Care
    - Trusts You Might Have Missed
    - pywerview
        - A (partial) Python rewriting of PowerSploit's PowerView
    - Veil-PowerView
        - Veil-PowerView is a powershell tool to gain network situational awareness on Windows domains. It contains a set of pure-powershell replacements for various windows `net *` commands, which utilize powershell AD hooks and underlying Win32 API functions to perform useful Windows domain functionality.

    - PowerShell-AD-Recon
        - AD PowerShell Recon Scripts
- **Linux**
    - How to determine Linux guest VM virtualization technology
- **Egress Testing**
    - Egress Testing using PowerShell
    - Egress Buster Reverse Shell
        - Egress Buster Reverse Shell – Brute force egress ports until one if found and execute a reverse shell(from trustedsec)
- **Network Awareness**
    - Packet sniffing with powershell
- **Miscellaneous**
    - Finding your external IP:
        - Simply curl any of the following addresses: `ident.me, ifconfig.me or whatsmyip.akamai.com`
    - Determine Public IP from CLI

Persistence

- **Persistence**
    - List of low-level attacks/persistence techniques. HIGHLY RECOMMENDED!
    - How to Remotely Control Your PC (Even When it Crashes)
- **Backdooring**
    - **Articles/Writeups**
        - I'm In Your $PYTHONPATH, Backdooring Your Python Programs
        - Introduction to Manual Backdooring - abatchy17

        - An Introduction to Backdooring Operating Systems for Fun and trolling - Defcon22
    - **Tools**
        - Pyekaboo
            - Pyekaboo is a proof-of-concept program that is able to to hijack/hook/proxy Python module(s) thanks to $PYTHONPATH variable. It's like "DLL Search Order Hijacking" for Python.
        - Pybuild
            - PyBuild is a tool for automating the pyinstaller method for compiling python code into an executable. This works on Windows, Linux, and OSX (pe and elf formats)(From trustedsec)
        - Debinject
            - Inject malicious code into .debs
        - WSUSpect Proxy
            - This is a proof of concept script to inject 'fake' updates into non-SSL WSUS traffic. It is based on our Black Hat USA 2015 presentation, 'WSUSpect – Compromising the Windows Enterprise via Windows Update'
            - Whitepaper
- **Windows Persistence**
    - Windows Event Log Driven Back Doors
    - Thousand ways to backdoor a Windows domain (forest)
    - Windows Firewall Hook Enumeration
        - We’re going to look in detail at Microsoft Windows Firewall Hook drivers from Windows 2000, XP and 2003. This functionality was leveraged by the Derusbi family of malicious code to implement port-knocking like functionality. We’re going to discuss the problem we faced, the required reverse engineering to understand how these hooks could be identified and finally how the enumeration tool was developed.
    - Evading Autoruns Kyle Hanslovan Chris Bisnett - DerbyCon 7
        - Evading Autoruns - DerbyCon 7.0
    - Hiding Files by Exploiting Spaces in Windows Paths
    - Stealing passwords every time they change - carnal0wnage

- Installing and Registering a Password Filter DLL - msdn.ms
- **AppDomain**
  - Use AppDomainManager to maintain persistence
- **Alternate Data Streams**
  - Putting data in Alternate data streams and how to execute it - oddvar.moe
  - Kurt Seifried Security Advisory 003 (KSSA-003)
  - NTFS Alternate Data Streams for pentesters (part 1)
  - Using Alternate Data Streams to Persist on a Compromised Machine
  - Using Alternate Data Streams to Persist on a Compromised Machine - enigma0x3
  - Evading Autoruns
    - When it comes to offense, maintaining access to your endpoints is key. For defenders, it's equally important to discover these footholds within your network. During this talk, Kyle and Chris will expose several semi-public and private techniques used to evade the most common persistence enumeration tools. Their techniques will explore ways to re-invent the run key, unconventionally abuse search order, and exploit trusted applications. To complement their technical explanations, each bypass will include a live demo and recommendations for detection.
    - Talk
- **bitsadmin**
  - Temporal Persistence with bitsadmin and schtasks /userland-persistence-with-scheduled-tasks-and-com-handler-hijacking/)
- **COM**
  - COM Object hijacking: the discreet way of persistence
  - Userland Persistence with Scheduled Tasks and COM Handler Hijacking
- **.NET**
  - CLR-Persistence
    - Use CLR to inject all the .NET apps

        - Using CLR to maintain Persistence
    - **Registry**
        - Windows Registry Attacks: Knowledge Is the Best Defense
        - Windows Registry Persistence, Part 1: Introduction, Attack Phases and Windows Services
        - Windows Registry Persistence, Part 2: The Run Keys and Search-Order
        - List of autorun keys / malware persistence Windows registry entries
    - **SC/Scheduled Tasks**
        - Sc
            - Communicates with the Service Controller and installed services. The SC.exe program provides capabilities similar to those provided in Services in the Control Panel.
        - schtasks
        - Script Task
            - Persistence Via MSSQL
    - **Shims**
        - Post Exploitation Persistence With Application Shims (Intro)
        - Shimming for Post Exploitation(blog)
        - Demystifying Shims – or – Using the App Compat Toolkit to make your old stuff work with your new stuff
        - Post Exploitation Persistence With Application Shims (Intro)
        - Shim Database Talks
        - Using Application Compatibility Shims
    - **SQL Server**
        - Maintaining Persistence via SQL Server – Part 1: Startup Stored Procedures - NETSPI
    - **Startup**
        - Windows Startup Application Database
        - SYSTEM Context Persistence in GPO Startup Scripts

- **Windows Instrumentation Management**
  - Abusing Windows Management Instrumentation (WMI) to Build a Persistent, Asyncronous, and Fileless Backdoor
- **WPAD**
  - WPAD Persistence
- **Miscellaneous**
  - backdoorme
    - Tools like metasploit are great for exploiting computers, but what happens after you've gained access to a computer? Backdoorme answers that question by unleashing a slew of backdoors to establish persistence over long periods of time. Once an SSH connection has been established with the target, Backdoorme's strengths can come to fruition. Unfortunately, Backdoorme is not a tool to gain root access - only keep that access once it has been gained.
  - Windows Program Automatic Startup Locations(2004) BleepingComputer

---

Linux Persistence

OS X Persistence

- **OS X Persistence**
  - Methods Of Malware Persistence On Mac OS X
  - What's the easiest way to have a script run at boot time in OS X? - Stack Overflow
  - Userland Persistence On Mac Os X "It Just Works" - Shmoocon 2015
    - Got root on OSX? Do you want to persist between reboots and have access whenever you need it? You do not need plists, new binaries, scripts, or other easily noticeable techniques. Kext programming and kernel patching can be troublesome! Leverage already running daemon processes to guarantee your access. As the

presentation will show, if given userland administrative access (read: root), how easy it is to persist between reboots without plists, non-native binaries, scripting, and kexts or kernel patching using the Backdoor Factory.

- Using email for persistence on OS X - n00py

Pivoting and Lateral movement:

- **Lateral Movement Techniques**
  - Lateral movement using excel application and dcom
  - **Pass-The-Hash**
    - PsExec and the Nasty Things It Can Do
      - An overview of what PsExec is and what its capabilities are from an administrative standpoint.
    - smbexec
      - A rapid psexec style attack with samba tools
    - Blogpost that inspired it
    - pth-toolkit I.e Portable pass the hash toolkit
      - A modified version of the passing-the-hash tool collection https://code.google.com/p/passing-the-hash/ designed to be portable and work straight out of the box even on the most 'bare bones' systems
    - Pass-the-Hash is Dead: Long Live Pass-the-Hash
    - Still Passing the Hash 15 Years Later: Using Keys to the Kingdom to Access Data - BH 2012
    - Still Passing the Hash 15 Years Later
    - The Evolution of Protected Processes Part 1: Pass-the-Hash Mitigations in Windows 8.1
    - Et tu Kerberos - Christopher Campbell
      - For over a decade we have been told that Kerberos is the answer to Microsoft’s authentication woes and now we know that isn’t the case. The problems with LM and NTLM are widely known- but the problems with Kerberos have only recently surfaced. In this talk we will look back at previous failures in order to look

forward. We will take a look at what recent problems in Kerberos mean to your enterprise and ways you could possibly mitigate them. Attacks such as Spoofed-PAC- Pass-the-Hash- Golden Ticket- Pass-the-Ticket and Over-Pass-the-Ticket will be explained. Unfortunately- we don't really know what is next – only that what we have now is broken.

- Battle Of SKM And IUM How Windows 10 Rewrites OS Architecture - Alex Ionescu - BHUSA2015
  - Slides
- **Password Spraying**
  - **Linux**
    - Raining shells on Linux environments with Hwacha
    - Hwacha
      - Hwacha is a tool to quickly execute payloads on `*` Nix based systems. Easily collect artifacts or execute shellcode on an entire subnet of systems for which credentials are obtained.
  - **Windows**
    - Use PowerShell to Get Account Lockout and Password Policy
    - DomainPasswordSpray
      - DomainPasswordSpray is a tool written in PowerShell to perform a password spray attack against users of a domain. By default it will automatically generate the userlist from the domain. DomainPasswordSpray is a tool written in PowerShell to perform a password spray attack against users of a domain. By default it will automatically generate the userlist from the domain.
    - NTLM - Open-source script from root9B for manipulating NTLM authentication
      - This script tests a single hash or file of hashes against an ntlmv2 challenge/response e.g. from auxiliary/server/capture/smb The idea is that you can identify re-used passwords between accounts that you do have the hash for and accounts that you do not have the hash for, offline and without cracking the password hashes. This saves you from trying your hashes against other accounts live, which triggers lockouts and alerts.
    - CredNinja

        - A multithreaded tool designed to identify if credentials are valid, invalid, or local admin valid credentials within a network at-scale via SMB, plus now with a user hunter.

- **Pivoting**
    - **Articles**
        - [More on Using Bash's Built-in /dev/tcp File (TCP/IP)](http://www.linuxjournal.com/content/more-using-bashs-built-devtcp-file-tcpip More on Using Bash's Built-in /dev/tcp File (TCP/IP))
        - The Grammar of WMIC
        - Authenticated Remote Code Execution Methods in Windows
        - SOCKS: A protocol for TCP proxy across firewalls
        - A Red Teamer's guide to pivoting
        - Pivoting Ssh Reverse Tunnel Gateway
        - Pivoting into a network using PLINK and FPipe
        - Portfwd - Pivot from within meterpreter
        - SSH Gymnastics and Tunneling with ProxyChains
        - SSH Cheat Sheet - pentestmonkey
        - Reverse SSL backdoor with socat and metasploit (and proxies)
        - How VPN Pivoting Works (with Source Code) - cs
        - Universal TUN/TAP device driver. - kernel.org
        - Tun/Tap interface tutorial - backreference
        - Pillage the Village Redux w/ Ed Skoudis & John Strand - SANS
        - Decrypting IIS Passwords to Break Out of the DMZ
            - Decrypting IIS Passwords to Break Out of the DMZ: Part 1
            - Decrypting IIS Passwords to Break Out of the DMZ: Part 2
    - **Tools**
        - Socat

        - socat is a relay for bidirectional data transfer between two independent data channels. Each of these data channels may be a file, pipe, device (serial line etc. or a pseudo terminal), a socket (UNIX, IP4, IP6 - raw, UDP, TCP), an SSL socket, proxy CONNECT connection, a file descriptor (stdin etc.), the GNU line editor (readline), a program, or a combination of two of these. These modes include generation of "listening" sockets, named pipes, and pseudo terminals.
        - Examples of use
        - Socat Cheatsheet
- **Discovery**
    - nextnet
        - nextnet is a pivot point discovery tool written in Go.
- **HTTP/HTTPS**
    - SharpSocks
        - Tunnellable HTTP/HTTPS socks4a proxy written in C# and deployable via PowerShell
- **Named Pipes**
    - Piper
        - Creates a local or remote port forwarding through named pipes.
- **PowerShell**
    - PowerShellDSCLateralMovement.ps1
- **SMB**
    - Invoke-Piper
        - Forward local or remote tcp ports through SMB pipes.
- **SSH**
    - SSHDog
        - SSHDog is your go-anywhere lightweight SSH server. Written in Go, it aims to be a portable SSH server that you can drop on a system and use for remote access without any additional configuration.
    - MeterSSH

        - MeterSSH is a way to take shellcode, inject it into memory then tunnel whatever port you want to over SSH to mask any type of communications as a normal SSH connection. The way it works is by injecting shellcode into memory, then wrapping a port spawned (meterpeter in this case) by the shellcode over SSH back to the attackers machine. Then connecting with meterpreter's listener to localhost will communicate through the SSH proxy, to the victim through the SSH tunnel. All communications are relayed through the SSH tunnel and not through the network.
- **Sockets/TCP/UDP**
    - shootback
        - shootback is a reverse TCP tunnel let you access target behind NAT or firewall
    - ssf - Secure Socket Funneling
        - Network tool and toolkit. It provides simple and efficient ways to forward data from multiple sockets (TCP or UDP) through a single secure TLS tunnel to a remote computer. SSF is cross platform (Windows, Linux, OSX) and comes as standalone executables.
    - PowerCat
        - A PowerShell TCP/IP swiss army knife that works with Netcat & Ncat
    - Udp2raw-tunnel
        - A Tunnel which tunnels UDP via FakeTCP/UDP/ICMP Traffic by using Raw Socket, helps you Bypass UDP FireWalls(or Unstable UDP Environment). Its Encrypted, Anti-Replay and Multiplexed. It also acts as a Connection Stabilizer.)
    - reGeorg
        - The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn.
    - redsocks – transparent TCP-to-proxy redirector
        - This tool allows you to redirect any TCP connection to SOCKS or HTTPS proxy using your firewall, so redirection may be system-wide or network-wide.
    - Tunna

        - Tunna is a set of tools which will wrap and tunnel any TCP communication over HTTP. It can be used to bypass network restrictions in fully firewalled environments.
    - **VNC**
        - Invoke-Vnc
            - Invoke-Vnc executes a VNC agent in-memory and initiates a reverse connection, or binds to a specified port. Password authentication is supported.
        - jsmpeg-vnc
            - A low latency, high framerate screen sharing server for Windows and client for browsers

---

Avoiding/Bypassing AV(Anti-Virus)/UAC/Whitelisting/Sandboxes/etc

- **101**
    - Noob 101: Practical Techniques for AV Bypass - Jared Hoffman - ANYCON 2017
        - The shortcomings of anti-virus (AV) solutions have been well known for some time. Nevertheless, both public and private organizations continue to rely on AV software as a critical component of their information security programs, acting as a key protection mechanism over endpoints and other information systems within their networks. As a result, the security posture of these organizations is significantly jeopardized by relying only on this weakened control.
- **Educational**
    - Learn how to hide your trojans, backdoors, etc from anti virus.
    - Easy Ways To Bypass Anti-Virus Systems - Attila Marosi -Trooper14
    - Muts Bypassing AV in Vista/Pissing all over your AV
        - presentation, listed here as it was a bitch finding a live copy
    - How to Bypass Anti-Virus to Run Mimikatz - **Spoiler, AV still suck, changing strings is helpful**
    - AMSI: How Windows 10 Plans to Stop Script-Based Attacks and How Well It Does It - labofapenetrationtester
- **Articles/Blogposts/Presentations/Talks/Writeups**

- Bypass Cylance Memory Exploitation Defense & Script Cntrl
- Three Simple Disguises for Evading Antivirus - BHIS
- AVLeak: Fingerprinting Antivirus Emulators Through Black-Box Testing
- Adventures in Asymmetric Warfare by Will Schroeder
  - As a co-founder and principal developer of the Veil-Framework, the speaker has spent a considerable amount of time over the past year and a half researching AV-evasion techniques. This talk will briefly cover the problem space of antivirus detection, as well as the reaction to the initial release of Veil-Evasion, a tool for generating AV-evading executables that implements much of the speaker's research. We will trace through the evolution of the obfuscation techniques utilized by Veil-Evasion's generation methods, culminating in the release of an entirely new payload language class, as well as the release of a new ..NET encryptor. The talk will conclude with some basic static analysis of several Veil-Evasion payload families, showing once and for all that antivirus static signature detection is dead.
- How to Accidently Win Against AV - RastaMouse
- EDR, ETDR, Next Gen AV is all the rage, so why am I enraged? - Michael Gough - Derbycon7
  - A funny thing happened when I evaluated several EDR, ETDR and Next Gen AV products, currently all the rage and latest must have security solution. Surprisingly to me the solutions kinda sucked at things we expected them to do or be better at, thus this talk so you can learn from our efforts. While testing, flaws were discovered and shared with the vendors, some of the flaws, bugs, or vulns that were discovered will be discussed. This talk takes a look at what we initially expected the solutions to provide us, the options or categories of what these solutions address, what to consider when doing an evaluation, how to go about testing these solutions, how they would fit into our process, and what we found while testing these solutions. What enraged me about these EDR solutions were how they were all over the place in how they worked, how hard or ease of use of the solutions, and the fact I found malware that did not trigger an alert on every solution I tested. And this is the next new bright and shiny blinky security savior solution? The news is not all bad, there is hope if you do some work to understand what these solutions target and provide, what to look for, and most importantly how to test them! What we never anticipated or expected is the tool we used to compare the tests and how well it worked and how it can help you.

    - Learn how to hide your trojans, backdoors, etc from anti virus.
    - [Virus] Self-modifying code-short overview for beginners
    - Escaping The Avast Sandbox Using A Single IOCTL
    - AVLeak: Fingerprinting Antivirus Emulators Through Black-Box Testing
- **Techniques**
    - **Code Injection**
    - **Debuggers**
        - Batch, attach and patch: using windbg's local kernel debugger to execute code in windows kernel
            - In this article I am going to describe a way to execute code in windows kernel by using windbg local kernel debugging. It's not a vulnerability, I am going to use only windbg's legal functionality, and I am going to use only a batch file (not powershell, or vbs, an old style batch only) and some Microsoft's signed executables (some of them that are already in the system and windbg, that we will be dumped from the batch file). With this method it is not necessary to launch executables at user mode (only Microsoft signed executables) or load signed drivers. PatchGuard and other protections don't stop us. We put our code directly into kernel memory space and we hook some point to get a thread executing it. As we will demonstrate, a malware consisting of a simple batch file would be able to jump to kernel, enabling local kernel debugging and using windbg to get its code being executed in kernel.
    - **DLL Fun**
        - MemoryModule
            - MemoryModule is a library that can be used to load a DLL completely from memory - without storing on the disk first.
    - **Native Binaries/Functionality**
        - Research on CMSTP.exe
            - Methods to bypass UAC and load a DLL over webdav
        - rundll32 lockdown testing goodness
        - Hack Microsoft Using Microsoft Signed Binaries - Pierre-Alexandre Braeken

        - Hack Microsoft Using Microsoft Signed Binaries - BH17 - pierre - alexandre braeken
            - Imagine being attacked by legitimate software tools that cannot be detected by usual defender tools. How bad could it be to be attacked by malicious threat actors only sending bytes to be read and bytes to be written in order to achieve advanced attacks? The most dangerous threat is the one you can't see. At a time when it is not obvious to detect memory attacks using API like VirtualAlloc, what would be worse than having to detect something like `f0xffffe0010c79ebe8+0x8 L4 0xe8 0xcb 0x04 0x10`? We will be able to demonstrate that we can achieve every kind of attacks you can imagine using only PowerShell and a Microsoft Signed Debugger. We can retrieve passwords from the userland memory, execute shellcode by dynamically parsing loaded PE or attack the kernel achieving advanced persistence inside any system.
        - RogueMMC
            - Execute Shellcode And Other Goodies From MMC
- **Bypassing UAC**
    - Bypassing UAC on Windows 10 using Disk Cleanup
    - Research on CMSTP.exe
        - Methods to bypass UAC and load a DLL over webdav
    - "Fileless" UAC Bypass Using eventvwr.exe and Registry Hijacking
    - Bypassing UAC using App Paths
    - "Fileless" UAC Bypass Using eventvwr.exe and Registry Hijacking
    - Bypass-UAC
    - Reading Your Way Around UAC (Part 1)
        - Reading Your Way Around UAC (Part 2)
        - Reading Your Way Around UAC (Part 3)
    - Fileless UAC Bypass using sdclt
    - Eventvwr File-less UAC Bypass CNA
    - Testing User Account Control (UAC) on Windows 10 - Ernesto Fernández Provecho
    - DccwBypassUAC

        - This exploit abuses the way "WinSxS" is managed by "dccw.exe" by means of a derivative Leo's Davidson "Bypass UAC" method so as to obtain an administrator shell without prompting for consent. It supports "x86" and "x64" architectures. Moreover, it has been successfully tested on Windows 8.1 9600, Windows 10 14393, Windows 10 15031 and Windows 10 15062.

- **Anti-Virus**
    - **Articles**
        - How to Bypass Anti-Virus to Run Mimikatz
        - pecloak.py - An Experiment in AV evasion
        - Practical Anti-virus Evasion - Daniel Sauder
        - Why Anti-Virus Software Fails
        - avepoc
            - some pocs for antivirus evasion
        - Sacred Cash Cow Tipping 2017 - BlackHills Infosec
            - We're going to bypass most of the major antivirus programs. Why? 1) Because it's fun. 2) Because it'll highlight some of the inherent weaknesses in our environments today.
        - Deep Dive Into Stageless Meterpreter Payloads
        - Execute ShellCode Using Python
            - In this article I am going to show you, how can we use python and its "ctypes" library to execute a "calc.exe" shell code or any other shell code.
    - **Bypassing**
        - Execute ShellCode Using Python
            - In this article I am going to show you, how can we use python and its "ctypes" library to execute a "calc.exe" shell code or any other shell code.
        - In-Memory Managed Dll Loading With PowerShell - 2012
        - Generic bypass of next-gen intrusion / threat / breach detection systems

        - The focus of this blog post is to bypass network monitoring tools, e.g. good-old IDS or next-generation threat detection systems in a generic way. The focus is on the exploit delivery.
    - Meterpreter stage AV/IDS evasion with powershell
    - Customising Meterpreter Loader DLL part. 2
    - Facts and myths about antivirus evasion with Metasploit - mihi - 2011
        - This article tries to given an overview about the current executable generation scheme of Metasploit, how AV detects them, and how to evade them. Note that this document only covers standalone EXE files (for Windows) that replace an EXE template's functionality, and not other payloads for exploits, service executables (like for the windows/psexec exploit) or executables that merely add to the original template's functionality (like the -k option of msfpayload).
- **Tools**
    - AVSignSeek
        - Tool written in python3 to determine where the AV signature is located in a binary/payload
    - SpookFlare: Stay In Shadows
        - SpookFlare - Github
    - avet framework
        - AVET is an AntiVirus Evasion Tool, which was developed for making life easier for pentesters and for experimenting with antivirus evasion techniques. In version 1.1 lot of stuff was introduced, for a complete overview have a look at the CHANGELOG file. Now 64bit payloads can also be used, for easier usage I hacked a small build tool (avet_fabric.py).
    - Don't Kill My Cat (DKMC)
        - Don't kill my cat is a tool that generates obfuscated shellcode that is stored inside of polyglot images. The image is 100% valid and also 100% valid shellcode. The idea is to avoid sandbox analysis since it's a simple "legit" image. For now the tool rely on PowerShell the execute the final shellcode payload.
        - Presentation - Northsec2017
    - Dr0p1t-Framework

    - Have you ever heard about trojan droppers ? In short dropper is type of trojans that downloads other malwares and Dr0p1t gives you the chance to create a stealthy dropper that bypass most AVs and have a lot of tricks (Trust me :D) ;)
- PowerLine
    - Presentation
- Invoke-CradleCrafter: Moar PowerShell obFUsk8tion by Daniel Bohannon
- Invoke-CradleCrafter v1.1
- wePWNise
    - WePWNise generates architecture independent VBA code to be used in Office documents or templates and automates bypassing application control and exploit mitigation software
- katz.xml
    - Downloads Mimikatz From GitHub, Executes Inside of MsBuild.exe
- Shellter
- SigThief
    - Stealing Signatures and Making One Invalid Signature at a Time
- SideStep
    - SideStep is yet another tool to bypass anti-virus software. The tool generates Metasploit payloads encrypted using the CryptoPP library (license included), and uses several other techniques to evade AV.
- peCloak.py - An Experiment in AV Evasion
- Making FinFisher Undetectable
- Bypass AV through several basic/effective techniques
- stupid_malware
    - Python malware for pentesters that bypasses most antivirus (signature and heuristics) and IPS using sheer stupidity
- InfectPE
    - Using this tool you can inject x-code/shellcode into PE file. InjectPE works only with 32-bit executable files.

        - MorphAES
            - IDPS & SandBox & AntiVirus STEALTH KILLER. MorphAES is the world's first polymorphic shellcode engine, with metamorphic properties and capability to bypass sandboxes, which makes it undetectable for an IDPS, it's cross-platform as well and library-independent.
- **Application Whitelisting**
    - Whitelist Evasion revisited
    - Shackles, Shims, and Shivs - Understanding Bypass Techniques
    - $@|sh – Or: Getting a shell environment from Runtime.exec
    - WSH Injection: A Case Study - enigma0x3
    - **Bypasses**
        - Bypass Application Whitelisting Script Protections - Regsvr32.exe & COM Scriptlets (.sct files)
        - Application Whitelist Bypass Techniques
            - A Catalog of Application Whitelisting Bypass Techniques - SubTee
        - Bypassing Application Whitelisting by using WinDbg/CDB as a Shellcode Runner
        - MS Signed mimikatz in just 3 steps
        - BinariesThatDoesOtherStuff.txt - api0cradle
        - GreatSCT
            - The project is called Great SCT (Great Scott). Great SCT is an open source project to generate application white list bypasses. This tool is intended for BOTH red and blue team.
        - RunMe.c
            - Trick to run arbitrary command when code execution policy is enforced (i.e. AppLocker or equivalent). Works on Win98 (lol) and up - tested on 7/8
        - Window Signed Binary
    - **Talks**
        - Modern Evasion Techniques Jason Lang - Derbycon7

        - Whitelisting Evasion - subTee - Shmoocon 2015
    - **Applocker**
        - AppLocker Case study: How insecure is it really? Part 1 oddvar.moe
        - AppLocker Case study: How insecure is it really? Part 2](https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/)
        - Backdoor-Minimalist.sct
            - Applocker bypass
        - AppLocker Bypass – Weak Path Rules
        - Applocker Bypass via Registry Key Manipulation
- **DeviceGuard Bypass**
    - Window 10 Device Guard Bypass
    - Defeating Device Guard: A look into CVE-2017-0007
    - DeviceGuard Bypasses - James Forshaw
        - This solution contains some of my UMCI/Device Guard bypasses. They're are designed to allow you to analyze a system, such as Windows 10 S which comes pre-configured with a restrictive UMCI policy.
    - Consider Application Whitelisting with Device Guard
    - Bypassing Application Whitelisting using MSBuild.exe - Device guard Example and Mitigations
- **Secured Environment Escape**
    - Sandboxes from a pen tester’s view - Rahul Kashyap
        - Description: In this talk we’ll do an architectural decomposition of application sandboxing technology from a security perspective. We look at various popular sandboxes such as Google Chrome, Adobe ReaderX, Sandboxie amongst others and discuss the limitations of each technology and it’s implementation. Further, we discuss in depth with live exploits how to break out of each category of sandbox by leveraging various kernel and user mode exploits – something that future malware could leverage. Some of these exploit vectors have not been discussed widely and awareness is important.
    - Windows Desktop Breakout

- Kiosk/POS Breakout Keys in Windows - TrustedSec
- Breaking out of secured Python environments
- **chroot**
  - chw00t: chroot escape tool
  - Breaking Out of a Chroot Jail Using PERL
- **Breaking out of Contained Linux Shells**
  - Escaping Restricted Linux Shells - SANS
  - Breaking out of rbash using scp - pentestmonkey
  - Escape From SHELLcatraz - Breaking Out of Restricted Unix Shells - knaps
- **ssh**
  - ssh environment - circumvention of restricted shells
- **Adobe Sandbox**
  - Adobe Sandbox: When the Broker is Broken - Peter Vreugdenhill
- **Python Sandbox**
  - Escaping a Python sandbox with a memory corruption bug
  - Breaking out of secured Python environments
  - Sandboxed Execution Environment
  - Documentation
    - Sandboxed Execution Environment (SEE) is a framework for building test automation in secured Environments. The Sandboxes, provided via libvirt, are customizable allowing high degree of flexibility. Different type of Hypervisors (Qemu, VirtualBox, LXC) can be employed to run the Test Environments.
  - Usermode Sandboxing
- **Citrix/Terminal Services**
  - Breaking Out! of Applications Deployed via Terminal Services, Citrix, and Kiosks
  - Breaking Out of Citrix and other Restricted Desktop Environments

- **Virtualbox**
  - VirtualBox Detection Via WQL Queries
  - Bypassing VirtualBox Process Hardening on Windows
  - VBoxHardenedLoader
    - VirtualBox VM detection mitigation loader

Payloads/Creating Custom Payloads/Etc.

- **Generation**
  - How to use msfvenom
  - msfpc
    - A quick way to generate various "basic" Meterpreter payloads via msfvenom (part of the Metasploit framework).
  - MorphAES
    - MorphAES is the world's first polymorphic shellcode engine, with metamorphic properties and capability to bypass sandboxes, which makes it undetectable for an IDPS, it's cross-platform as well and library-independent.
  - SharpShooter
    - SharpShooter is a payload creation framework for the retrieval and execution of arbitrary CSharp source code. SharpShooter is capable of creating payloads in a variety of formats, including HTA, JS, VBS and WSF. It leverages James Forshaw's DotNetToJavaScript tool to invoke methods from the SharpShooter DotNet serialised object. Payloads can be retrieved using Web or DNS delivery or both; SharpShooter is compatible with the MDSec ActiveBreach PowerDNS project. Alternatively, stageless payloads with embedded shellcode execution can also be generated for the same scripting formats.
- **Go**
  - Hershell

        - Simple TCP reverse shell written in Go. It uses TLS to secure the communications, and provide a certificate public key fingerprint pinning feature, preventing from traffic interception.
        - [EN] Golang for pentests : Hershell
- **HTA**
    - genHTA
        - Generates anti-sandbox analysis HTA files without payloads
    - morpHTA
        - Morphing Cobalt Strike's evil.HTA
    - Demiguise
        - The aim of this project is to generate .html files that contain an encrypted HTA file. The idea is that when your target visits the page, the key is fetched and the HTA is decrypted dynamically within the browser and pushed directly to the user. This is an evasion technique to get round content / file-type inspection implemented by some security-appliances. This tool is not designed to create awesome HTA content. There are many other tools/techniques that can help you with that. What it might help you with is getting your HTA into an environment in the first place, and (if you use environmental keying) to avoid it being sandboxed.
- **Keying**
    - GoGreen
        - This project was created to bring environmental (and HTTP) keying to scripting languages. As its common place to use PowerShell/JScript/VBScript as an initial vector of code execution, as a result of phishing or lateral movement, I see value of the techniques for these languages.
- **LNK Files**
    - LNKUp
        - Generates malicious LNK file payloads for data exfiltration
    - Embedding reverse shell in .lnk file or Old horse attacks
- **MSI Binaries**
    - Wix Toolkit

        - Tool for crafting msi binaries
- **.NET**
    - DotNetToJScript
        - A tool to create a JScript file which loads a .NET v2 assembly from memory.
    - Payload Generation with CACTUSTORCH
        - Code
- **Powershell**
    - Invoke-PSImage
        - Invoke-PSImage takes a PowerShell script and embeds the bytes of the script into the pixels of a PNG image. It generates a oneliner for executing either from a file of from the web (when the -Web flag is passed). The least significant 4 bits of 2 color values in each pixel are used to hold the payload. Image quality will suffer as a result, but it still looks decent. The image is saved as a PNG, and can be losslessly compressed without affecting the ability to execute the payload as the data is stored in the colors themselves. It can accept most image types as input, but output will always be a PNG because it needs to be lossless. Each pixel of the image is used to hold one byte of script, so you will need an image with at least as many pixels as bytes in your script. This is fairly easy—for example, Invoke-Mimikatz fits into a 1920x1200 image.
- **Python**
    - Pupy
        - Pupy is a remote administration tool with an embeded Python interpreter, allowing its modules to load python packages from memory and transparently access remote python objects. The payload is a reflective DLL and leaves no trace on disk
    - Winpayloads
        - Undetectable Windows Payload Generation with extras Running on Python2.7
    - Cloak
        - Cloak generates a python payload via msfvenom and then intelligently injects it into the python script you specify.
- **SCT Files**

    - SCT-obfuscator
        - SCT payload obfuscator. Rename variables and change harcoded char value to random one.
- **VBA**
    - VBad
        - VBad is fully customizable VBA Obfuscation Tool combined with an MS Office document generator. It aims to help Red & Blue team for attack or defense.
- **Polyglot**
    - BMP / x86 Polyglot

Kerberos Related

- **General**
    - Attacking Microsoft Kerberos: Kicking the Guard Dog of Hades
        - Kerberos- besides having three heads and guarding the gates of hell- protects services on Microsoft Windows Domains. Its use is increasing due to the growing number of attacks targeting NTLM authentication. Attacking Kerberos to access Windows resources represents the next generation of attacks on Windows authentication.In this talk Tim will discuss his research on new attacks against Kerberos- including a way to attack the credentials of a remote service without sending traffic to the service as well as rewriting tickets to access systems.He will also examine potential countermeasures against Kerberos attacks with suggestions for mitigating the most common weaknesses in Windows Kerberos deployments.
    - Et tu - Kerberos?
        - For over a decade we have been told that Kerberos is the answer to Microsoft’s authentication woes and now we know that isn’t the case. The problems with LM and NTLM are widely known- but the problems with Kerberos have only recently surfaced. In this talk we will look back at previous failures in order to look forward. We will take a look at what recent problems in Kerberos mean to your enterprise and ways you could possibly mitigate them. Attacks such as Spoofed-PAC- Pass-the-Hash- Golden Ticket- Pass-the-Ticket and Over-Pass-

the-Ticket will be explained. Unfortunately- we don't really know what is next – only that what we have now is broken.
    - Abusing Kerberos
- **Tools**
    - PyKEK
        - PyKEK (Python Kerberos Exploitation Kit), a python library to manipulate KRB5-related data. (Still in development)`
    - Kerberom
        - Kerberom is a tool aimed to retrieve ARC4-HMAC'ed encrypted Tickets Granting Service (TGS) of accounts having a Service Principal Name (SPN) within an Active Directory

---

Docker & Containers

- **Articles/Blogposts/Writeups**
    - Is it possible to escalate privileges and escaping from a Docker container? - StackOverflow
    - The Dangers of Docker.sock
    - Abusing Privileged and Unprivileged Linux Containers - nccgroup
    - Understanding and Hardening Linux Containers - nccgroup
        - Operating System virtualisation is an attractive feature foThis project provides a command line tool called nms that recreates the famous data decryption effect seen on screen in the 1992 hacker movie Sneakers. For reference, you can see this effect at 0:35 in this movie clip.r efficiency, speed and modern application deployment, amid questionable security. Recent advancements of the Linux kernel have coalesced for simple yet powerful OS virtualisation via Linux Containers, as implemented by LXC, Docker, and CoreOS Rkt among others. Recent container focused start-ups such as Docker have helped push containers into the limelight. Linux containers offer native OS virtualisation, segmented by kernel namespaces, limited through process

cgroups and restricted through reduced root capabilities, Mandatory Access Control and user namespaces. This paper discusses these container features, as well as exploring various security mechanisms. Also included is an examination of attack surfaces, threats, and related hardening features in order to properly evaluate container security. Finally, this paper contrasts different container defaults and enumerates strong security recommendations to counter deployment weaknesses-- helping support and explain methods for building high-security Linux containers. Are Linux containers the future or merely a fad or fantasy? This paper attempts to answer that question.

    - docker-layer2-icc
        - Demonstrating that disabling ICC in docker does not block raw packets between containers.

- **Tools**

    - **Docker**
        - docker-bench-security
            - The Docker Bench for Security is a script that checks for dozens of common best-practices around deploying Docker containers in production.
        - Vulnerable Docker VM
            - For practicing pen testing docker instances
    - **Kubernetes**
    - **Agnostic**
        - nsjail
            - A light-weight process isolation tool, making use of Linux namespaces and seccomp-bpf syscall filters (with help of the kafel bpf language)

- **Talks/Videos**

    - Docker: Security Myths, Security Legends - Rory McCune

Code Injection

- injectAllTheThings
  - Single Visual Studio project implementing multiple DLL injection techniques (actually 7 different techniques) that work both for 32 and 64 bits. Each technique has its own source code file to make it easy way to read and understand.
- Inject All the Things - Shut up and hack
  - Accompanying above project
- PowerLoaderEX
- Injection on Steroids: Code-less Code Injections and 0-Day Techniques
- Injection on Steroids: Code less Code Injections and 0 Day Techniques - Paul Schofield Udi Yavo
- InfectPE
  - Using this tool you can inject x-code/shellcode into PE file. InjectPE works only with 32-bit executable files.
- InjectProc - Process Injection Techniques
- PowerLoaderEX
  - Advanced Code Injection Technique for x32 / x64
- pyrasite
  - Tools for injecting arbitrary code into running Python processes.
- Less is More, Exploring Code/Process-less Techniques and Other Weird Machine Methods to Hide Code (and How to Detect Them)
- Equip: python bytecode instrumentation
  - equip is a small library that helps with Python bytecode instrumentation. Its API is designed to be small and flexible to enable a wide range of possible instrumentations. The instrumentation is designed around the injection of bytecode inside the bytecode of the program to be instrumented. However, the developer does not need to know anything about the Python bytecode since the injected code is Python source.
- Jugaad - Thread Injection Kit

    - Jugaad is an attempt to create CreateRemoteThread() equivalent for `*nix` platform. The current version supports only Linux operating system. For details on what is the methodology behind jugaad and how things work under the hood visit http://null.co.in/section/projects for a detailed paper.
- linux-injector
    - Utility for injecting executable code into a running process on x86/x64 Linux. It uses ptrace() to attach to a process, then mmap()'s memory regions for the injected code, a new stack, and space for trampoline shellcode. Finally, the trampoline in the target process is used to create a new thread and execute the chosen shellcode, so the main thread is allowed to continue. This project borrows from a number of other projects and research, see References below.
- linux-inject
    - Tool for injecting a shared object into a Linux process
- injectso64
    - This is the x86-64 rewrite of Shaun Clowes' i386/SPARC injectso which he presented at Blackhat Europe 2001.

Papers

- Adapting Software Fault Isolation to Contemporary CPU Architectures
    - Adapting Software Fault Isolation to Contemporary CPU ArchitecturesSoftware Fault Isolation (SFI) is an effective approach to sandboxing binary code of questionable provenance, an interesting use case for native plugins in a Web browser. We present software fault isolation schemes for ARM and x86-64 that provide control-flow and memory integrity with average performance overhead of under 5% on ARM and 7% on x86-64. We believe these are the best known SFI implementations for these architectures, with significantly lower overhead than previous systems for similar architectures. Our experience suggests that these SFI implementations benefit from instruction-level parallelism, and have particularly small impact for work- loads that are data memory-bound, both properties that tend to reduce the impact of our SFI systems for future CPU implementations.] (https://static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/35649.pdf)

- NaCl SFI model on x86-64 systems
  - This document addresses the details of the Software Fault Isolation (SFI) model for executable code that can be run in Native Client on an x86-64 system