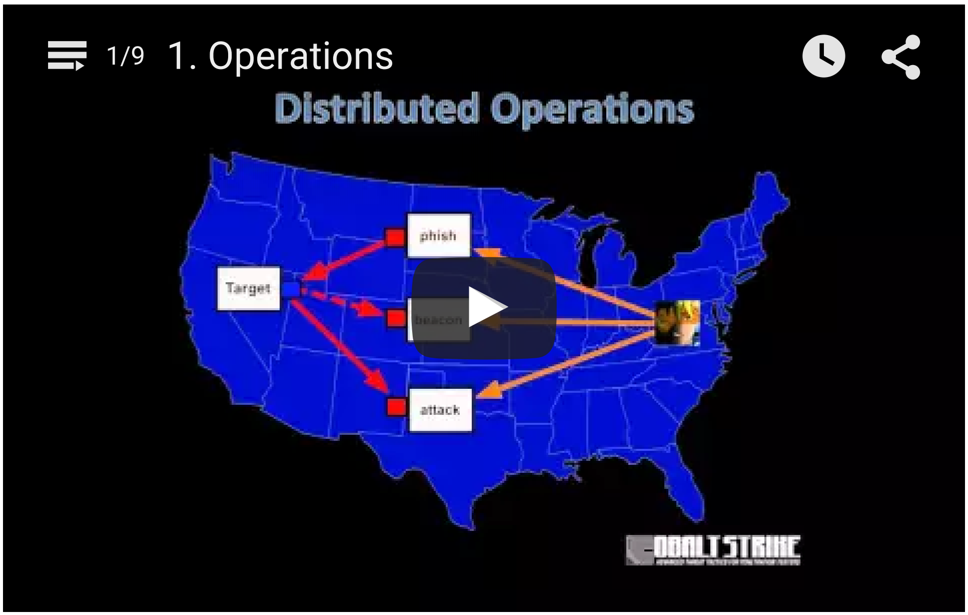
A blog about Armitage, Cobalt Strike, and Red Teaming

Advanced Threat Tactics – Course and Notes

September 30, 2015

The release of Cobalt Strike 3.0 also saw the release of Advanced Threat Tactics, a nine-part course on red team operations and adversary simulations. This course is nearly six hours of material with an emphasis on process, concepts, and tradecraft.

If you'd like to jump into the course, it's on YouTube:



Here are a few notes to explore each topic in the course with more depth.

0. Introduction

This is a course on red team operations and adversary simulations.

To learn more about Adversary Simulations and Red Team Operations:

- Watch Assume Breach: An Inside Look at a Cloud Security Service Provider. I'm a big believer in assume breach. This is an engagement philosophy where a red team is given access and focuses on the post-exploitation steps of a long-term embedded adversary to exercise detection and response.
- Read Microsoft's Enterprise Cloud Red Teaming whitepaper. Here they explain the "Assume Breach" philosophy and discuss how they use their red team to measure and improve time-to-detect and time-to-remediate of their security operations over time.
- Read Raphael's Magic Quadrant. Here I summarize the shifts in our industry driving the development of Adversary Simulations as a service. I write a lot about this topic and my thoughts are in the Adversary Simulations category on this blog.
- Browse the Red + Blue = PURPLE slides from 2015's FIRST Technical Colloquium in the Netherlands. Here Stan Hegt from KPMG covers Adversary Simulations vs. Penetration

Testing and goes through a case study working with a Dutch Bank.
- Read Models for Red Team Operations. There is more to red team operations than "kick down the door and seduce the security guard" type assessments. In this post I try to point out some of the different uses of red teams.

Advanced Threat Actors:

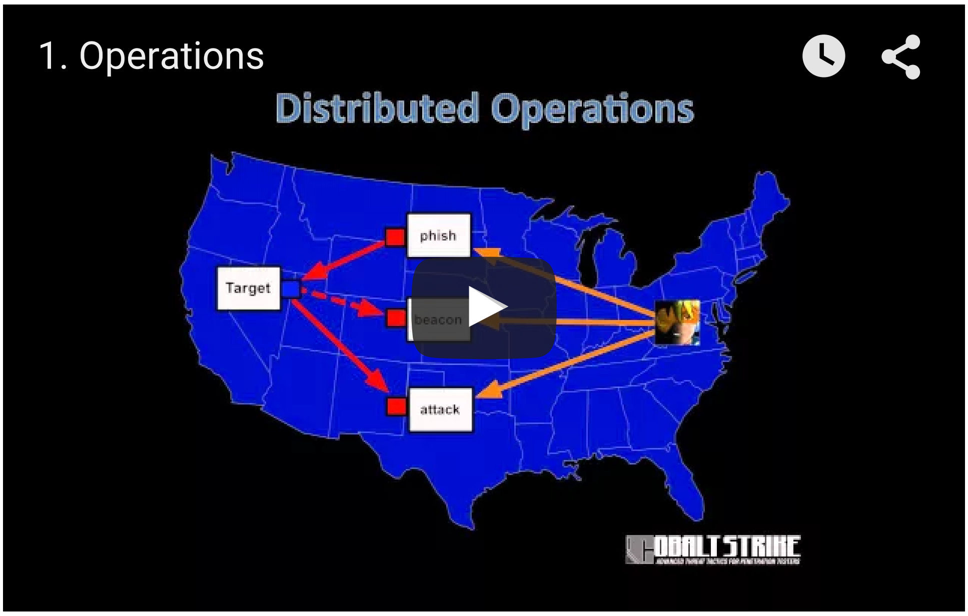
- Kiran Blanda maintains a GitHub repository with copies of public threat intelligence reports. Some companies put out material that shows their analysts know how to use IDA and take screenshots. Others provide some depth and speculate on the actor's tradecraft. I really like the reports from Kaspersky and CrowdStrike.
- Watch Michael Daly's 2009 USENIX talk, The Advanced Persistent Threat. This talk predates the marketing bonanza over APT actors and their work. This is a common sense discussion of the topic without an agenda. Even though it's from 2009, the material is spot on.

Tools used in this course:

- The primary operating platform in this course is Kali Linux 2.0.
- While Cobalt Strike 3.0 no longer depends on Rapid7's Metasploit Framework, it's still an amazing collection of capability. This course demonstrates the synergy between Cobalt Strike and the Metasploit Framework in several places.
- This course also uses PowerSploit, a powerful collection of PowerShell post-exploitation capability.
- We also take advantage of PowerView and PowerUp from the PowerShell Empire Project's PowerTools collection.
- Later on, this course demonstrates how to use the Veil Evasion Framework to generate executables that evade most anti-virus products.

1. Operations

Advanced Threat Tactics starts with a high-level overview of Cobalt Strike's model for distributed operations and red team collaboration.

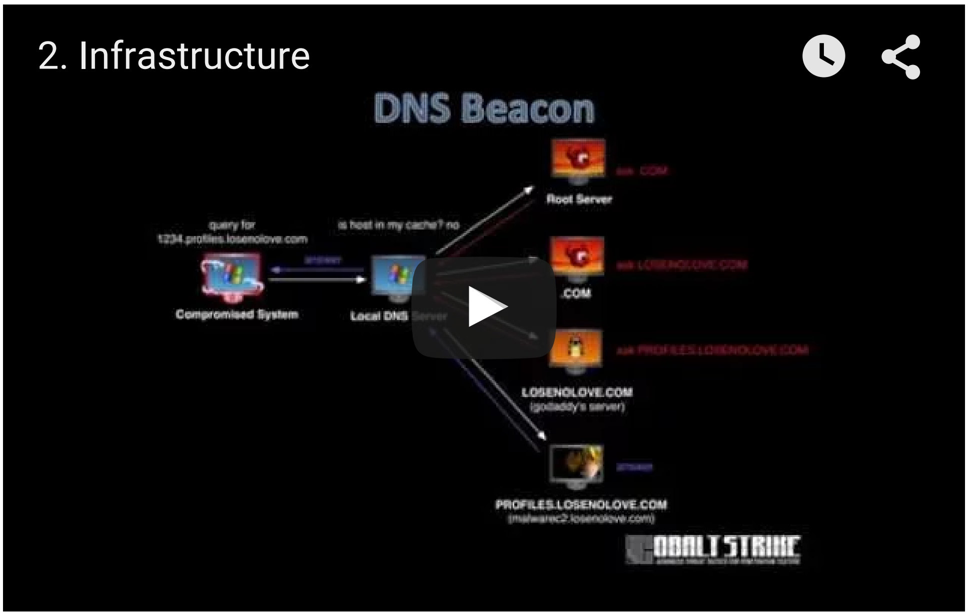


To learn more about Cobalt Strike's model for collaboration and operations:

- Watch Force Multipliers for Red Team Operations. This is my favorite talk I've given. Here, I summarize my work and insights on the red team collaboration problem. Today, I consider this a completed research project with the following blog posts capturing lessons learned on how to build infrastructure and organize a large red team to support operations (primarily in an exercise context).
- Read A Vision for Distributed Red Team Operations to learn more about Cobalt Strike's model for distributed operations with multiple team servers.
- Read The Access Management Team [Shell Sherpas]. This blog post discusses the Access Manager role in depth.
- Read about The Post Exploitation Team. These are my notes on the folks who interact with targets to complete objectives and find interesting information.
- Read Infrastructure for Red Team Operations. Infrastructure is the foundation of any engagement. This post is my best practices for organizing infrastructure to support a long-term op with multiple targets.

2. Infrastructure

Infrastructure is the collection of domains, servers, and software that support your operation. One of Cobalt Strike's strengths is its variety of communication channels and the flexibility you have to configure them. This lecture goes through the HTTP/HTTPS, DNS, and named pipe channels and shows you how to use special features with each. I also take you through how to stand up redirectors and test your infrastructure before an engagement.



To learn more about payload staging:

- Read OJ Reeve's Deep Dive into Stageless Meterpreter Payloads on the Metasploit blog. This post provides depth on the staging process for Meterpreter and explains stageless Meterpreter payloads.
- I also wrote Staged Payloads – What Penetration Testers Should Know. These are my thoughts on the subject if any of the above is unclear. 🙂 Understanding staging is very important to understand the behavior and design decisions in tools like Cobalt Strike.

Beacon Communication:

- Read Cloud-based Redirectors for Distributed Hacking. This post describes redirectors, why you would want to use them, and how to set them up with socat. Very similar to the model discussed in this course.
- Read How to use a Valid SSL certificate with the HTTPS Beacon.
- The introduction of the DNS data channels in Cobalt Strike led to several folks claiming, That'll never work–we don't allow port 53 out. This post calmly answers these claims with an explanation of how the DNS Beacon communicates.
- DNS Communication is a pain in the rear to get right. Ron Bowes (author of DnsCat 2) goes through his lessons learned in the Secrets of DNS talk from DerbyCon 2014. His blog at skullsecurity.org is worth a read as well.
- Read Stealthy Peer-to-peer C&C over SMB pipes. I added a named pipe channel to Cobalt Strike in late-2013. This feature wasn't well understood, so I wrote this blog post to explain it better.

3. Targeted Attacks

This lecture goes through a process to execute a targeted spear phishing attack to get a foothold in a modern enterprise.

3. Targeted Attacks
MORNING CATCH PHISHING INDUSTRIES
"There's plenty of ~~suckers~~ fish in the sea."

To learn more about this material:

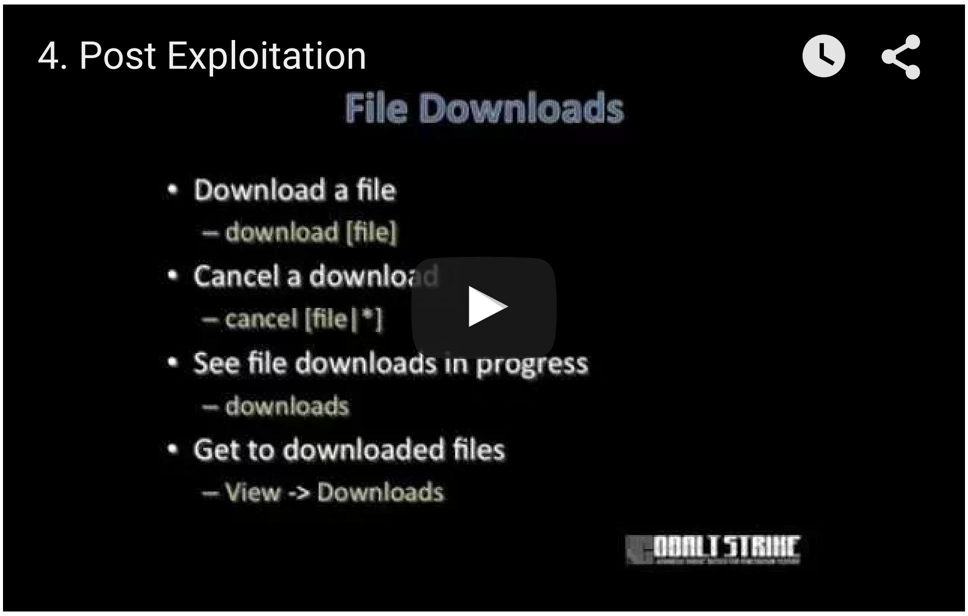
- Read What's the go to phishing technique or exploit? This blog post summarizes the process I use to get a foothold in a modern enterprise.
- Read the MetaPhish paper and watch the MetaPhish presentation. This talk greatly influenced my work.
- Go deeper with the System Profiler in phishing system profiles without phone calls.
- Go to BrowerSpy.dk to learn which information your browser tells others about you.

User-Driven Attacks:

- Read User-driven Attacks. This blog post details the user-driven attacks available in Cobalt Strike 2.5. Most made it over to 3.0. 🙂
- Read about why Cobalt Strike exposes x86 payloads over x64 payloads. There's a valid(?) reason behind it.
- The Microsoft Office Macro is one of my favorite user-driven attacks. Matt Weeks' has a great blog post on Direct Shellcode Execution in MS Office Macros.
- Watch the Java Applet Code Signing Tutorial to learn how to extend the life of Cobalt Strike's Signed Applet Attack. The Java Applet attack was popular for a long time. January 2014 really changed things for this attack. Obituary for the Java Signed Applet Attack provides some details on this.

4. Post Exploitation

This lecture shows how to use Beacon for post-exploitation. If you have to operate with Beacon, this is good core material to know.



4. Post Exploitation

File Downloads

- Download a file
  - download [file]
- Cancel a download
  - cancel [file|*]
- See file downloads in progress
  - downloads
- Get to downloaded files
  - View -> Downloads

To learn more about this material:

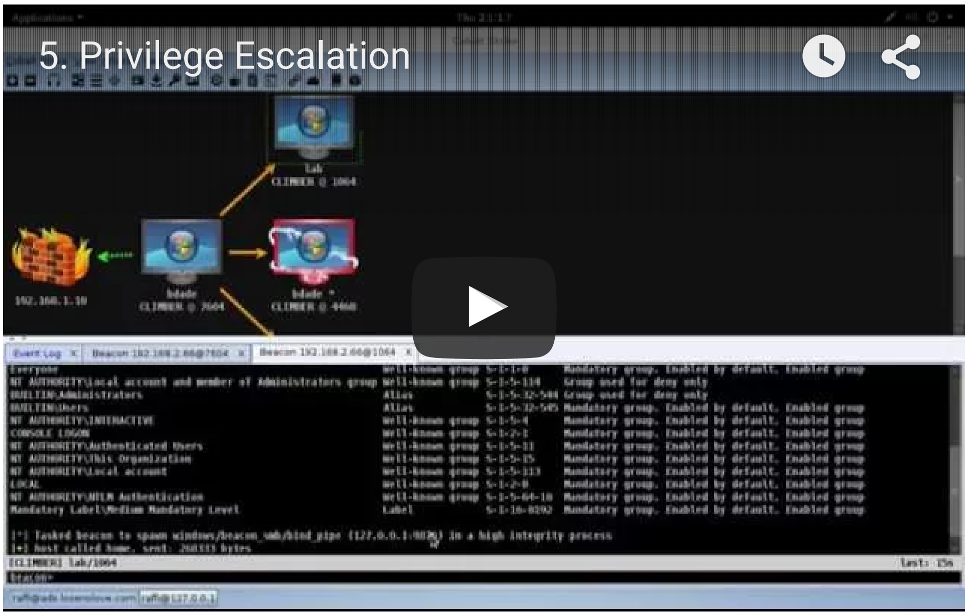
- Read Evolution of a Modern Hacking Payload. Beacon started life as an asynchronous lifeline to spawn Meterpreter sessions as needed. Over time Beacon gained features to allow an operator to use Beacon when Meterpreter was not an option. This post tells that story.
- Read Beacon: An Operator's Guide. This post discusses the concepts to know when using Beacon.
- Browser Pivoting is a Cobalt Strike technique for man-in-the-browser session stealing with Internet Explorer. I wrote about this technique previously and presented it at DerbyCon 2013.

Post-Exploitation:

- Buy the Red Team Field Manual. This is a must-own for anyone working in this space. The tips and tricks here are quite applicable for all Beacon operators.

5. Privilege Escalation

Think of this lecture as post exploitation, part 2. We dive into how to elevate privileges and use these privileges to harvest credentials and password hashes.



```
Everyone                                                     Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114    Group used for deny only
BUILTIN\Administrators                                       Alias            S-1-5-32-544 Group used for deny only
BUILTIN\Users                                                Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                                     Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                                                Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users                             Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization                               Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                                   Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                                        Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication                             Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level                       Label            S-1-16-8192  Mandatory group, Enabled by default, Enabled group

[*] Tasked beacon to spawn windows/beacon_smb/bind_pipe (127.0.0.1:[illegible]) in a high integrity process
[+] host called home, sent: 268333 bytes
[CLIMBER] lab/1064                                                                                                         last: 15s
beacon>
```

To learn more about User Account Control and the Bypass UAC attack:

- Read User Account Control — What Penetration Tester's Should Know. This blog post dives deep into user account control and different methods to elevate from a medium integrity context to a high integrity context.
- Read Windows 7 UAC Whitelist: Code-injection Issue (and more) by Leo Davidson. This is the original reference on the UAC bypass attack.

Privilege Escalation:

- Read Windows Privilege Escalation Fundamentals. This tutorial has a number of command-line recipes to find files with credentials and other things you should look for when trying to elevate your rights.
- Read What you know about 'bout GPP? This blog post offers a look at the Group Policy Preferences privilege escalation vector. This is one of those issues that, while patched, remains an issue because the patch does not cleanup the problems created by this feature when it was last used. I didn't have time to cover this problem in the course [six hours is enough!]; but this is a staple thing you should always check for.

PowerUp:

- Read PowerUp: A Usage Guide by its author Will Schroeder. This blog post will give you some ideas of other things PowerUp can do. Will's presentation PowerUp – Automating Windows Privilege Escalation is worth a quick flip through as well.
- Also read, Utilizing PowerUp.ps1 to Escalate Privileges on Windows 7 using an Unquoted Path Vulnerability. This blog post is a look at another one of PowerUp's elevation vectors.

Mimikatz:

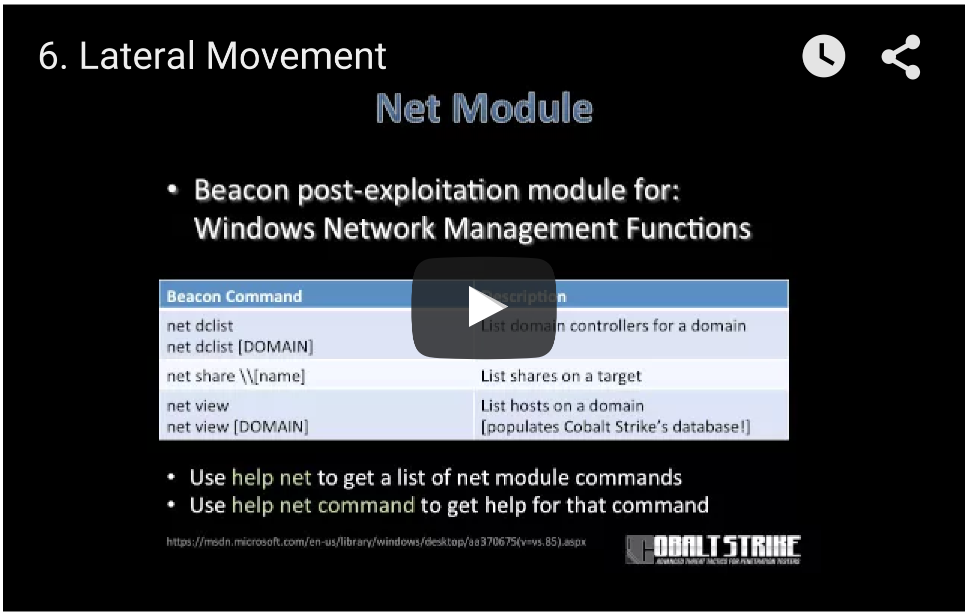
- Study the Mimikatz Wiki to start your journey understanding what this tool can do. To get the most from mimikatz, you'll really need to read its source code to really understand a feature.
- Read Attackers Can Now Use Mimikatz to Implant Skeleton Key on Domain Controllers & BackDoor Your Active Directory Forest by Sean Metcalf. This post describes the mimikatz command **misc::skeleton** which applies an in-memory patch on a DC to allow a second password to work for any user in the domain. This is an advanced threat tactic described

by Dell Secureworks CTU in their Skeleton Key Malware Analysis paper.

- Sean Metcalf regularly blogs about Mimikatz at adsecurity.org. I recommend spending an afternoon to go through each of his posts on mimikatz.

6. Lateral Movement

This lecture is the use and abuse of native Windows capability and behavior to trade-up privileges and move around a network.



6. Lateral Movement

Net Module

- Beacon post-exploitation module for: Windows Network Management Functions

Beacon Command	Description
net dclist net dclist [DOMAIN]	List domain controllers for a domain
net share \\[name]	List shares on a target
net view net view [DOMAIN]	List hosts on a domain [populates Cobalt Strike's database!]

- Use help net to get a list of net module commands
- Use help net command to get help for that command

https://msdn.microsoft.com/en-us/library/windows/desktop/aa370675(v=vs.85).aspx

To learn more about enumeration and reconnaissance in a Windows Active Directory network:

- Watch Passing the Torch: Old School Red Teaming, New School Tactics? Here David McGuire and Will Schroeder go through their tricks to understand a Windows enterprise network the old school way (net view /DOMAIN and friends) vs. the new school way (with PowerShell).
- Read PowerView: A Usage Guide to understand this wonderful tool from Will Schroeder to automate enumerating trusts, users, and hosts in an active directory environment.
- Check out Netview by Rob Fuller. This tool enumerates systems using the Win32 Network Management API. I believe it was one of the original inspirations for PowerView and it certainly inspired Beacon's net module as well.
- Read Trusts You Might Have Missed by Will Schroeder for a quick primer on domain trusts in Windows Active Directory networks. You'll really want to go through all of Will's blog to understand this topic fully. He posts a lot about domain trusts and user hunting. Too much for me to keep up with here.
- Also, read I Hunt Sys Admins by Will Schroeder (him, again!) to learn different ways to find where a particular user lives on the network. This is important for targeting systems that may have trust material that gets you closer to the data you want or to DA rights on the network.

Remote Management without Malware:

- Read WinRM is my Remote Access Tool to learn about how to use WinRM to control a remote system from Beacon.
- pHEAR the Invoke-WmiCommand cmdlet added to PowerSploit by Matt Graeber. This cmdlet uses WMI as a C2 channel to post commands AND get output back.
- Read Malware Free Intrusions: Adversary Tricks and Treats on the CrowdStrike blog. This post goes over how the actor, Deep Panda, uses wmic to enable a backdoor that allows them to access a SYSTEM-level shell via RDP.

Pass-the-Hash:

- Read How to Pass-the-Hash with Mimikatz. This blog post documents how to use mimikatz to pass-the-hash from Beacon
- Read Pass-the-Hash is Dead: Long Live Pass-the-Hash by Will Schroeder. This blog post covers the May 2014 patch to Windows that puts restrictions around pass-the-hash.

Kerberos:

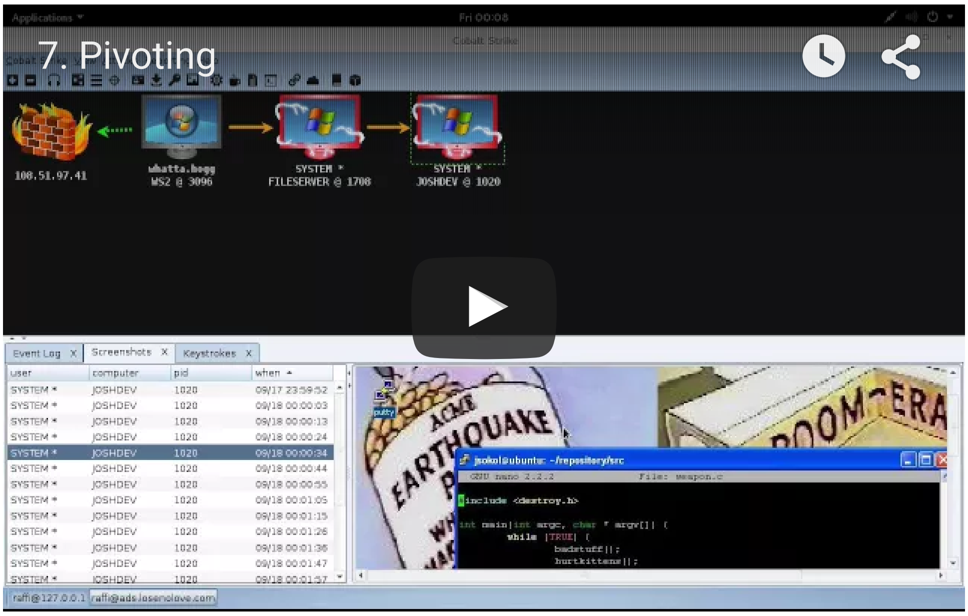
- Read Detecting Forged Kerberos Ticket (Golden Ticket & Silver Ticket) Use in Active Directory by Sean Metcalf. This blog post provides an overview of how Kerberos works, the Golden Ticket, the Silver Ticket, and ms14-068.
- Watch The Secret Life of Krbtgt by Chris Campbell to understand the Golden Ticket and its significance.
- Read MS14-068 to DA by the mysterious idzer0. This one was patched awhile ago, but I had fun with it a few times. This exploit was an immediate elevation to DA. This blog post uses the Python Kerberos Exploitation Kit to kick off the attack. MWR InfoSecurity has a good write-up on this attack on their blog too. *nudge* *nudge* Beacon has a **kerberos_ccache_use** command now.

Remote Code Execution:

- Read Authenticated Remote Code Execution in Windows by Matt Weeks for more ways to schedule or run a process on a remote system.
- Read Covert Lateral Movement with High-Latency C&C to see my recipes for (manual) lateral movement with Beacon.
- Read Phishing, Lateral Movement, SCADA, Oh My! by idzer0 goes through a case study of using SMB Beacon, PowerView, and WMI to pivot five levels deep and reach a SCADA controller.
- Watch Lateral Movement given by Harlan Carvey at B-Sides Cincinnati. This talk describes several manual methods for lateral movement and indicators they leave behind.

7. Pivoting

SOCKS, SOCKS, SOCKS! This lecture is about how to pivot with Beacon. You could also think about it as using and abusing SOCKS forwards, backwards, and any other way you want it.



user	computer	pid	when
SYSTEM *	JOSHDEV	1020	09/17 23:59:52
SYSTEM *	JOSHDEV	1020	09/18 00:00:03
SYSTEM *	JOSHDEV	1020	09/18 00:00:13
SYSTEM *	JOSHDEV	1020	09/18 00:00:24
SYSTEM *	JOSHDEV	1020	09/18 00:00:34
SYSTEM *	JOSHDEV	1020	09/18 00:00:44
SYSTEM *	JOSHDEV	1020	09/18 00:00:55
SYSTEM *	JOSHDEV	1020	09/18 00:01:05
SYSTEM *	JOSHDEV	1020	09/18 00:01:15
SYSTEM *	JOSHDEV	1020	09/18 00:01:26
SYSTEM *	JOSHDEV	1020	09/18 00:01:36
SYSTEM *	JOSHDEV	1020	09/18 00:01:47
SYSTEM *	JOSHDEV	1020	09/18 00:01:57

jsokol@ubuntu: ~/repository/src

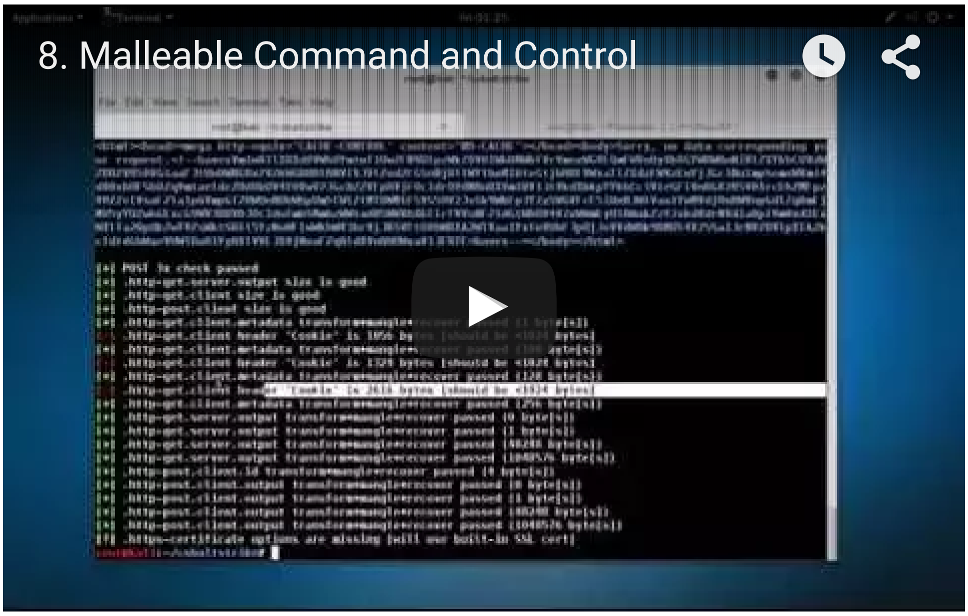
```
  GNU nano 2.2.2                File: weapon.c

#include <destroy.h>

int main(int argc, char * argv[]) {
        while (TRUE) {
                badstuff();
                hurtkittens();
```

More on this topic:

- Read the SOCKS protocol specification. SOCKS is a simple (1 page) protocol that allows a SOCKS-aware application to connect to a SOCKS server and ask that server to initiate a connection on the client's behalf.
- Read Pivoting through SSH. This blog post describes the Proxies option in the Metasploit Framework.
- Read Hacking through a Straw: Pivoting over DNS. This post talks about the SOCKS pivoting capability in Beacon.
- Take a look at Cobalt Strike's VPN Pivoting feature. I don't talk about it much, because I don't use it often. If you'd like to learn about layer-2 pivoting, I wrote a blog post on how this technology works with source code. It's simpler than you might think.

8. Malleable C2

Malleable C2 is Cobalt Strike's domain specific language to change indicators in the Beacon payload. This ability to make Beacon look like other malware is arguably what makes it a threat emulation tool.



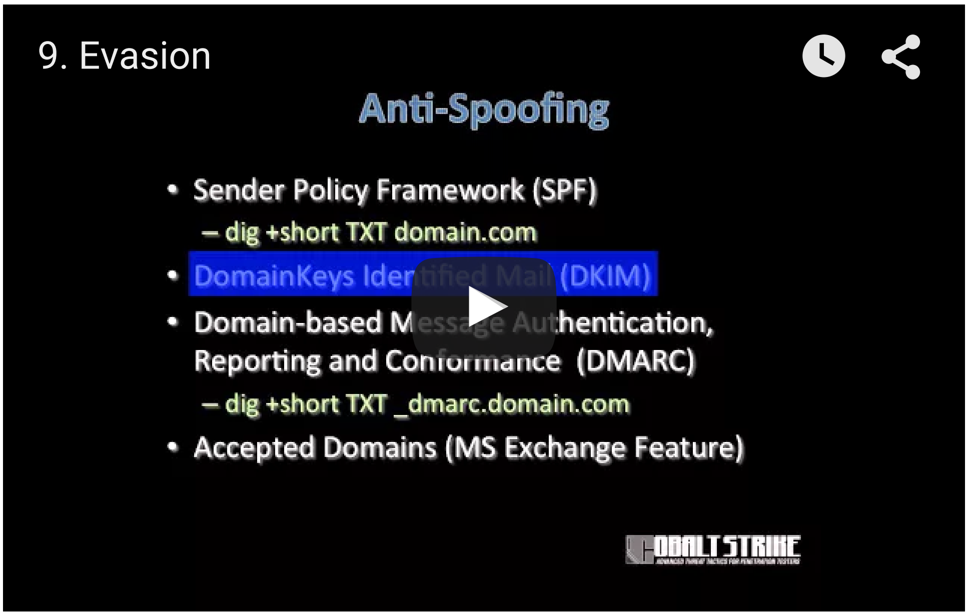
```
[illegible]

[+] POST 3x check passed
[+] .http-get.server.output size is good
[+] .http-get.client size is good
[+] .http-post.client size is good
[+] .http-get.client.metadata transform+mangle+recover passed (1 byte[s])
[!] .http-get.client header 'Cookie' is 1056 bytes (should be <1024 bytes)
[+] .http-get.client.metadata transform+mangle+recover passed (100 byte[s])
[!] .http-get.client header 'Cookie' is 1329 bytes (should be <1024 bytes)
[+] .http-get.client.metadata transform+mangle+recover passed (128 byte[s])
[!] .http-get.client header 'Cookie' is 2616 bytes (should be <1024 bytes)
[+] .http-get.client.metadata transform+mangle+recover passed (256 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (0 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (1 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (48248 byte[s])
[+] .http-get.server.output transform+mangle+recover passed (1048576 byte[s])
[+] .http-post.client.id transform+mangle+recover passed (4 byte[s])
[+] .http-post.client.output transform+mangle+recover passed (0 byte[s])
[+] .http-post.client.output transform+mangle+recover passed (1 byte[s])
[+] .http-post.client.output transform+mangle+recover passed (48248 byte[s])
[+] .http-post.client.output transform+mangle+recover passed (1048576 byte[s])
[!] .https-certificate options are missing [will use built-in SSL cert]
root@kali:~/cobaltstrike# 
```

More on this topic:

- Go to the Malleable C2 Profiles collection on Github. These are example profiles you may use as-is or as a base to build your own profiles.
- Read the Malleable C2 documentation. There's no substitute for reading the documentation on this feature. The documentation will take you through all of the concepts in this video.
- Watch the Puttering my Panda and Other Threat Replication Case Studies videos. These three case studies show how to use Cobalt Strike and Malleable C2 to emulate various advanced threat actors.

9. Evasion

The Advanced Threat Tactics course concludes with a deep dive into evasion. This video is my to-the-minute notes on this topic.



Anti-Spoofing

- Sender Policy Framework (SPF)
  - – dig +short TXT domain.com
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)
  - – dig +short TXT _dmarc.domain.com
- Accepted Domains (MS Exchange Feature)

To learn more about phishing and e-mail delivery:

- Read E-mail Delivery – What Penetration Testers Should Know. This is a long blog post on the inner workings of email, SPF, DKIM, and DMARC.

- Read SPF, DKIM, and DMARC Demystified by McAfee. This whitepaper summarizes the why and what of these technologies.
- Watch Spoof my SMTP from This Week in Enterprise Tech, Episode 71. Here, I practice what I preach, and show how to deliver a carefully crafted phish to a webmail account I setup for testing purposes.

Anti-virus evasion:

- Read Facts and myths about antivirus evasion with Metasploit by Michael Schierl.
- Read the Artifact Kit documentation. This is Cobalt Strike's source code framework to build executables and DLLs to get past some anti-virus products.

Application Whitelisting:

- Watch Simple Application Whitelisting Evasion by Casey Smith. Casey is constantly dropping whitelist evasion knowledge on Twitter. I also recommend reading his blog for more on this topic as well.
- Read How to Inject Shellcode from Java. This blog post details how Cobalt Strike's default applet attacks inject shellcode into memory from Java.

Egress Restrictions:

- Read An Unnecessary Addiction to DNS Communication. I often hear from folks who insist that DNS is the only way out of their network and the only way to reach servers that are otherwise isolated from the network. This post goes into depth on the evasion options with Cobalt Strike's DNS communication scheme and it digs into the capability available in Cobalt Strike's other Beacon variants.
- Read HTTP Proxy Authentication for Malware to understand how Beacon's HTTP/S stagers react to proxy authentication failures.

Active Defenders:

- Watch Operating in the Shadows given by Carlos Perez at DerbyCon 2015. In this talk, Carlos goes over the different advancements in blue's ability to instrument Windows and the impact it will have on red teams and penetration testers who need to challenge them. This is a sign of things to come.
- Read Advances in Scripting Security and Protection in Windows 10 and PowerShell V5. Windows 10 will change the security game in a big way. This post from Microsoft goes through the new logging hooks to understand PowerShell activity on a system and the hooks that allow anti-virus engines to look for malicious PowerShell.
- Take a look at Microsoft's Advanced Threat Analytics technology. This defense tracks which systems/users pull which active directory objects, when, and how often. It's designed to catch that awesome stuff discussed in part 6 of this course.
- Also, check out UpRoot, an agentless host-based IDS written in PowerShell that leverages WMI subscriptions. UpRoot reports process creates, new network connections, and other host activity. Tools like UpRoot show the scrutiny red operators will need to learn to cope with when working with a mature hunt team.

Posted in Cobalt Strike, Red Team |

ḡ Follow

Follow “Strategic Cyber LLC”