Veil-Pillage: Post-Exploitation 2.0

Will
@harmj0y
Veris Group – Adaptive Threat Division

$ whoami

- Security researcher and pentester/red teamer for Veris Group's Adaptive Threat Division
- Co-founder of the Veil-Framework #avlol
  - www.veil-framework.com
  - **Shmoocon '14:** AV Evasion with the Veil Framework
  - co-wrote Veil-Evasion, wrote Veil-Catapult, Veil-PowerView, and PowerUp
- Active Cortana, Powershell, and NovaHacker!

tl;dr

- The Veil-Framework
- Post Exploitation; redux
- Veil-Pillage
- Current Module Overview
- Hashdumping and Plaintext Creds
- Demos
- KB 2871997 (Microsoft PTH fix?)
- Module Releases and Development
- Recap

The Veil-Framework

How We Got Here

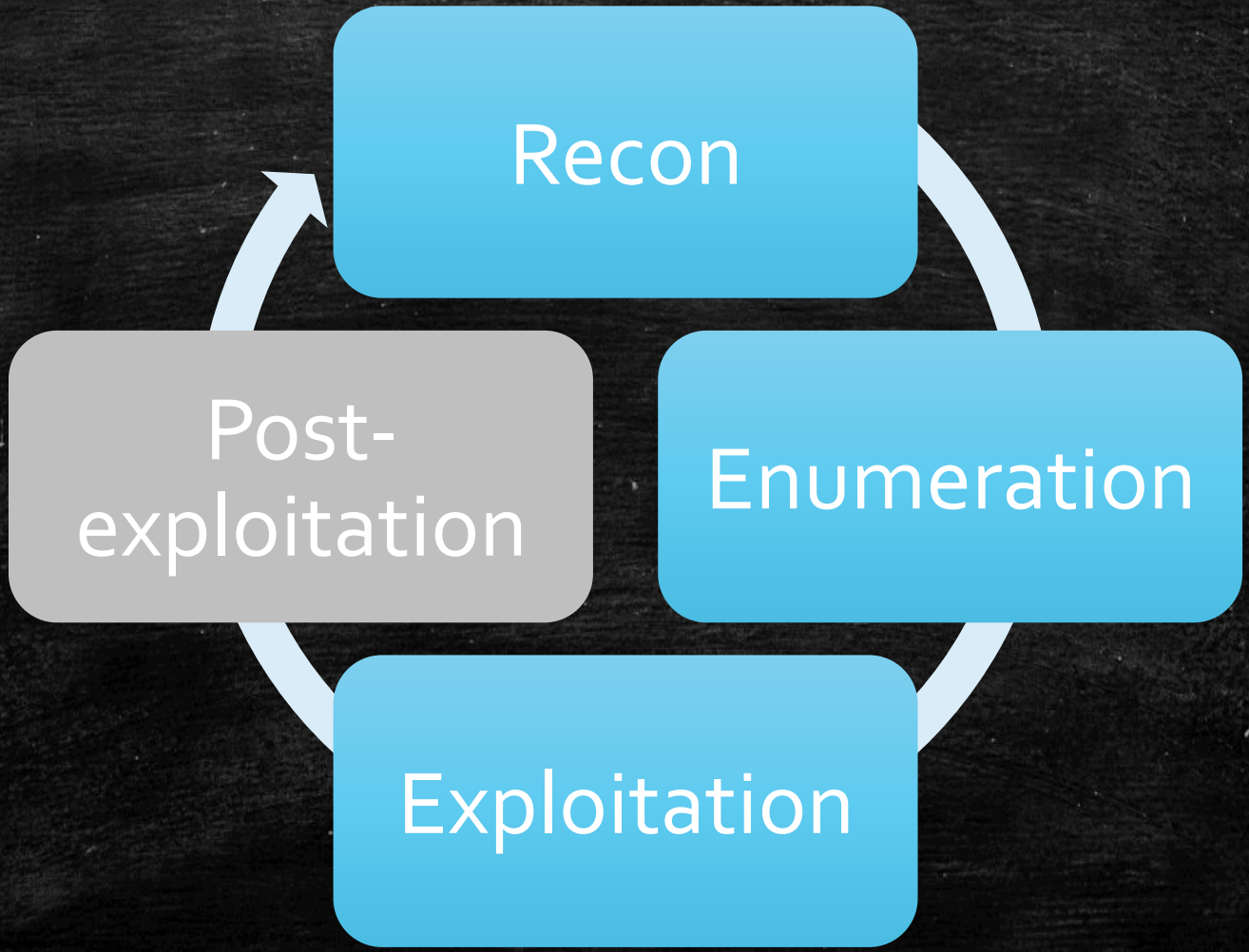
Background

- Started with the May 2013 release of 'Veil', later renamed to 'Veil-Evasion'
- Utilizes various languages and techniques to generate AV-evading payloads
  - shellcode injection and 'pure' meterpreter stagers
- Debuted at Shmoocon '14: "*AV-Evasion with the Veil-Framework*"
  - https://www.veil-framework.com/

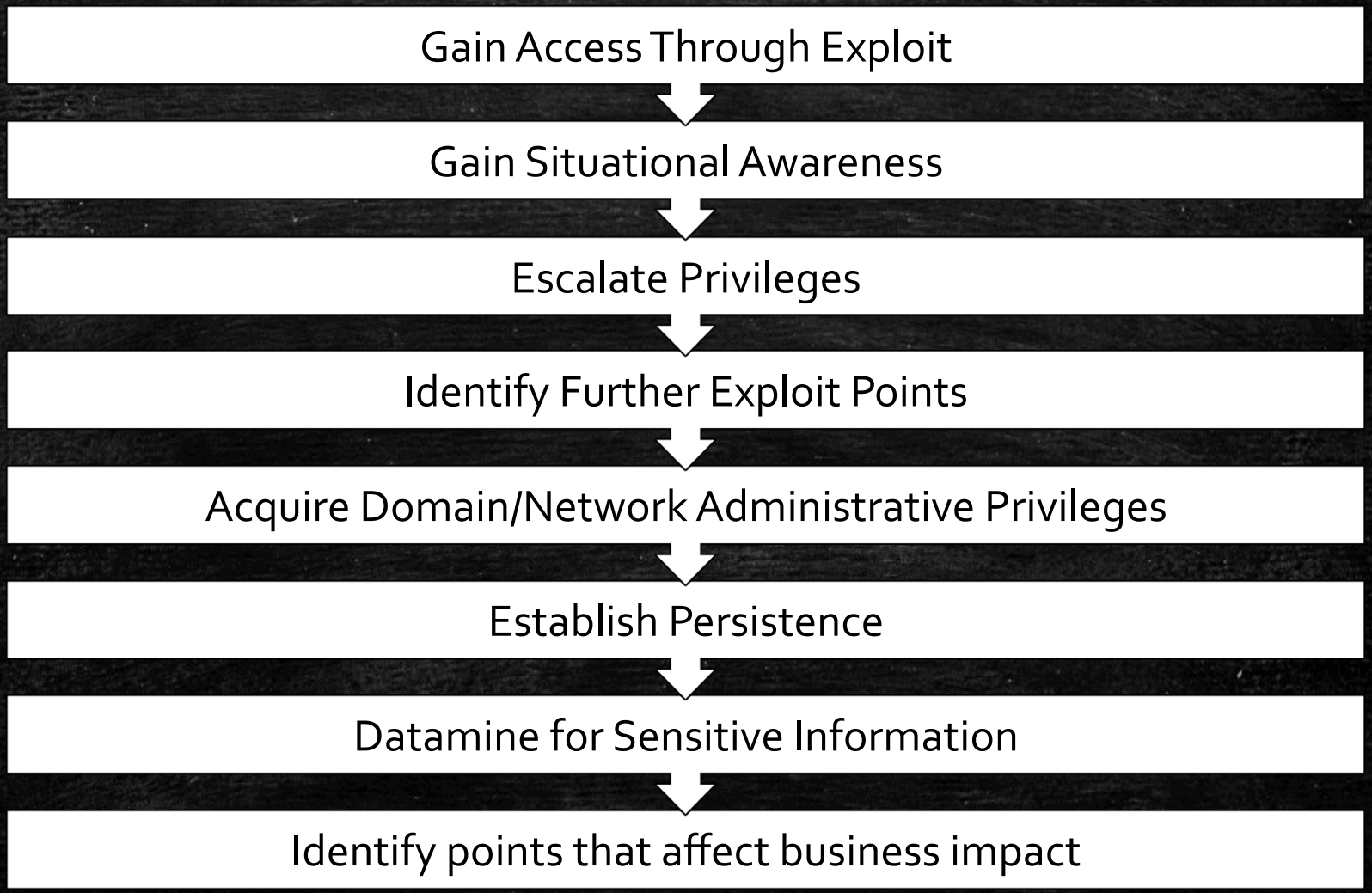
How We Got Here

- After dealing with AV-evasion, focus moved to payload delivery
- Wanted a way to trigger backdoors on target boxes in a stealthy way
- Released at **Shmoocon '14**, Veil-Catapult can upload/host and execute binaries, as well as few other common tricks

The Attack Cycle



Post-Exploitation; Redux



Post-Exploitation; English

- If you have access and/or credentials for one or more machines on a network, what can you do?

- **Example:** say you have a local administrator hash for remote hosts, and want to grab plaintexts of other logged on users on those hosts?

Post-Exploitation; Today

- **Option #1:** PSEXEC to a box with Metasploit, then getsystem/wdigest
- **Advantages:**
  - Flexible, can utilize the entire Metasploit framework
- **Drawbacks:**
  - service running as SYSTEM created
  - LOTS of non-standard traffic
  - "known" malicious binary dropped to disk

Post-Exploitation; Today

- **Option #2:** use smbexec to upload/ execute a wce.exe binary
- **Advantages:**
  - Don't need to establish a full Meterpreter session
  - Doesn't rely on MSF binary templates
- **Drawbacks:**
  - SYSTEM service still created
  - And another "known" malicious binary is uploaded/executed

Post-Exploitation; Today

- **Option #3:** use the passing-the-hash toolkit and PowerSploit
- **Advantages:**
  - No service created!!
  - No binaries dropped to disk!!
- **Drawbacks:**
  - Usage isn't the simplest
  - What if you want to do this on a lot of hosts?
  - What if powershell is disabled, or not installed?

What We Want

- **Trigger Options:** with a preference for stealth
- **Modularity:** want it to be easy to implement new post-exploitation techniques
  - And want to be able to easily integrate our code/techniques into other tools
- **Completeness:** automation, comprehensive logging, cleanup, etc.

Veil-Pillage

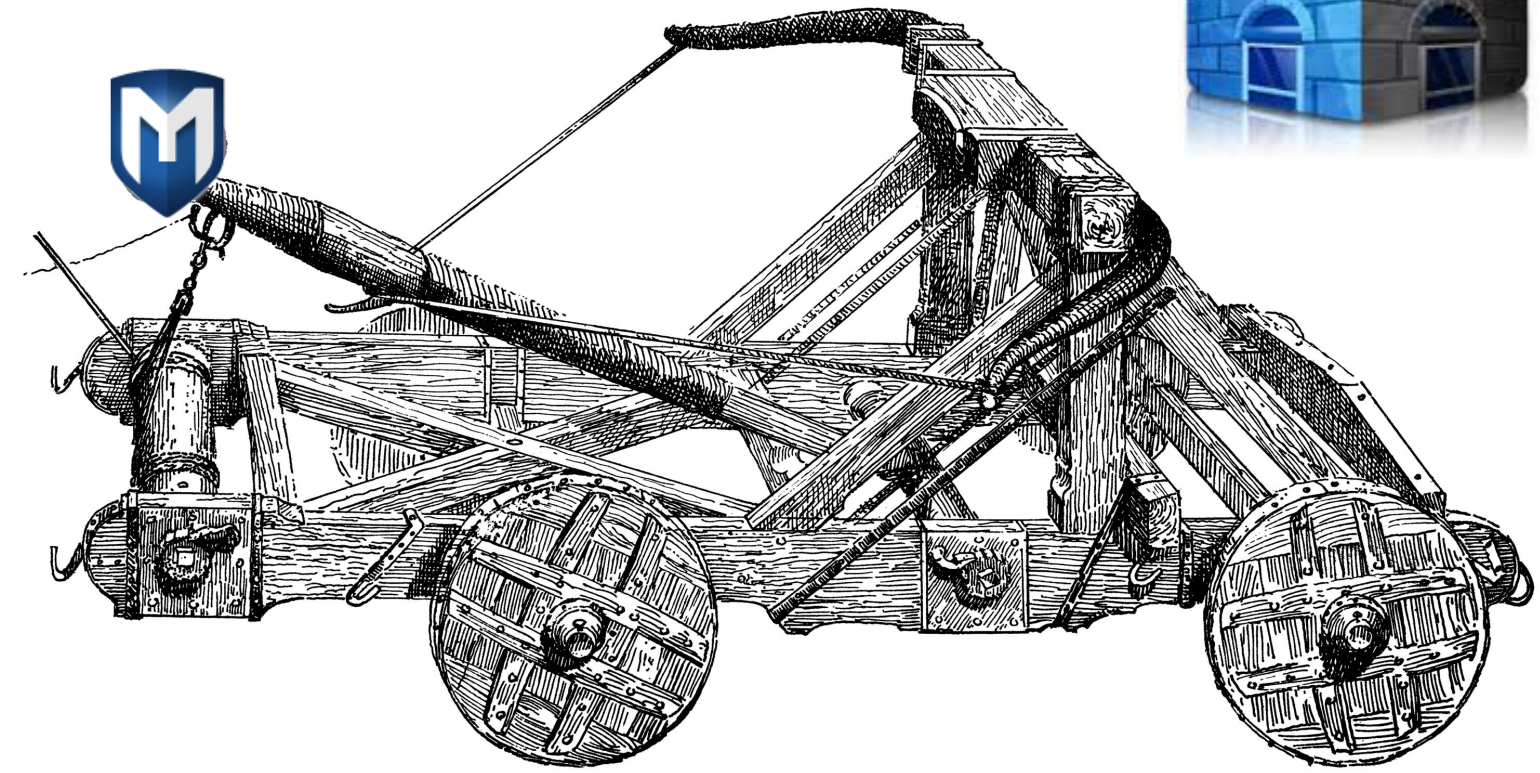
Catapult 2.0

Veil-Pillage Primitives

- **pth-wmis :** no service created
- **pth-winexe :** runs as system, binary dropped
- **Impacket-smbexec :** service created, but no binaries dropped
- **Impacket:** smbservers and clients and more

- Everything abstracted out to common library methods

Veil-Catapult Integration



Veil-Catapult Integration

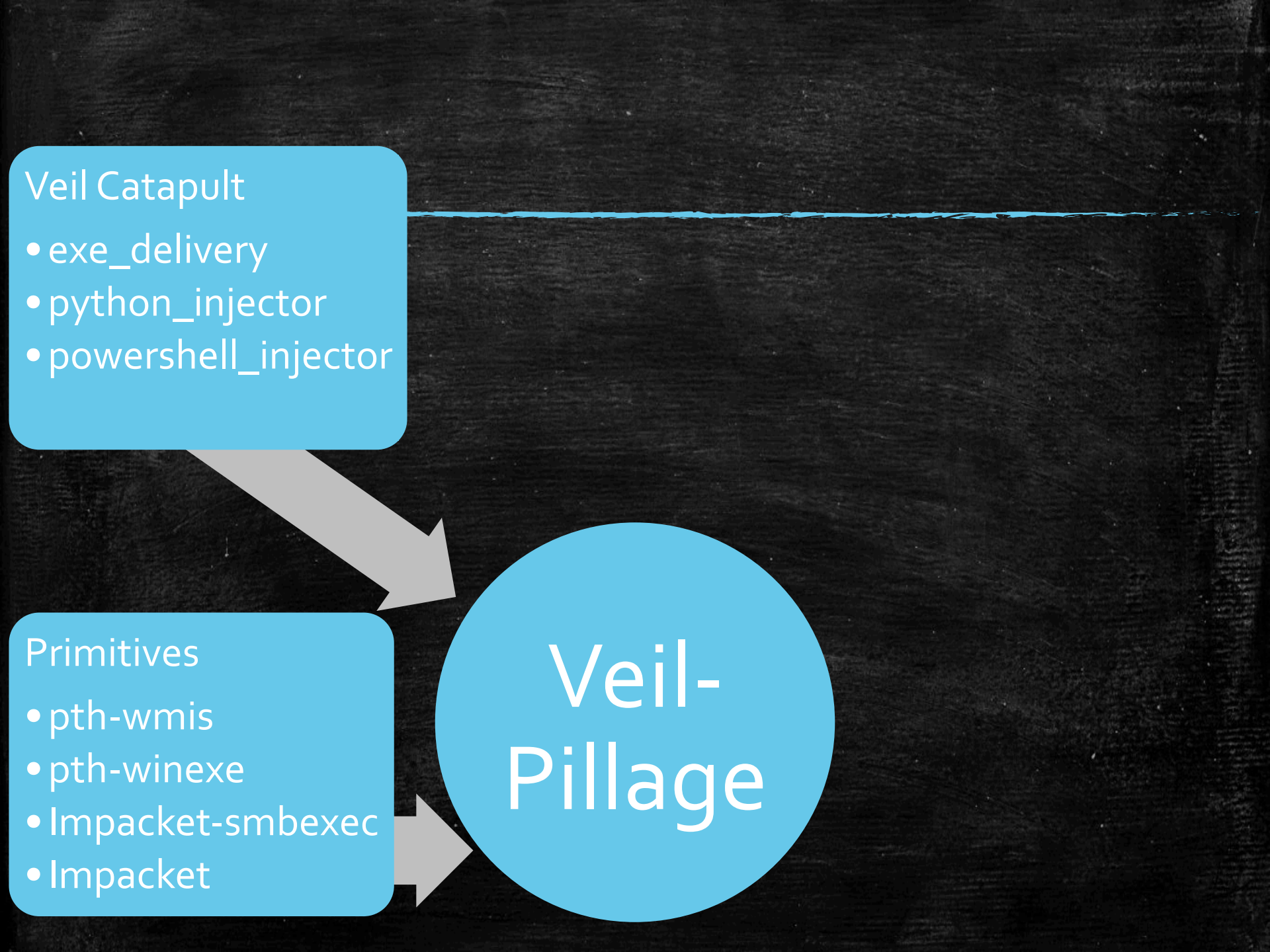
- All of Veil-Catapult's functionality has been modularly integrated into Veil-Pillage:
  - payload_delivery/exe_delivery
  - payload_delivery/powershell_injector
  - payload_delivery/python_injector
  - persistence/registry/sticky_keys
- Veil-Catapult will now be obsoleted :(
- Blog post on transitioning up soon

exe_delivery

- Catapult functionality ported to Pillage
- Executables can be specified, or generated with seemless Veil-Evasion integration
- .EXEs are then uploaded/triggered, or hosted/triggered with a \\UNC path
  - This gets some otherwise disk-detectable .EXEs right by some AVs

python_injector

- Uploads a minimal python .zip installation and 7zip binary
- Python environment unzipped, shellcode invoked using "-c …"
- The only files that touch disk are trusted python libraries and a python interpreter


Veil Catapult
• exe_delivery
• python_injector
• powershell_injector
Primitives
• pth-wmis
• pth-winexe
• Impacket-smbexec
• Impacket
Veil-Pillage

Veil-Pillage

New Features

powershell_stager

- Last month, the Veil team released custom-written, 'pure' powershell meterpreter stagers :
  - reverse_tcp/reverse_http/reverse_https

- These don't utilize any shellcode, and work great with the passing-the-hash toolkit

Output/Cleanup

- Logs logs logs
- Also, we want to leave boxes how we found them
  - Clients are so picky :)
- Why not do all of this in a nice and systematic way

Random features

- State preservation
  - On exit/rage quit, all options preserved
- MSF database interaction
  - pull in existing hosts and credential sets
- Tab-completion, error-checking, complete command line options, etc.

External Integration

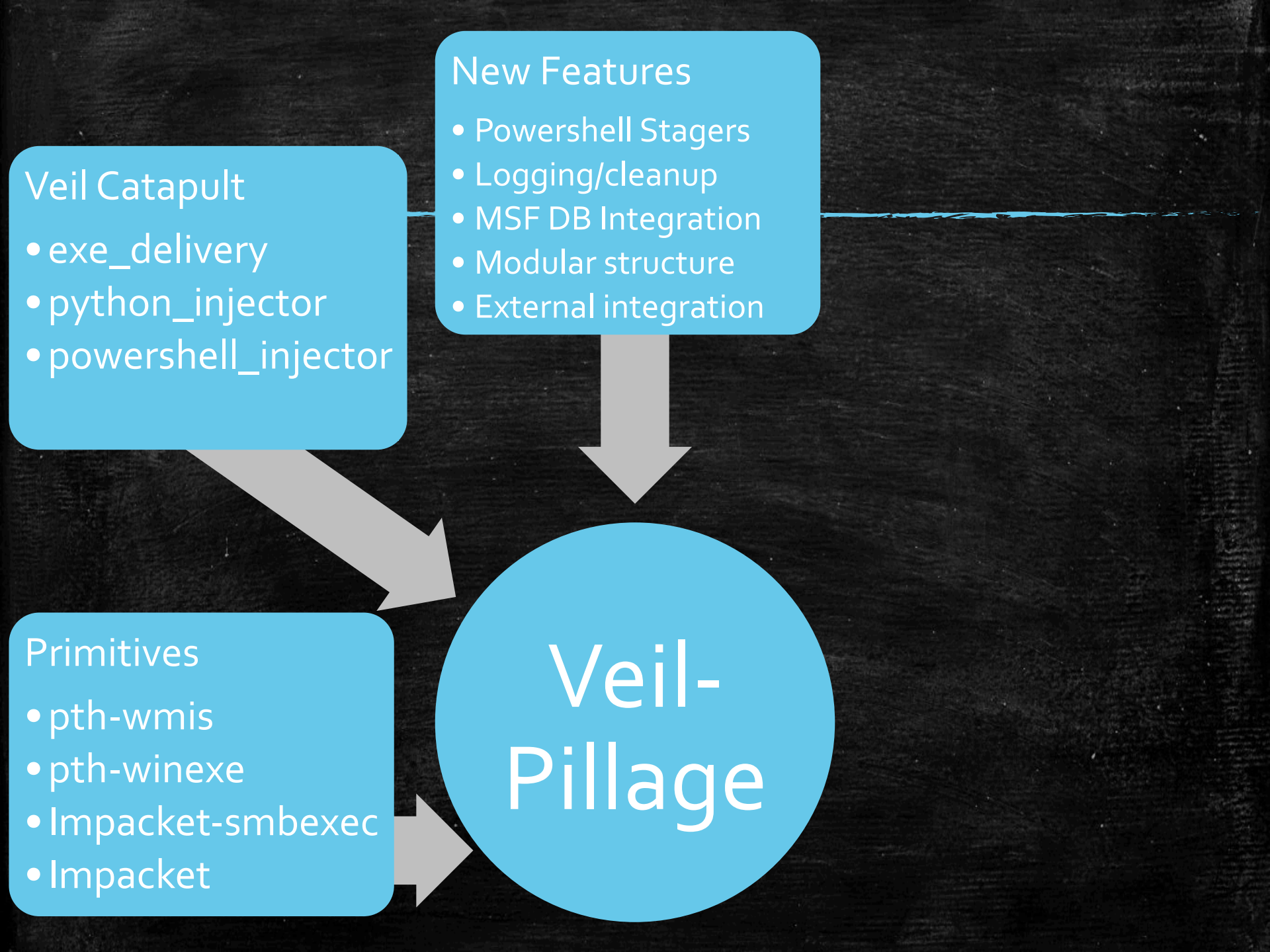
- Veil-Pillage contains complete command line flags for whatever you can think of
- Makes it easy to script-up and integrate Veil-Pillage into your own code

- see **./Veil-Pillage.py -h**

External Integration

- Similar to Veil-Evasion, it's easy to integrate Veil-Pillage's functionality as a library import:

```
from modules.management import check_uac
module = check_uac.Module(
        targets=["192.168.1.100"],
        creds=[["Administrator", "password"]])
module.run()
print module.output
```


New Features
• Powershell Stagers
• Logging/cleanup
• MSF DB Integration
• Modular structure
• External integration
Veil Catapult
• exe_delivery
• python_injector
• powershell_injector
Primitives
• pth-wmis
• pth-winexe
• Impacket-smbexec
• Impacket
Veil-Pillage

Veil-Pillage

New Modules

enumeration/*

- host/credential_validation
  - checks what creds work on what systems
- domain/user_hunter
  - finds where Windows domain users are logged in on the network
- host/enum_host
  - performs several standard enumeration actions

management/*

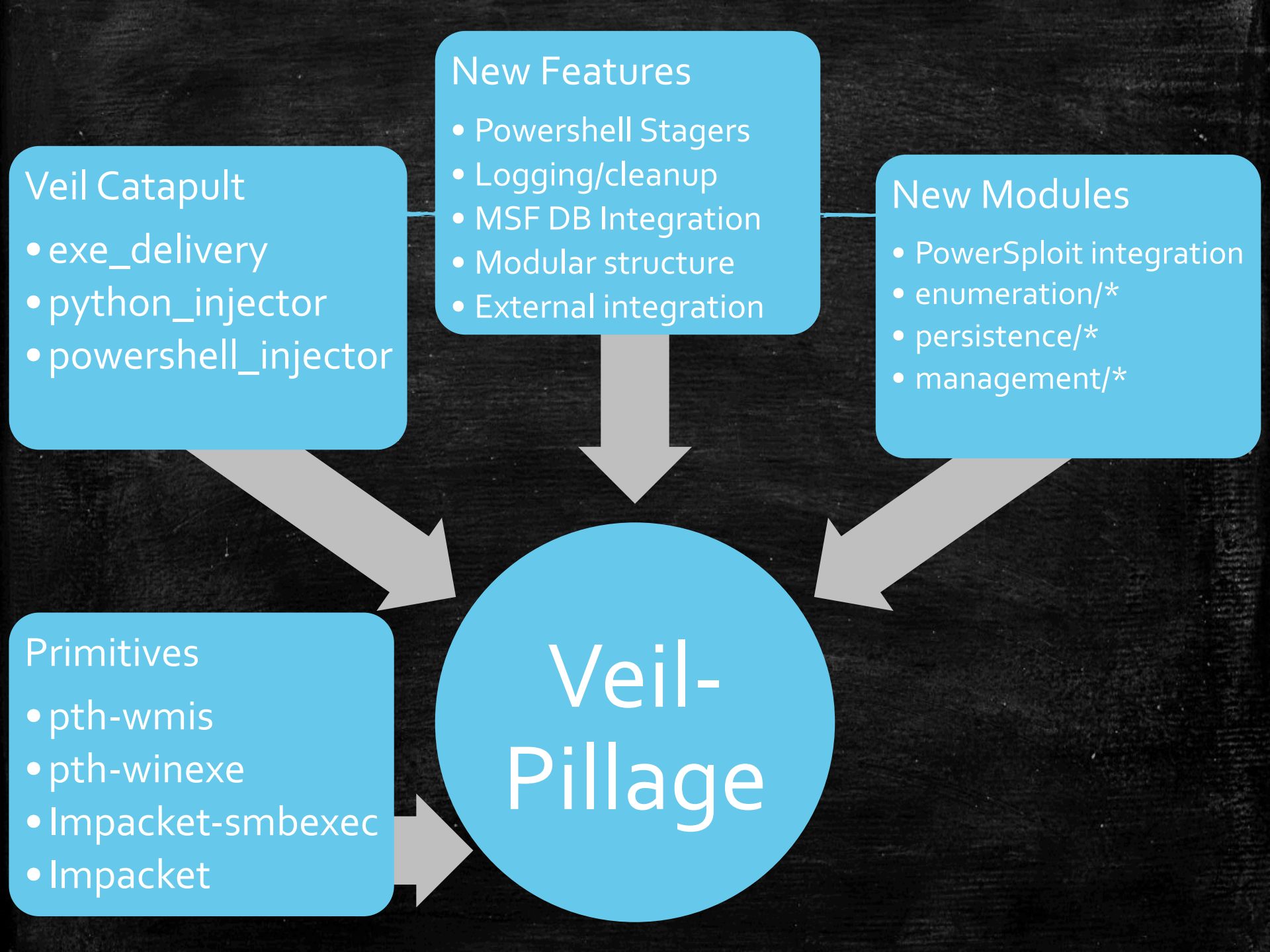
- check_uac/disable_uac/enable_uac
  - full user account control management
- enable_rdp/disable_rdp
  - enables RDP and the necessary firewall rules
- force_[logoff/reboot/shutdown]
  - needed to trigger some particular post-exploitation effects

persistence/*

- bitsadmin
  - adds a nice background job to download/ execute an .exe backdoor
- registry/sticky_keys*
  - Sets the stickkeys cmd.exe trick, or uploads an executable for to trigger
- registry/unc_dll
  - appends \\ATTACKER_IP; to %PATH%, allowing you to monitor for .dll hijacking opportunies

powersploit/*

- Several PowerSploit modules are included in Pillage
- A web server is stood up in the background
  - the 'IEX (New-Object Net.WebClient).DownloadString(...)' cradle is transparently triggered
- Makes it easy to run PowerSploit across multiple machines


New Features
• Powershell Stagers
• Logging/cleanup
• MSF DB Integration
• Modular structure
• External integration
Veil Catapult
• exe_delivery
• python_injector
• powershell_injector
New Modules
• PowerSploit integration
• enumeration/*
• persistence/*
• management/*
Primitives
• pth-wmis
• pth-winexe
• Impacket-smbexec
• Impacket
Veil-Pillage

Hashes and Plaintexts

Getting the Goods

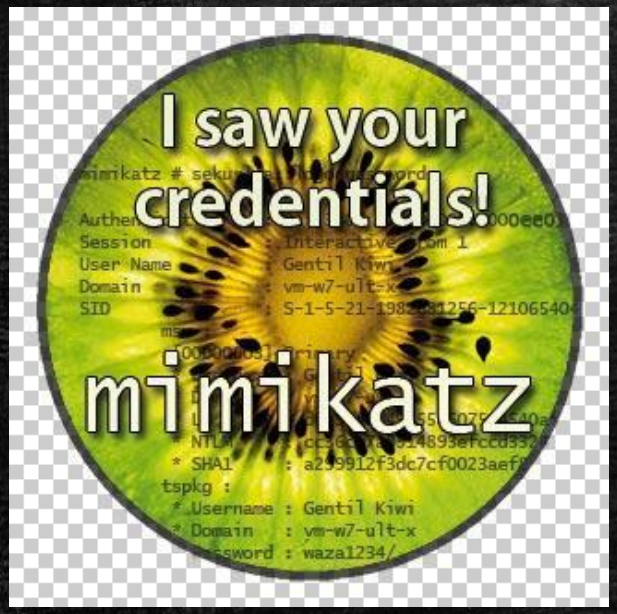
Hashdumping

- There are a diverse number of ways to dump hashes on a system
- **Traditional:**
  - gsecdump, credump, etc.
  - Registry backups w/ reg.exe
  - Meterpreter (hashdump/wdigest)
- **New Hotness:**
  - Powerdump.ps1
  - WCE/Mimikatz binaries
  - PowerSploit/Exfiltration/Invoke-Mimikatz.ps1

Hashdumping

- Different approaches work in different situations
- Dependent on architecture, Powershell installation, AV-installation, etc.
- Some involve dropping well-known, close-sourced tools to disk

In-Memory Mimikatz



+

= <3

In-Memory Mimikatz

- PowerSploit/Exfiltration/Invoke-Mimikatz.ps1
- Utilizes Joe "clymb3r" Bialek's prior work in Invoke-ReflectivePEInjection to inject an architecture-appropriate Mimikatz .dll
- Harnesses the power of Mimikatz without touching disk

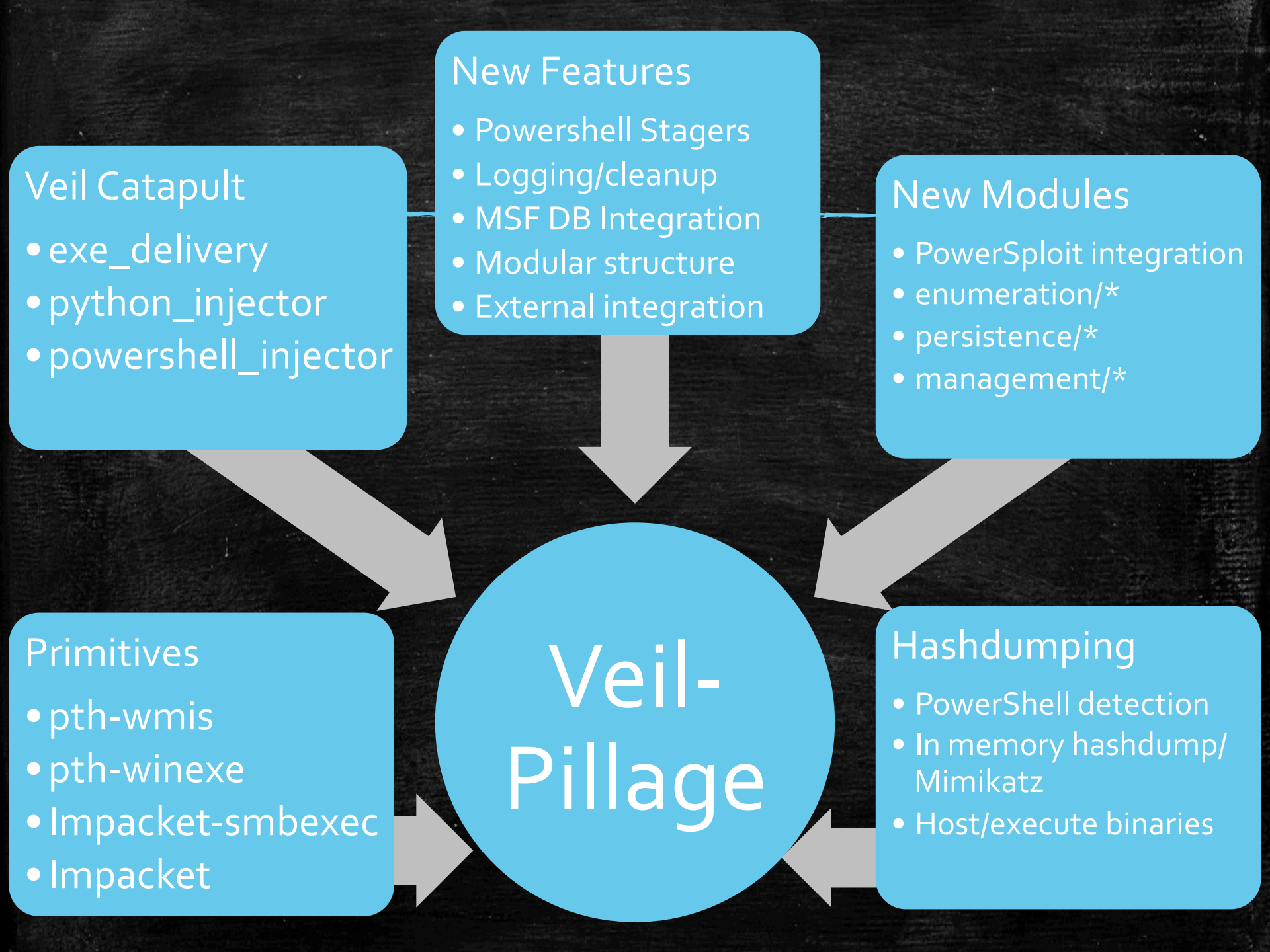
Pillage Style

- Let's aggregate some of the best techniques and build some logic in

```
if (powershell_installed)
    { Powerdump/PowerSploit}

else {
    determine_arch {
        host/execute appropriate binaries }}
```

- Expose these techniques to the user for situation-dependent decisions


New Features
• Powershell Stagers
• Logging/cleanup
• MSF DB Integration
• Modular structure
• External integration
Veil Catapult
• exe_delivery
• python_injector
• powershell_injector
New Modules
• PowerSploit integration
• enumeration/*
• persistence/*
• management/*
Veil-Pillage
Primitives
• pth-wmis
• pth-winexe
• Impacket-smbexec
• Impacket
Hashdumping
• PowerShell detection
• In memory hashdump/ Mimikatz
• Host/execute binaries

Demos

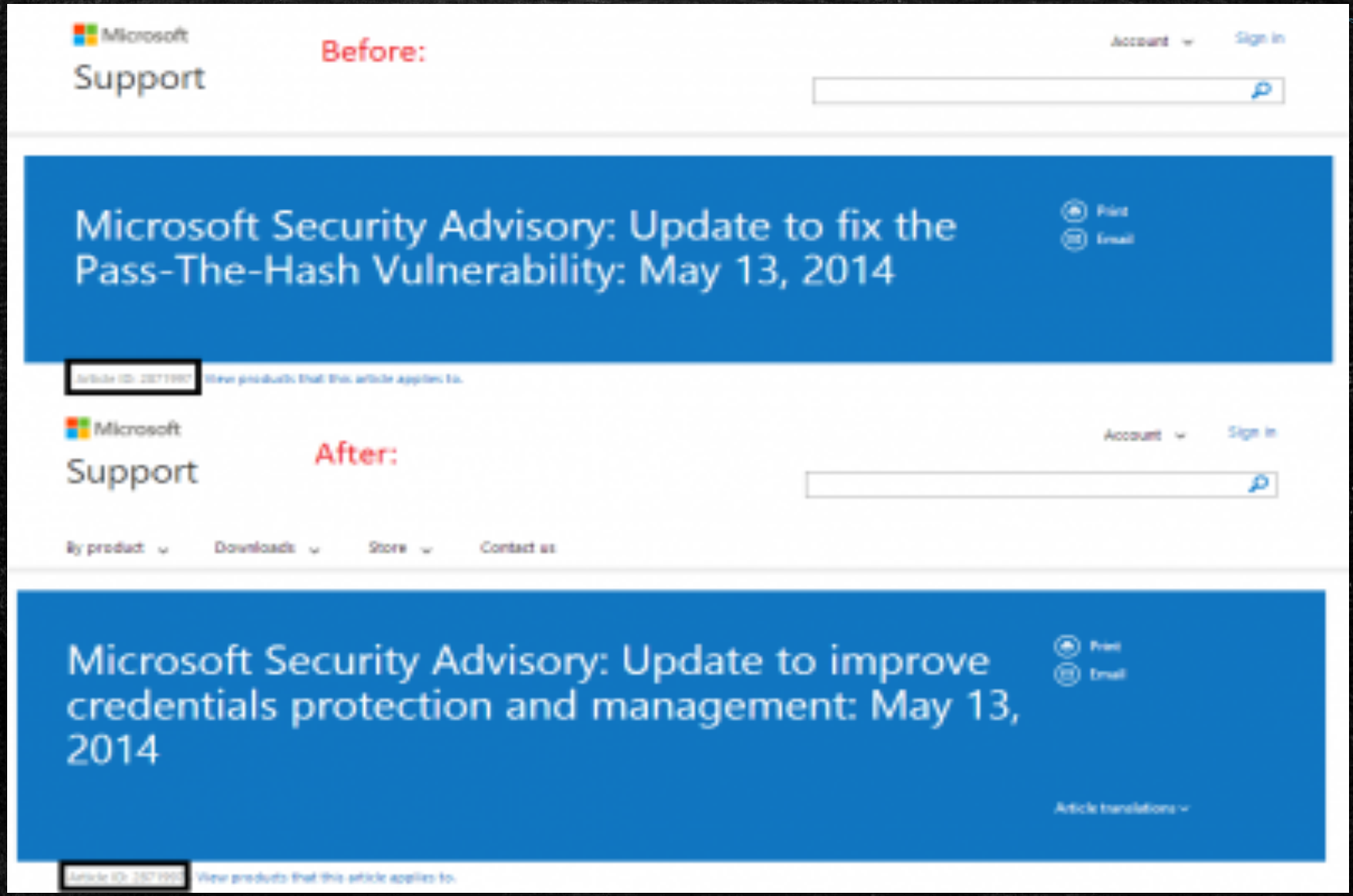
KB 2871997

OMG US PENTESTERS ARE OUT OF A JOB!!

KB 2871997

- The “pass-the-hash” killing patch, aka the “Mimikatz KB” :)
- Microsoft backport of Windows 8.1 protections that prevents “…network logon and remote interactive logon to domain-joined machine using local accounts”
- Sounds ominous…

PTH-killer? lol :)



KB 2871997 tl;dr

- The rid-500 Administrator account (if it's enabled) and domain accounts in the Administrators localgroup can still PTH
  - This account is often still enabled in many enterprise environments
- Powershell Remoting still works fine
- Windows XP/2003 obviously unaffected
- Raises the bar, but PTH isn't going away anytime soon

Local Admin Enumeration

- With a local/unprivileged domain account, you can use PowerShell (or Nmap) to:
  - find what the local rid-500 is renamed to and whether it's enabled
  - enumerate what domain accounts have local admin privileges on a machine
- Powershell functions have been integrated into Veil-Powerview
- More information: http://harmj0y.net

Local Admin Enumeration

```
PS C:\Users\matt\Desktop> Get-NetLocalGroup -HostName WINDOWS2


Server      : WINDOWS2
IsGroup     : False
AccountName : TEST/WINDOWS2/Administrator
Disabled    : False
SID         : S-1-5-21--658203039-1802703417-1428183180-500

Server      : WINDOWS2
IsGroup     : False
AccountName : TEST/WINDOWS2/mike
Disabled    : False
SID         : S-1-5-21--658203039-1802703417-1428183180-1000

Server      : WINDOWS2
IsGroup     : True
AccountName : TEST/Domain Admins
Disabled    : False
SID         : S-1-5-21--521750488-1329950333-216995329-512

Server      : WINDOWS2
IsGroup     : False
AccountName : TEST/jason
Disabled    : False
SID         : S-1-5-21--521750488-1329950333-216995329-1111
```

Module Releases

- Just like Veil-Evasion, lots of module ideas
  - more if people want to contribute :)
- Planned releases on the 1st of the month
- Check http://www.veil-framework.com for updates

Module Development

- Implement whatever post-exploitation fun you can think of
- Triggering methods, file downloads, etc. are all available as library methods
- Template included in the tree and blog post up soon on developing your own modules

Recap

- A flexible framework for post-exploitation of remote machines
- Three separate ways of triggering
- New modules are easy to implement with the common library
- Automation, full logging capabilities, cleanup scripts, big UI focus, active development

Questions?

- **Contact me:**
  - @harmj0y
  - harmj0y@veil-framework.com
  - harmj0y in #veil on Freenode
- **Read more:**
  - https://www.veil-framework.com
- **Get the Veil-Framework:**
  - https://github.com/Veil-Framework/