25 JUNE 2018 / BLUETEAM

Blue Team Tips

From a recent conversation between friends (red/blue teamers) - What are the best recommendations to a completely vulnerable, easily pwnable network? Where do you start? What tools? What logging? etc. Which has turned into a list of tips. Some of these are easier then others.

1. Basic Network Diagram

Understand what you have. A **Good Basic Network Diagram** including ingress / egress points across all sites - do a physical site survey if you must. As stated in the Applied Network Security, be sure to include:

- The high-level logical overview of the network.
- All routing devices, proxies, or gateways that affect the flow of traffic.
- External/Internal IP addresses of routing devices, proxies, and gateways.
- Workstations, servers or other devices -- these should be displayed in groupings and not individually, unless they are particularly critical devices.
- IP address ranges for workstation, server, and device groupings.

Use internal/external network scanning via NMAP (or others) will help highlight your attack surface and what is on your network. Keep painting that picture and KEEP IT UPTO DATE!

2. Control Your Local Administrator Account

Deploy Microsoft LAPS - Microsoft's official "Local Administrator Password Solution". Enterprises in the past have had one global Local Administrator password across all of their endpoints, if this was compromised at any stage lateral movement is incredibly easy. LAPS will create a unique Administrator password for each endpoint which is securely stored and managed in Active Directory. It requires agent installation and GPO creation. See my blog "Blue Team Basics - Local Admin Password Administration" post for an overview.

---

3. Gain Visibility Into PowerShell Execution

Enable Advanced PowerShell Logging - You need this to help gain visibility when it

executes in your environment, watch No Easy Breach to explain why. PowerShell has gained a tremendous amount of popularity among attackers. Some of those attack frameworks are: PowerSploit, Empire, Nishang, PoshC2 etc. Quite a few APT groups are using such frameworks to hinder attribution.

You need at least version 5 of PowerShell installed that will enable you to use the logging features. Enabling this provides PowerShell module logging, scriptblock logging (input/output of commands) and automatic suspicious script detection. It also deobfuscates encoded PowerShell commands. If you don't know what this is check out Invoke-Obfuscation by Daniel Bohannon @danielhbohannon.

Windows 7 comes with PowerShell version 2 and Windows 10 comes with version 5 but with logging disabled. Watch out for adversary tactics to downgrade PowerShell to bypass detection. Detect downgrade attacks, the “Windows PowerShell” classic event log has event ID 400. This is the “Engine Lifecycle” event, and includes the Engine Version. Or, simply remove PowerShell v2 `Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root`. Once again proven that PowerShell logging isn't perfect.

MDSec
@MDSecLabs

New blog post on Exploring PowerShell AMSI and Logging evasion by @_xpn_ mdsec.co.uk/2018/06/explor…

♡ 134 1:25 PM - Jun 18, 2018

68 people are talking about this

More information on installation Step-by-Step see Greater Visibility Through PowerShell Logging Note: you can install WMF v5.1 straight onto Windows 7 without the need for WMFv4 as a intermediary.

4. Easily Track Process Creation

Enable Advance Event Logging / Process Creation - Following on from the above, for everything else, Process Execution is key for anything malicious infecting or running on your system. Process Creation logging a.k.a Event ID 4688 can be enabled via Group Policy. There is a 60 / 40 split where the noise this generates is quite high so there is some filtering post ingestion as it will capture everything being executed. One thing to be aware, logging might capture command line passwords as submitted arguments and thus available to attackers who are looking through the Event Logs!

> *A review of @MITREattack data sources shows me that*
> *Process Command Line Parameter*
> *as a data source,*
> *might help you detect 82/219 Techniques....*
> *Not sure where to start hunting?*
> *Maybe start looking at Command Line Events.https://t.co/ZFQw7PWg7i*
> *Also:https://t.co/CdoeUQASww*
>
> — Casey Smith (@subTee) May 11, 2018

5. Advanced System Logging with SysMon

Another popular option which is more customizable than the 4688 Process Creation, but requires much more planning, is to **Deploy Microsoft Sysinternals SysMon**. SysMon provides more

information about parent processes, can provide multiple types of file hashes including import function hashes (imphashes), describes network connections, loading of drivers or DLLs with their signatures and hashes, registry events (CREATE/DELETE/KEY VALUE RENAMES etc.) and WmiEvents (WmiEventFilter/Consuming activity) Are just a few features. SwiftOnSecurity's config is a good start but you must filter out noisy applications as Sysmon can be very verbose. A great paper from Crypsis Group on all things SysMon is probably one of the best reads on the subject. Also to note, research from Olaf on SysMon detections across the Mitre ATT&CK matrix.

Olaf Hartong
@olafhartong

@nader_shalabi love your Sysmon tooling! Inspired by Cyb3rward0g and Swift I created a fully modular config, mapped to MITRE ATT&CK github.com/olafhartong/sy… would be great if this was available in SysmonShell as well.

olafhartong/sysmon-modular

A repository of sysmon configuration modules. Contribute to olafhartong/sysmon-modular development by creating an account on GitHub.

github.com

♡ 16 10:30 PM - Jan 20, 2018

See Olaf Hartong's other Tweets

6. Start Visualising Active Directory

Find the attack path to Domain Admin with Bloodhound Released on-stage at DEF CON 24 as part of the Six Degrees of Domain Admin presentation by @_waldo @CptJesus @harmjoy Bloodhound is a tool the blue team can't afford not to use. If you have ever administered Active Directory you know how complicated and misconfigured it can get if not in the right hands. Someone said that the only people who can configure AD correctly is Microsoft themselves! :)

> *BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. Attacks 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*

To quickly get started you need to install the base Bloodhound framework which needs Java, neo4j and then the Bloohound application itself. Once you have that running, you will need to run one of the "ingestors" to pull the data out of Active Directory using Sharphound (C#) or the Invoke-BloodHound (PowerShell) tools. Once these have ran they will generate .csv files ready to be uploaded into the Bloodhound application.

Pre-built analytic queries include:

- Final all Domain Admins
- Find Shortest Paths to Domain Admin
- Find Top 10 Users with Most Sessions
- Find Top 10 Computers with Most Local Admin Rights
- Find Top 10 Computers with Most Admin
- Users with Foreign Domain Group Memebership

Still not convinced then look at Automating the Empire with the Death Star: getting Domain Admin with a push of a button

> *Ever since Empire and BloodHound, pentesting Active Directory has become pretty straight forward for 95% of the environments I get dropped in.*

> *straight forward for 95% of the environments I get dropped in*

Reversing roles on Bloodhound for a second, to detect this in your environment you will need to be monitoring LDAP TCP port 329 traffic between your endpoints and your Domain Controllers. A large set of queries would be very suspicious to this kind of activity.

---

7. Go On The Active Directory Defense

Harden Active Directory Probably the best resource for hardening is from adsecurity.org which is maintained by MVP / MCM Sean Metcalf @PyroTek3 - this guy knows his stuff. As a former Domain Admin I know how difficult it can be to keep on top of this but a few keys ones IMHO:

- **Implement fine grained password policy** in AD via GPO see [ADSecurity]. (https://adsecurity.org/?p=1684). You should have a complex password policy that is 8 or more characters containing alpha numeric including special characters as a base anyway. **Kerberoasting**! is a method to query Service Accounts via their SPNs (Service Principal Names) to access the hash for that Service Account which you can brute force offline. So force strong passwords, minimum of 25 characters for Service Accounts and minimize the rights you give these. Denying logon interactively for any account with an SPN set is also havily recommended.

- **Use a tiered segregation for administrative accounts** for servers and domain admins (for example SA_SMONKEY for Server Admin work and DA_SMONKEY for Domain Admin work) see this excellent guide to Tiered Security by Microsoft
- **Remove hardcoded credentials in SYSVOL Group Policy items**. Legacy scripts such as .bat and .vbs files etc. could contain credentials for a myriad of reasons (mapping drives, creating scheduled tasks). The newer way introduced in Windows Server 2008 is based on .xml files called "Group Policy Preferences" which can also contain credentials. Still a common place for attackers to quickly harvest credentials by simply searching through it for keyboard "CPassword" (clients cache GPP locally so look here too). Another is to use PowerSploit's Get-GPPPassword which can decrypt the AES stored credentials! There is a patch out KB2962486 to prevent this though, but it won't remove the old files/records! Check out Grouper.

> *Existing preferences that contain a password cannot be updated. They can only be deleted or disabled, as appropriate for the specific preference*

Areas that contained credentials:
* Drive Maps
* Local Users and Groups
* Scheduled Tasks
* Services

* Data Sources

- **Monitoring of admin group membership**. On the odd occasion you could use Bloodhound, but you will want something scheduled to constantly notify you of the changes. Scripts are avialable to help or simply write your own Domain Administrator

  Group poller. Another way is to configure Advanced Audit Policies to fire Event ID 4737 - A security-enabled global group was changed, when this action occurs but you must be logging the Security Event Logs to alert on it. Domain Administrators should never be more than 5 regardless of organisation size!

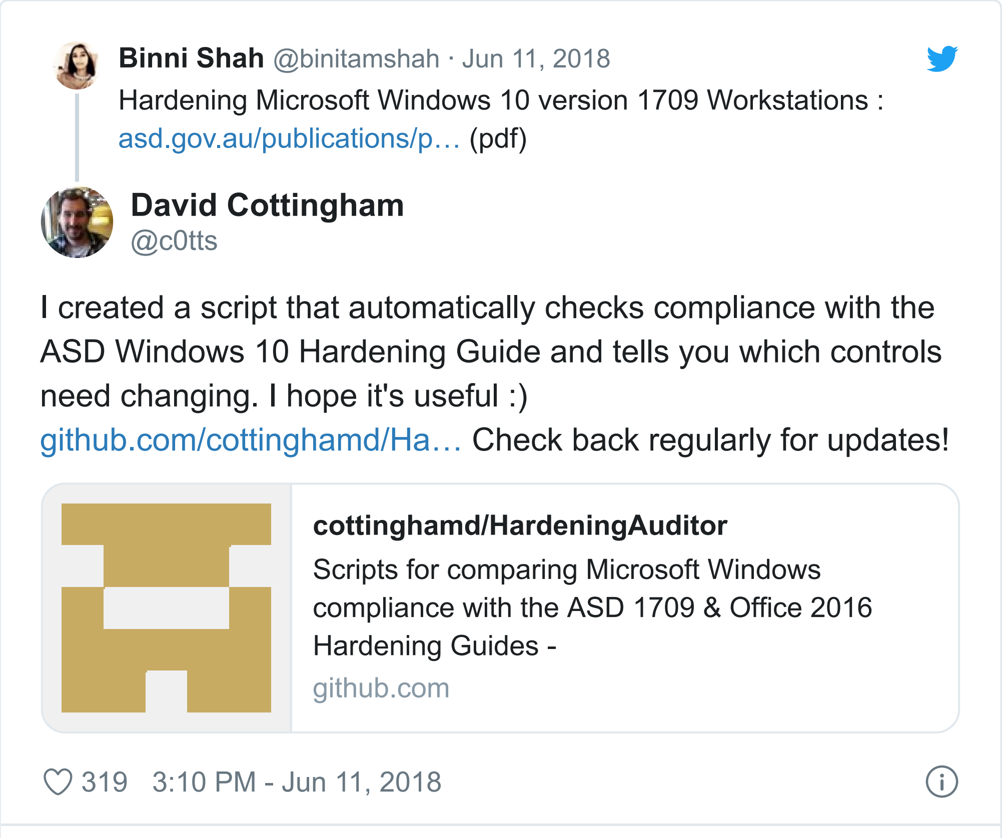
rumour has it that Microsoft have 3

- **Mimkatz DCSync** - If an endpoint user account has the right permission "replicating directory changes" via (Domain Admin / Enterprise Admin / Administrators and Domain Controller groups) they can synchronise/replicate a 'copy' of the entire domain, including account password hashes. For detection, the synchronisation traffic should only be allowed between DC sync partners. IDS sig from Sidier Stevens

```
alert tcp !$DC_SERVERS any -> $DC_SERVERS any (msg:"Mimikatz DRSUAPI"; flow:established,to_serve
alert tcp !$DC_SERVERS any -> $DC_SERVERS any (msg:"Mimikatz DRSUAPI DsGetNCChanges Request"; fl
```

8. Minimizing Your Attack Surface

Harden your endpoint Gold Images. To see where you stand - and there is a lot of configuration here to tackle, the ASD (Australian Signals Directorate) Cyber Security Centre have recently provided a great hardening guide.



Binni Shah @binitamshah · Jun 11, 2018
Hardening Microsoft Windows 10 version 1709 Workstations : asd.gov.au/publications/p… (pdf)

David Cottingham
@c0tts

I created a script that automatically checks compliance with the ASD Windows 10 Hardening Guide and tells you which controls need changing. I hope it's useful :) github.com/cottinghamd/Ha… Check back regularly for updates!

cottinghamd/HardeningAuditor
Scripts for comparing Microsoft Windows compliance with the ASD 1709 & Office 2016 Hardening Guides -
github.com

319 3:10 PM - Jun 11, 2018

157 people are talking about this

Audit first by running this PowerShell script against your endpoint - this will show you discrepancies in the configuration. Use the ASD - May 2018 - Windows 10 1709 Release Guide to understand the impact and fix those into your build. Cross reference with NCSC Windows 10 guidance for reassurance. There are plenty of guides out there but these have been my go to references lately. Another shout out to ADSecurity.org for their hardening recommendations too.

---

9. Penetrate Yourself Using Best Practice :S

Adhere to a detection framework/standard. The Mitre Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Matrix is the latest infosec trend and is being called

> *A Revolution in Security*

Endgame

> *...best current repositories of attacker tactics has been collected by the team at MITRE.*

RedCanary

All aboard the hype train. You could think of this as a detailed version of the Lockheed's Cyber Kill Chain framework which has been around for years. The good thing about ATT&CK is that this provides your detailed breakdown of the specific attack and which threat actor uses it (from submitted Open Source Intelligence).
Start by carrying out a gap analysis against the Mitre ATT&CK Matrix of your current detection methods - a great post on this is from Roberto Rodriguez (@cyb3rward0g) How Hot Is Your Hunt Team, use Florian Roth's (@cyb3rops) Sigma (a Generic Signature Format for SIEM Systems) for generating detection rules and JPCERT Detecting Lateral Movement v2 to help cover gaps easily. Also, test your endpoints (in a lab) with one of the many Red Teaming Frameworks out there, I like especially the Canary Redteam framework. Together with these testing frameworks and attack detection matrixes you start to cover gaps. Keep adapting detections and be sure to check out DOSobfuscation

- Redcanary https://redcanary.com/atomic-red-team/
- Red Team Automation https://github.com/endgameinc/RTA
- Caldera https://github.com/mitre/caldera
- Metta https://github.com/uber-common/metta
- APT Simulator https://github.com/NextronSystems/APTSimulator
- Dumpster Fire https://github.com/TryCatchHCF/DumpsterFire

All can be found in https://github.com/redhuntlabs/RedHunt-OS in a virtual machine for lab use.

While these frameworks are useful for testing, questions have been raised about the future of red teaming/penetration testing. I don't think they are a direct replacement for a penetration test or a Red Team engagement but do offer the Blue Team a great resource to cover "basics" and for detection to be built upon.

---

10. Be Proactive

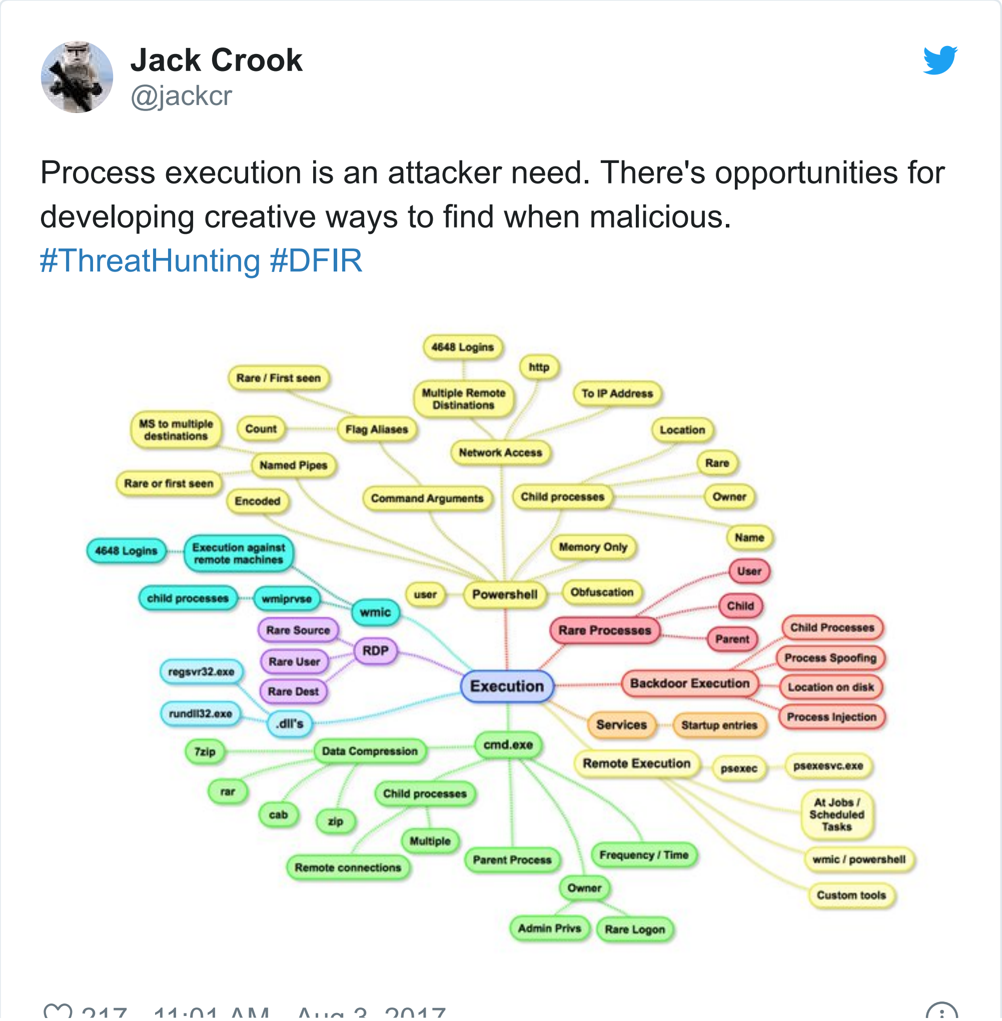
Go Threat Hunting.

> *In Hunting organizations, the IR team actively goes looking for incidents based on known patterns of activity, intelligence, or even just hunches. Once the hunt team finds a new incident they begin an IR as usual.*

Basically, Threat Hunting increases the likehood of detecting unkown threats in your environment.

Set some time aside Daily / Weekly, monthly runs/searches to find anomalies and outlier

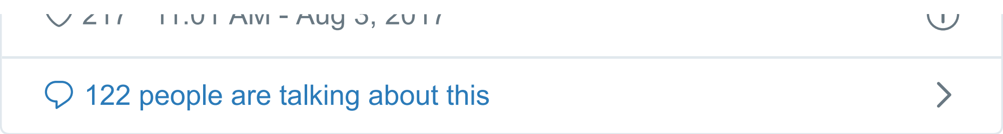
Set some time aside Daily / Weekly, monthly runs/ searches to find anomalies and outlier detections - these are human driven activities and are not classified as alerts. Record and automate any things you can. The Endgame Guide to Threat Hunting is an excellent resource. Living off the land hunt is a good start. Other ideas for hunts can come via the community and especially Jack Crook @jackcr - follow!



Jack Crook
@jackcr

Process execution is an attacker need. There's opportunities for developing creative ways to find when malicious.
#ThreatHunting #DFIR

♡ 217 11:01 AM - Aug 3, 2017



♡ 217 11:01 AM - Aug 3, 2017

122 people are talking about this

Malware Archeology's logging cheat sheets are great for a quick insight into the details of advanced logging aswell as providing search strings within Splunk.

Sqrrl are another company doing good in the Threat Hunting arena and provide excellent resources such as Hunt Evil. A great place to start your Threat Hunting programme.

11. Network Meta-data

Network Tap ingress/egress locations. Basically, tap into your network and see what is normal. Investigate the things that aren't.

> *Visibility and continuous monitoring of network traffic must encompass all levels of the network, to include gateway, midpoint, and endpoints. If a rule-set alerts at the network level, analysts must be able to pinpoint and isolate the actual end-host which generated the activity*

https://www.nsa.gov/resources/cybersecurity-professionals/

You need to be logging network metadata to accompany the typical IDS which primary fires on

You need to be logging network metadata to accompany the typical IDS which primary fires on known bad. Bro IDS is one of these systems that can help track the mounds of meta data that runs across your network.

You can look at it like WireSharks protocol analyser but instead of a GUI front end Bro will log to multiple .txt files per protocol ready for SIEM ingestion - a list of them all are available from Corelight in a nice PDF format - Keep an eye out for Corelight as Seth Hall one of the creators of Bro works. Key logs are DNS, HTTP, CONN, SMB and SSL/x509 data. If you can create a TLS inspection zone (MiTM) and get a mirrored copy over to Bro then even better. A great book I've already pitched that has helped me tremendously is Applied Network Security by Jason Smith, Chris Sanders.

Check out my post on "RaspberryPi NSM" to see how simple it is to create a sensor. Code available on Github

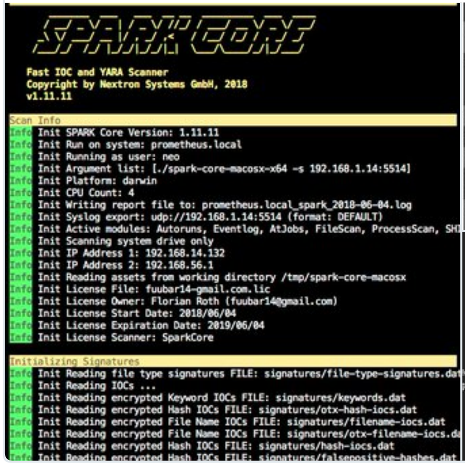
12. Looking For Known Bad

Deploy Advanced Endpoint Scanning. Not just Antivirus but something you can control/create signatures for. Tools such as the **free** Loki IOC scanner and more recently released the Go programmed SparkCore

Florian Roth
@cyb3rops

I am very happy to announce the release of SPARK Core, a free version of our enterprise-grade scanner SPARK. ✊
We've been working on this for weeks. See the comparison chart & website for details. twitter.com/thor_scanner/s…

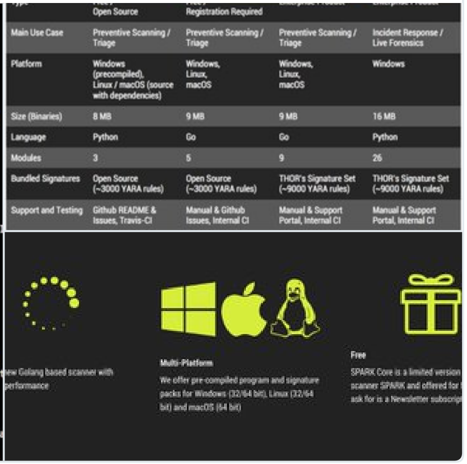
Nextron Systems @thor_scanner
SPARK Core v1.12
Our new and free multi-platform IOC & YARA scanner
> Open-Source signature base
> Windows, Linux & macOS
> Free / Subscription required
> add your custom IOCs or YARA rules and hunt them down 🏹
nextron-systems.com/spark-core/



```
Fast IOC and YARA Scanner
Copyright by Nextron Systems GmbH, 2018
v1.11.11

Scan Info
Info Init SPARK Core Version: 1.11.11
Info Init Run on system: prometheus.local
Info Init Running as user: neo
Info Init Argument list: [./spark-core-macosx-x64 -s 192.168.1.14:5514]
Info Init Platform: darwin
Info Init CPU Count: 4
Info Init Writing report file to: prometheus.local_spark_2018-06-04.log
Info Init Syslog export: udp://192.168.1.14:5514 (format: DEFAULT)
Info Init Active modules: Autoruns, Eventlog, AtJobs, FileScan, ProcessScan, SH
Info Init Scanning system drive only
Info Init IP Address 1: 192.168.14.132
Info Init IP Address 2: 192.168.56.1
Info Init Reading assets from working directory /tmp/spark-core-macosx
Info Init License File: fuubar14-gmail.com.lic
Info Init License Owner: Florian Roth (fuubar14@gmail.com)
Info Init License Start Date: 2018/06/04
Info Init License Expiration Date: 2019/06/04
Info Init License Scanner: SparkCore

Initializing Signatures
Info Init Reading file type signatures FILE: signatures/file-type-signatures.dat
Info Init Reading IOCs ...
Info Init Reading encrypted Keyword IOCs FILE: signatures/keywords.dat
Info Init Reading encrypted Hash IOCs FILE: signatures/otx-hash-iocs.dat
Info Init Reading encrypted File Name IOCs FILE: signatures/filename-iocs.dat
Info Init Reading encrypted File Name IOCs FILE: signatures/otx-filename-iocs.da
Info Init Reading encrypted Hash IOCs FILE: signatures/hash-iocs.dat
Info Init Reading encrypted Hash IOCs FILE: signatures/falsepositive-hashes.dat
```



	Open Source	Registration Required		
Main Use Case	Preventive Scanning / Triage	Preventive Scanning / Triage	Preventive Scanning / Triage	Incident Response / Live Forensics
Platform	Windows (precompiled), Linux / macOS (source with dependencies)	Windows, Linux, macOS	Windows, Linux, macOS	Windows
Size (Binaries)	8 MB	9 MB	9 MB	16 MB
Language	Python	Go	Go	Python
Modules	3	5	9	26
Bundled Signatures	Open Source (~3000 YARA rules)	Open Source (~3000 YARA rules)	THOR's Signature Set (~9000 YARA rules)	THOR's Signature Set (~9000 YARA rules)
Support and Testing	Github README & Issues, Travis-CI	Manual & Github Issues, Internal CI	Manual & Support Portal, Internal CI	Manual & Support Portal, Internal CI

ew Golang based scanner with performance

Multi-Platform

We offer pre-compiled program and signature packs for Windows (32/64 bit), Linux (32/64 bit) and macOS (64 bit)

Free

SPARK Core is a limited version scanner SPARK and offered for ask for is a Newsletter subscrip

382 6:39 AM - Jun 14, 2018

210 people are talking about this

Both can be utilised to run and dump results out locally ready for ingestion into your SIEM product. Another feature is that you can compile your own Yara signature set into the tools as well as the default signatures that Florian provides. Keep an eye on Nextron-Systems for free and enterprise ready versions.
Note: *I used Loki in my SANS 508 CTF final day to quickly scan several machines using custom signatures (which you learn about throughout the week) to detect a heavily compromised machine to which you can pivot off and start your investigation.*

---

13. Stop Responding

Netbios and LLMNR Name Poisoning Could go down under the OS hardening section but this is a key configuration to thwart some of the new hacking tools out there.

> *Link-Local Multicast Name Resolution (LLMNR) and Netbios Name Service (NBT-NS) allow machines on the same subnet help each other identify hosts when DNS fails.*

The goal is to prevent Responder (Python LLMNR, NBT-NS, WPAD and MDNS poisoner / HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server) / Inveigh (PowerShell LLMNR/mDNS/NBNS spoofer) which are Man-In-The-Middle tools for gathering of NTLM

LLMNR/mDNS/NBNS spoofer) which are Man-In-The-Middle tools for gathering of NTLM hashes that will be use for lateral movement. Check out @byt3bl33d3r's blog on the topic Practical guide to NTLM Relaying in 2017 (A.K.A getting a foothold in under 5 minutes)

Recommendations;

- **Disable Netbios NBT-NS** or set this registry entry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces\` set DWORD value `NetbiosOptions` to be changed to `2`
- **Disable LLMNR**. `Computer Configuration\Policies\Administrative Templates\Network\DNS Client\Turn off Multicast Name Resolution` set to `Enabled`
- **Disable old SMB versions** and **enable SMB signing** that digitally signs the traffic communication between endpoints preventing spoofed attempts.

To accomplish this via Group Policy - A good how-to is available from 4ARMed.

> *In our experience of using this technique during penetration testing engagements, we have very often captured and cracked credentials for Domain Admin accounts, leading to rapid compromise of the entire Active Directory domain and its resources. One further reason why administrators should not use privileged accounts for non-administrative activities such as Internet browsing.*

Further reading here; https://medium.com/@adam.toscher/top-five-ways-i-got-domain-admin-on-your-internal-network-before-lunch-2018-edition-82259ab73aaa

---

14. Account Breaches - 5,115,553,456 And Counting!

Enable 2-Factor Authentication / Multi-factor Authentication is a must nowadays. I'm still coming across this for a few enterprises! Worrying thing is, I've spoken to IT "professionals" that don't have this enabled.

What's the difference between 2FA and MFA? - 2FA is something you personally have on your that will need to be used as part of the authentication process such as a Phone(SMS), a hard token(Yubikey/RSA Token) or even a soft token(Authy/Google Authenticator). SMS - bad example i know! the SS7 network is vulnerable to interception.

From an enterprise perspective *all* external login portals and VPNs are a must. High risk portals internally of which if they were compromised would be devasting for the company then they should have a verification process added to them incorporating a hardware token for extra security.

If I had to implement 2FA I could definitely check out DUO Security as their documentation across a wealth of technology stacks is amazingly good.

For physical tokens, I'm a fan of Yubikeys which range between £18-£40 depending on the capabilities your after for example, NFC. For Soft tokens I would use Authy but this is a cool list of other products here on Wikipedia

For websites that support 2FA then check out TwoFactorAuth.org and enable it for EVERYONE you have!!1

15. Password Management

Leading on from the above really. Use a **centralised Password Manager** and combined this with a YubiKey or a soft token system like Authy. This method be used to secure Password databases such as KeePass / Dashlane / Bruce Schneier's PasswordSafe / 1Pass / LastPass

> *They reduce security friction - making security easier and more convenient. If security is difficult, tedious, appears to add no value or gets in the way of the main task we're trying to do, then we tend to find (insecure) ways around it*

NCSC

This will encourage unique credentials across the estate. Same with your personal passwords, if one site were to get breached you don't want that being used against your other accounts. A cool feature from 1Password is that it will now check your password against the HaveIBeenPwned list of compromised accounts to warn you on your poor password choice.

Sign up for notifications for each of your email accounts on HaveIBeenPwned.com or subscribe to their RSS feed

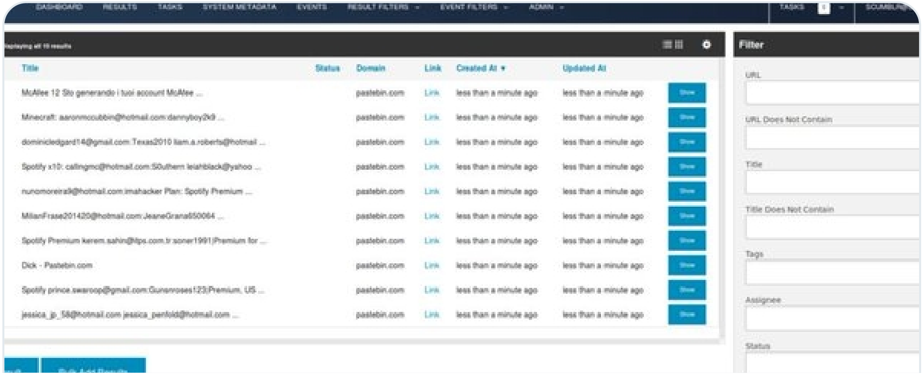
16. Sieving Through The Internet

Create an **automated OSINT capability** to see what is out there already exposed based on criteria you specify. Limit what is out there by removing content or changing found credentials and keys. Credentials, keyword searches for sensitive projects/parts, source code containing API keys and credentials are just a few areas of interest an attacker is looking for against your organization.

A popular choice is Netflix's Scumblr which can use APIs to crawl a dozen data sources including Social media. Check out @PortUnreachable's quick overview of Scumblr

Gary Hoffman
@PortUnreachable

Just published my latest blog on "Automated #OSINT with Scumblr"portunreachable.com/automated-osin…



Displaying all 10 results

Title	Status	Domain	Link	Created At ▾	Updated At	
McAfee 12 Sto generando i tuoi account McAfee ...		pastebin.com	Link	less than a minute ago	less than a minute ago	Show
Minecraft: aaronmccubbin@hotmail.com:dannyboy2k9 ...		pastebin.com	Link	less than a minute ago	less than a minute ago	Show
dominicledgard14@gmail.com:Texas2010 liam.a.roberts@hotmail ...		pastebin.com	Link	less than a minute ago	less than a minute ago	Show
Spotify x10: callingmc@hotmail.com:S0uthern leiahblack@yahoo ...		pastebin.com	Link	less than a minute ago	less than a minute ago	Show
nunomoreira9@hotmail.com:imahacker Plan: Spotify Premium ...		pastebin.com	Link	less than a minute ago	less than a minute ago	Show
MilanFrasa201420@hotmail.com:JeaneGrana650064 ...		pastebin.com	Link	less than a minute ago	less than a minute ago	Show
Spotify Premium kerem.sahin@tips.com.tr:soner1991|Premium for ...		pastebin.com	Link	less than a minute ago	less than a minute ago	Show
Dick - Pastebin.com		pastebin.com	Link	less than a minute ago	less than a minute ago	Show
Spotify prince.swaroop@gmail.com:Gunsnroses123|Premium, US ...		pastebin.com	Link	less than a minute ago	less than a minute ago	Show
jessica_jp_58@hotmail.com jessica_penfold@hotmail.com ...		pastebin.com	Link	less than a minute ago	less than a minute ago	Show

Automated OSINT with Scumblr

We all know that open source intelligence gathering can be quite time consuming, but the information found is sometimes invaluable

portunreachable.com

♡ 36 11:20 AM - May 7, 2018

18 people are talking about this

Just to show how extensive this area is check out this "Awesome OSINT list". Other tools of note are;

- https://github.com/mdsecactivebreach/LinkedInt
- https://github.com/michenriksen/gitrob
- https://github.com/kevthehermit/PasteHunter
- https://bitbucket.org/LaNMaSteR53/recon-ng

Out of scope but a final note on how powerful this can be;

> *The US military destroyed an Islamic State bomb factory a mere 23 hours after a jihadi posted a selfie revealing the roof structure of the building, which is perhaps the most powerful example of the military using OSINT for targeted operations*

A Brief History of OSINT

17. Response Is Key!

Create an Incident Response triage tool to quickly gather forensic artefacts within your environment. Be aware that gathering data (especially large collections such as memory) to the victim’s disk will overwrite data that might be valuable. Agent based tools are available but at a cost.

> *…live data collection is not without risk, however. An important consideration is to minimize changes to the system made due to the collection process…*
>
> *…there are folks who are purists, in a way, who believe that absolutely no action should be taken on a system that can affect its current state…*

Weigh up the risk before execution! Here are some artefacts to gather but not a complete list:

- Gather Live Memory

- Application Crash Dumps/Mini dumps.
- Hibernation file
- Pagefile
- EventLogs
- Prefetch Logs
- Amcache Logs
- Shimcache Logs
- Master File Table
- Running Processes
- Installed services

- Live Network Connections
- Arp/DNS Cache
- Local Groups/Users
- Network Shares
- Autoruns
- WMI Repository Database
- Scheduled Tasks

- Alternate Data Streams
- Registry Dump
- Web Cache
- Custom Yara Scan and output.

You should definitely create your own tool to fit your needs. Check out these to start you off;

- PowerForensics FREE
- Google Rapid Response FREE

or for an enterpise ready solution which is pitched in as part of the Incident Response SANS courses is F-Response - though I don't have much experience with this.

---

18. Protect Your Creds

Prevent cleartext passwords in memory. Not an exhaustive list of preventions/dections but a quick win.

> *The threat actor would modify key systems to store plaintext credentials in memory. In one instance, the threat actor executed the following command.*

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" /v UseLogonCredentia
```

US CERT TA18-074A Alert

- This attack can’t be performed on Windows 2012R2+ and Windows 8.1+.
- On older systems KB2871997 should be installed

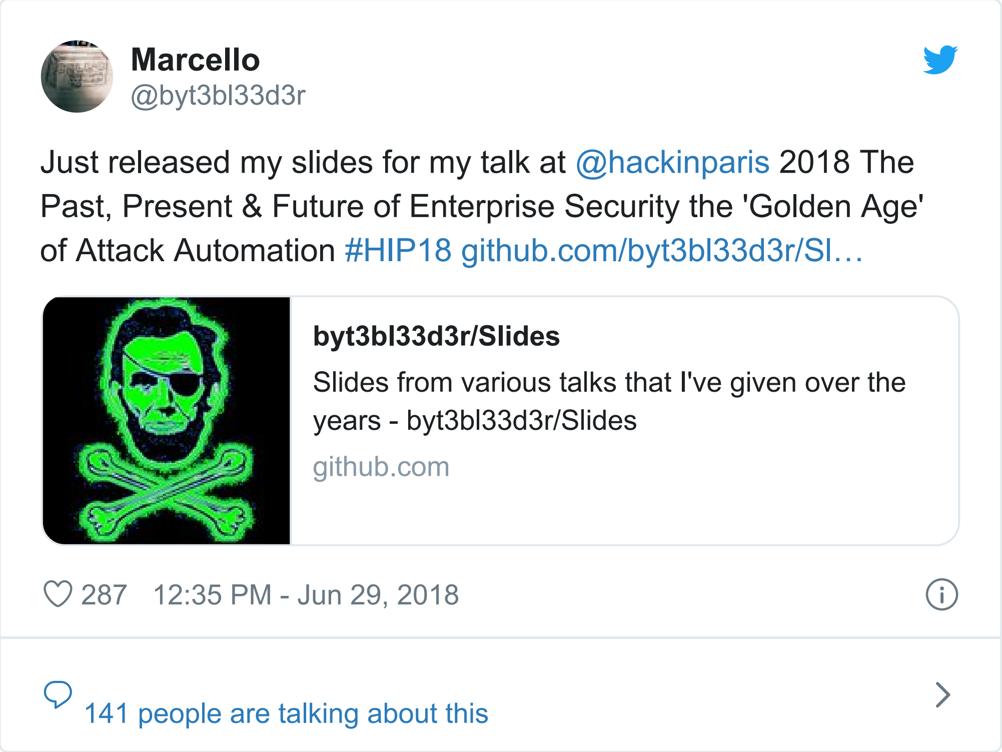
> *"Note By default in Windows 8.1 and Windows Server 2012 R2 and later versions, caching of credentials in memory for WDigest is disabled (the UseLogonCredential value defaults to 0 when the registry entry is not present)."*

For other Windows machines ensure detection is in place or prevent modification for the follow registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest
```

- If the UseLogonCredential value is set to 0, WDigest will not store credentials in memory.
- If the UseLogonCredential value is set to 1, WDigest will store credentials in memory.

Finally from:



Marcello
@byt3bl33d3r

Just released my slides for my talk at @hackinparis 2018 The Past, Present & Future of Enterprise Security the 'Golden Age' of Attack Automation #HIP18 github.com/byt3bl33d3r/Sl…

byt3bl33d3r/Slides
Slides from various talks that I've given over the years - byt3bl33d3r/Slides
github.com

287 12:35 PM - Jun 29, 2018

141 people are talking about this

> *Your Administrators should have a separate workstation for their administrative*

> *activities!*

Microsoft PAW (Priviledge Access Workstation) is the solution here. "Jump Box" solutions do exist but for now Microsoft have some basic coverage here.

---

19. Control the Power of PowerShell

Restrict and detect PowerShell usage as much as possible using some of the following methods.

- **The PowerShell “Version 2 problem"**. Once you have installed a newer version of PowerShell be sure to uninstall version 2! This will prevent downgrade attacks as explained earlier. Why would adversaries want to do this?
  - no AMSI (Antimalware Scan Interface)
    - Evaluate code just prior to execution (deobfuscated). Excellent when going up against https://github.com/danielbohannon/Invoke-Obfuscation.
  - no ScriptBlock Logging

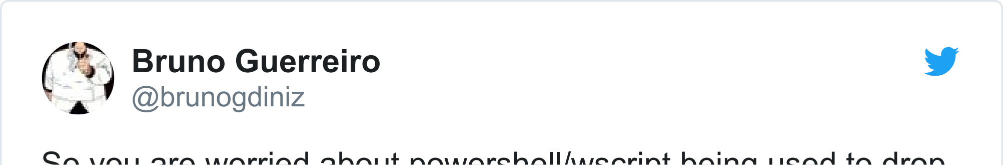
    - no Module Logging
    - no Transcription Logging

  Easily achievable if the default version is still installed on an endpoint. All they have to do is specify
  `PowerShell –Version 2`
  If you are delaying uninstallation for whatever reason, then for detection look for Event ID 400 (Engine Lifecycle) events from the “Windows PowerShell” log. Be sure to ingest these Event IDs first. See these cheat-sheets.

- **Lock PowerShell down to only talk to RFC1918 ranges** via host based firewall rules. Therefore restricting any outbound ranges used to download malicious payloads and still allowing sysadmins to do their job. WIN WIN.

  > *10.0.0.0/8 (255.0.0.0)*
  > *172.16.0.0/12 (255.240.0.0)*
  > *192.168.0.0/16 (255.255.0.0)*

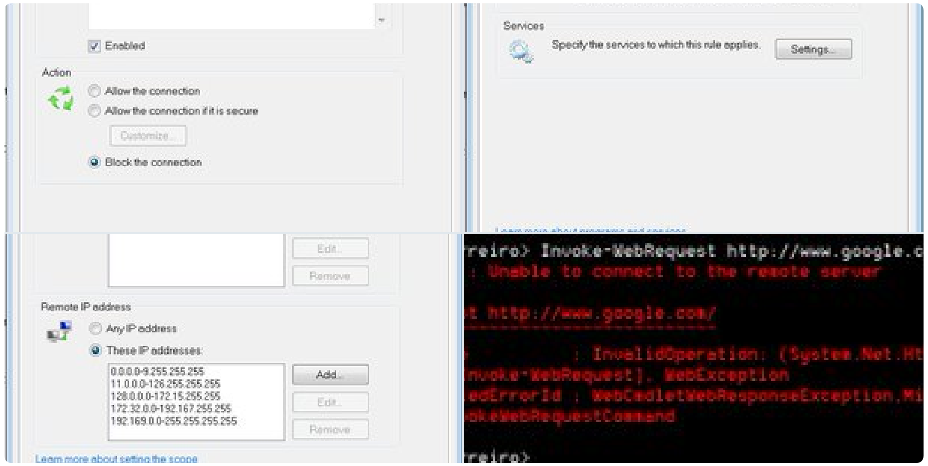
Excellent idea from @brunogdiniz;



Bruno Guerreiro
@brunogdiniz

So you are worried about powershell/wscript being used to drop

So you are worried about powershell/wscript being used to drop malware. How about applying Host Firewall rules to avoid it to connect non-RFC1918 addresses? Excellent idea that I learned other day here at twitter.#BlueTeam stuff



☑ Enabled

Action

○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

Services

Specify the services to which this rule applies.

Remote IP address

○ Any IP address

● These IP addresses:

```
0.0.0.0-9.255.255.255
11.0.0.0-126.255.255.255
128.0.0.0-172.15.255.255
172.32.0.0-192.167.255.255
192.169.0.0-255.255.255.255
```

```
reiro> Invoke-WebRequest http://www.google.c
 : Unable to connect to the remote server

t http://www.google.com/

              : InvalidOperation: (System.Net.Ht
nvoke-WebRequest], WebException
edErrorId : WebCmdletWebResponseException,Mi
okeWebRequestCommand

reiro>
```

♡ 824   10:06 PM - Aug 22, 2018

390 people are talking about this

- **Monitor for PowerShell .NET assembly calls** or more specifically system.management.automation.dll loading from third party applications.

> *..."allowing the execution of Powershell functionality without the use of Powershell.exe. Primarily this project uses.NET assemblies/libraries to start execution of the Powershell scripts."*
> *PowerPick Project*

So the idea here is to monitor executables that call PowerShell functionality (bypassing security features and the need for powershell.exe). C# and PowerShell are just frontends to .NET methods. Ideal for adversaries, as again, like the version downgrade, this eliminates the security features offered by the later PowerShell versions. This is known defensive evasion technique.

> *"...loading of system.management.automation.dll into non-powershell.exe processes."*
> *SpectreOp's GhostPack*

For detection you will need Sysmon (ingesting the DLL 'ImageLoaded' events) or similiar EDR functionality and look for;

- System.Management.Automation.dll
- System.Management.Automation.ni.dll ('ni' environment specific version)
- System.Reflection.dll

Further reading:

- BlackHills InfoSecurity Powershell Without Powershell – How To Bypass Application Whitelisting, Environment Restrictions & AV
- Endgames's Hunting For In-Memory .NET Attacks

20. Know your ASEP locations

Detect basic persistence mechanisms using Sysinternals tool Autoruns. This can be used to highlight malware persistence (T1060) , for trickier stuff manually query areas to dig in deeper but for a source for Threat Hunting this can be a treasure trove. Build detection around the Autoruns output once you have it to quickly highlight suspicious entries and then take remediation steps to remove known bad. A few of the key areas Autoruns highlights;

- Run Keys
- Services
- Scheduled Tasks
- Drivers
- WMI Consumers

Ingesting this data has been made easier by using the following script by Palantir to generate a custom Event Log to store the results of scheduled Autoruns job. Configure your SIEM to collect this extra Autoruns Event Log source to centralise the data and make it searchable (detect recent changes, unique entries etc.)

There are known methods to bypass or hide within Autoruns so use sparingly if you are viewing with the GUI. Some other notes:

- Autoruns WMI will only query root:subscription. Creation elsewhere will need manual querying.
- Be cautious of filtering by "Signed binaries" and or "Hide Windows Entities". For example, rundll32.exe and cmd.exe are legit binaries but can be chained to run malicious payloads.
- File Extension Search Order bypass (run .COM files before .EXE)

For others check out this awesome talk by the Huntress team.
https://youtu.be/AEmuhCwFL5I

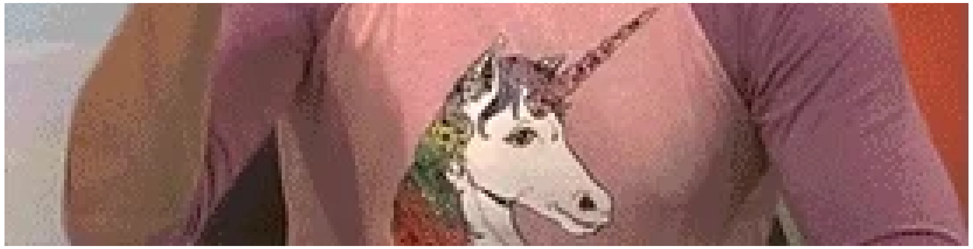
21. Active Directory Magic Tricks

Check for AD persistence - kicking a compromised account from your environment might not be effective as you think. Understanding AD persistence mechanisms is another line of defence for the Blue Team. One of which is this AdminSDHolder ACL template.

The AdminSDHolder ACL will be processed by SDProp, every 60 minutes (by default) on the PDC, re-applying any specified accounts/groups added with access rights over "protected groups".

Take Note: Administrative rights are needed in the first place to edit the AdminSDHolder "template" ACL for protected AD groups (Domain/Enterprise Admins, Server/Backup Operators, Print Operators etc).

SCENARIO: The attacker compromises an account and escalates it to Domain Admin, but has also edited the AdminSDHolder ACL with another new basic user. Blue Team, detect the compromised Domain Admin account and have reset/disabled it. Not knowing about that back-doored account, this will auto-update (60 minutes) via the SDProp on the PDC and grant the attacker rights over the "protected groups" once more. Basically allowing them to add themselves back in as Domain Admin. 😎



via GIPHY

Defense and detection against this persistence;

1. Look for orphaned accounts with `adminCount=1`. These still have rights over protected groups.

> *When a user is removed from a protected group, the adminCount attribute on that user account does not change; the value 1 remains.*

Snippet from ADSEcurity.org for detection

```
Import-Module ActiveDirectory Get-ADObject -LDAPFilter “(&(admincount=1)(|(objectcategory=person)(objectcategory=group)))” -Properties MemberOf,Created,Modified,AdminCount
```

2. Look for AdminSDHolder object permissions and alert on any changes made. See Object Access policies, or 3rd party tooling such as QUEST Change Auditor for example.

Several other AD persistence mechanisms can be found over here at ADSecurity and the talk DERBYCON talk Break Me03 Red vs Blue Modern Active Directory Attacks Defense Sean Metcalf 👍
Microsoft references for those wanting to further read up.

Mark

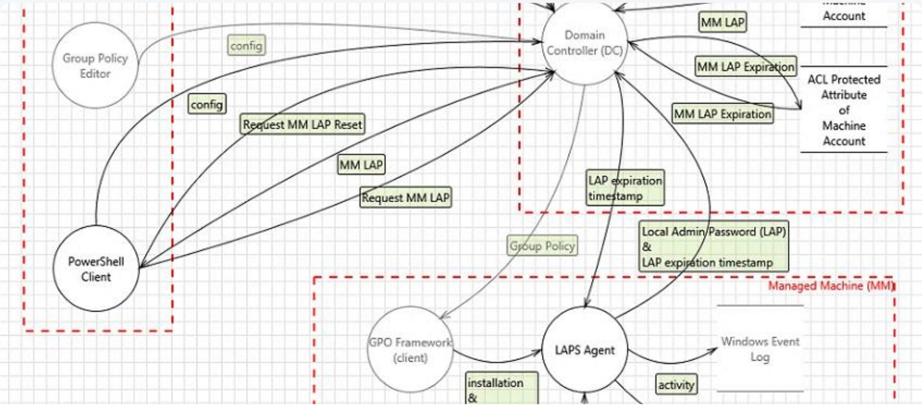
Read more posts by this author.

Read More

TRICKBOT

TRICKBOT - Analysis

Research into how to decode the TRICKBOT config, quickly



BLUETEAM

Blue Team Basics - Local Admin Password

analyse to provide context and help incident response/blue teams.

MARK

Blue Team Basics - Local Admin Password Administration

I used to be a Domain Administrator for a large AD deployment. Centralised account and access management was always a struggle so any solution to aid the manageability of administrative credentials is a

MARK

you sneakymonkey! © 2019

Latest Posts · Twitter · Ghost