Things That Can Kill You

- Old Systems
- Please, please ask about this in the RoE/Scope Meeting
- "So, any systems from 2008 we should know about?"
- "What are the top five systems that keep going down?"
- "Have other tests ever crashed something?"
- Document

Random Testing Thought: Compliance Mapping

- You will be asked to map your findings to a compliance framework
- Do not panic.
- Just raise the rate by 10% and use CIS
- Seriously

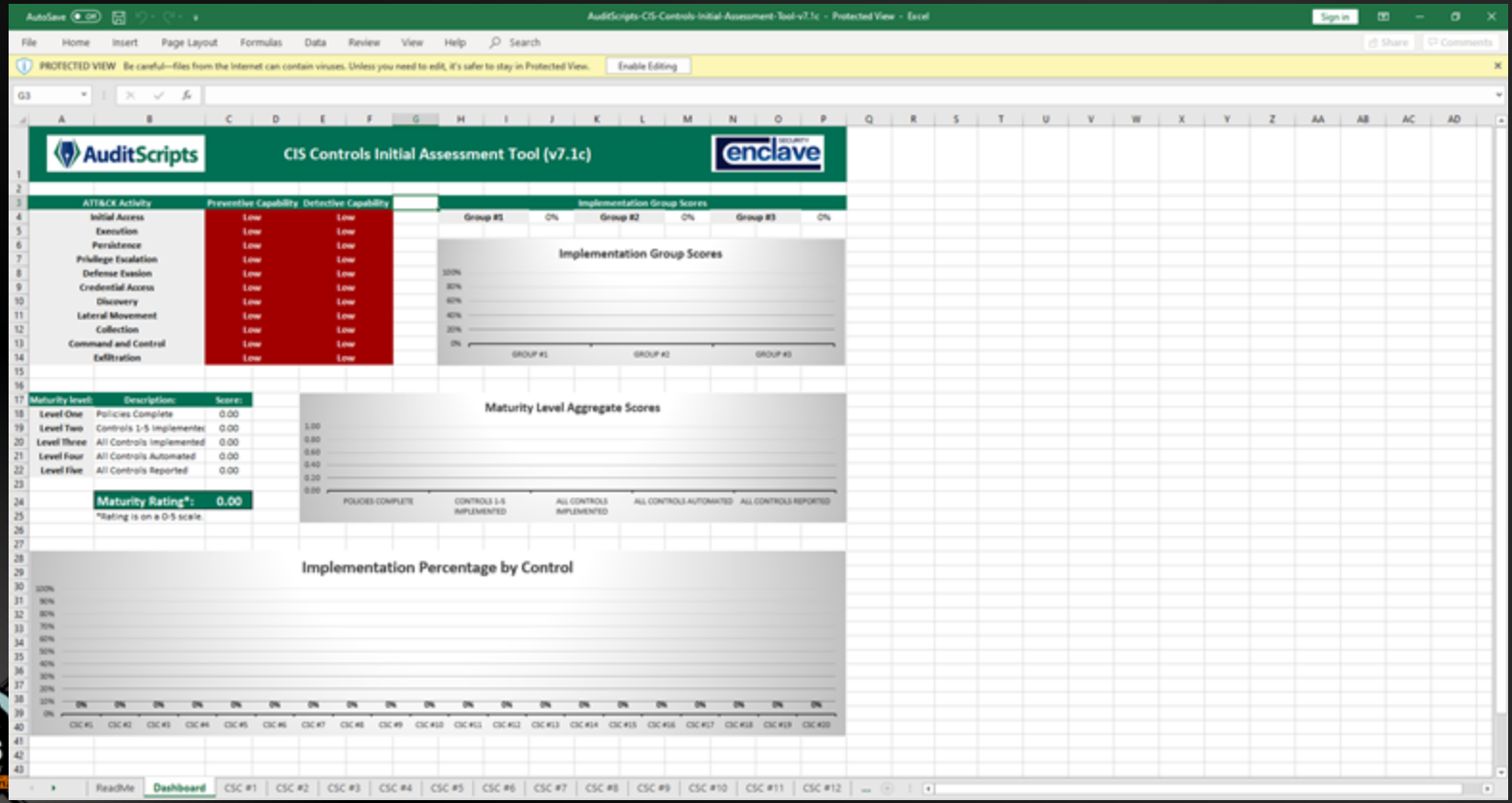
Compliance Issues

- Far too many frameworks
- Overlapping and conflicting recommendations
- Recommendations get out of date quickly
- NIST Greenbook
- PCI Min Password length
- Meeting the Minimum

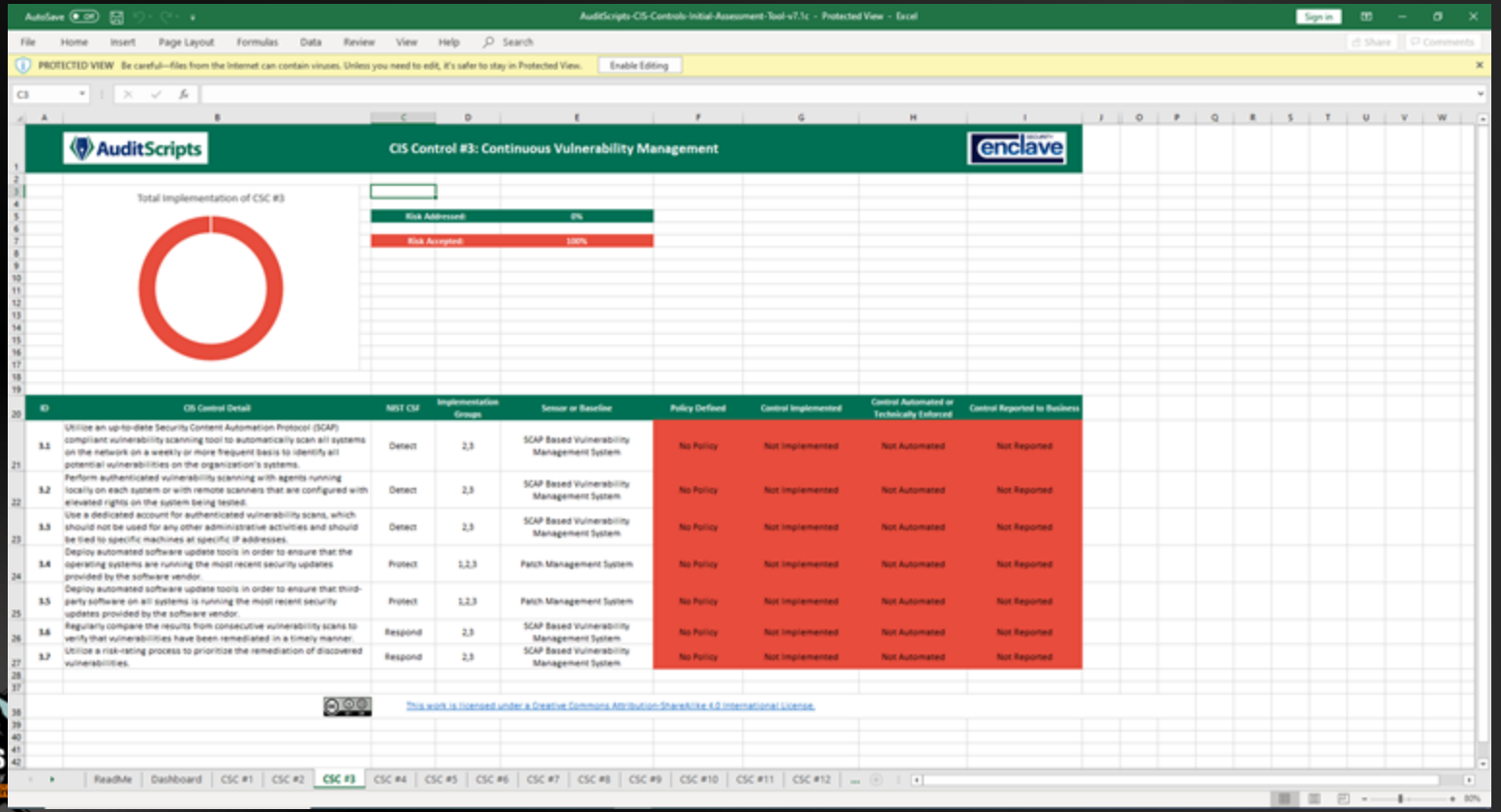
AuditScripts Spreadsheets

- Create a smaller framework set
- Create a framework based on actual attacks and things that matter
- Create a cross-reference to other frameworks
- Differing levels of compliance
- Dynamic meant to be updated regularly
- History and Future
- Heavy lifting by James and Kellie Tarala
- https://www.auditscripts.com/free-resources/critical-security-controls/

AuditScripts Spreadsheets



AuditScripts Spreadsheets



AutoSave OFF — AuditScripts-CIS-Controls-Initial-Assessment-Tool-v7.1c - Protected View - Excel

File Home Insert Page Layout Formulas Data Review View Help Search

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

AuditScripts

CIS Control #3: Continuous Vulnerability Management

enclave

Total Implementation of CSC #3

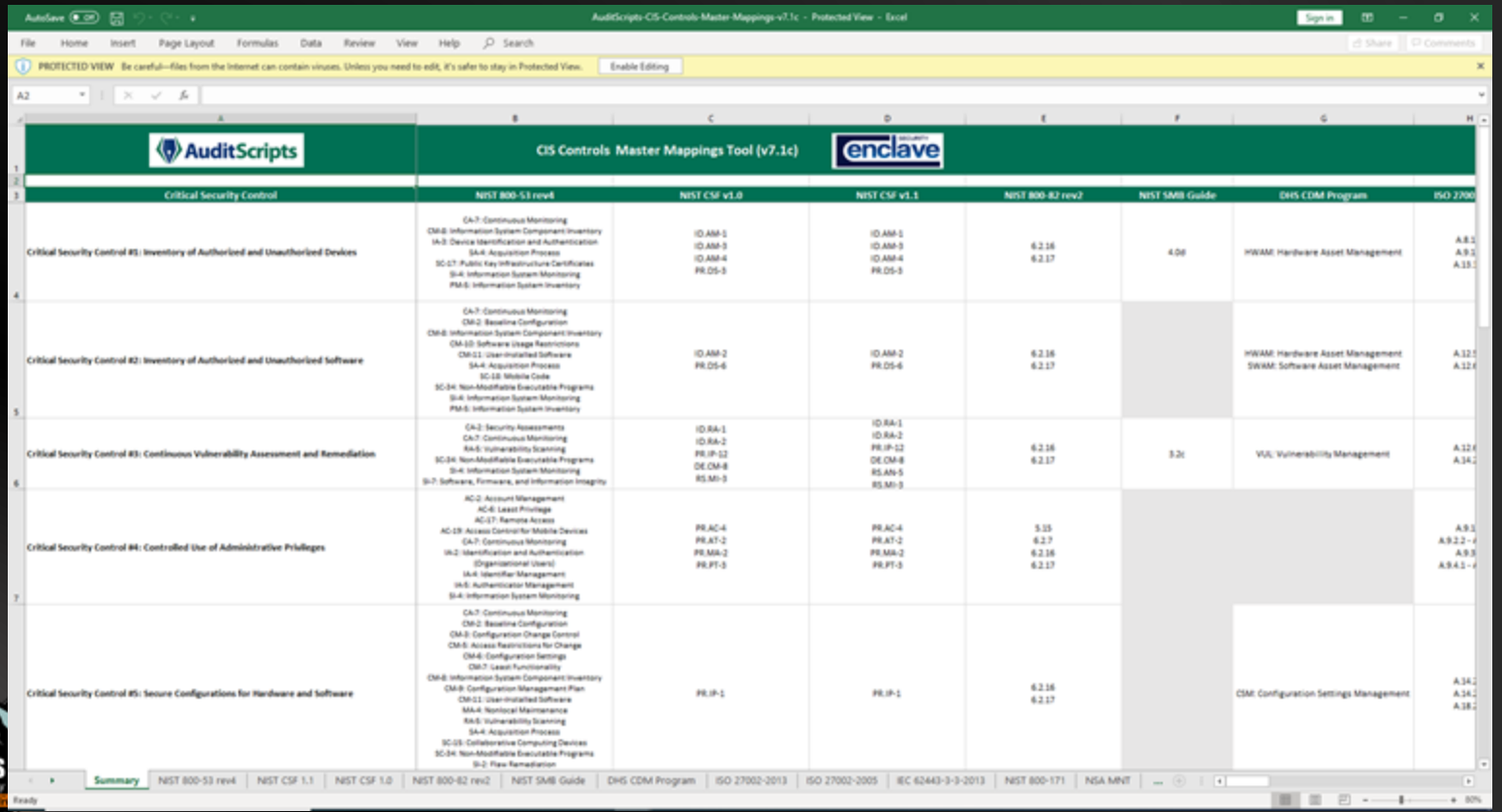
Risk Addressed:	0%
Risk Accepted:	100%

ID	CIS Control Detail	NIST CSF	Implementation Groups	Sensor or Baseline	Policy Defined	Control Implemented	Control Automated or Technically Enforced	Control Reported to Business
3.1	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	Detect	2,3	SCAP Based Vulnerability Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.2	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	Detect	2,3	SCAP Based Vulnerability Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.3	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	Detect	2,3	SCAP Based Vulnerability Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.4	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	Protect	1,2,3	Patch Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.5	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	Protect	1,2,3	Patch Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.6	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	Respond	2,3	SCAP Based Vulnerability Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.7	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	Respond	2,3	SCAP Based Vulnerability Management System	No Policy	Not Implemented	Not Automated	Not Reported

ReadMe | Dashboard | CSC #1 | CSC #2 | CSC #3 | CSC #4 | CSC #5 | CSC #6 | CSC #7 | CSC #8 | CSC #9 | CSC #10 | CSC #11 | CSC #12

BLACK HILLS Information Security CELEBRATING 10 YEARS ★2008-2018★

AuditScripts Spreadsheets



AutoSave — AuditScripts-CIS-Controls-Master-Mappings-v7.1c - Protected View - Excel

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

AuditScripts — CIS Controls Master Mappings Tool (v7.1c) — enclave

Critical Security Control	NIST 800-53 rev4	NIST CSF v1.0	NIST CSF v1.1	NIST 800-82 rev2	NIST SMB Guide	DHS CDM Program	ISO 2700
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices	CA-7: Continuous Monitoring CM-8: Information System Component Inventory IA-3: Device Identification and Authentication SA-4: Acquisition Process SC-17: Public Key Infrastructure Certificates SI-4: Information System Monitoring PM-5: Information System Inventory	ID.AM-1 ID.AM-3 ID.AM-4 PR.DS-3	ID.AM-1 ID.AM-3 ID.AM-4 PR.DS-3	6.2.16 6.2.17	4.04	HWAM: Hardware Asset Management	A.8.1 A.9.1 A.13.1
Critical Security Control #2: Inventory of Authorized and Unauthorized Software	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-8: Information System Component Inventory CM-10: Software Usage Restrictions CM-11: User-Installed Software SA-4: Acquisition Process SC-18: Mobile Code SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring PM-5: Information System Inventory	ID.AM-2 PR.DS-6	ID.AM-2 PR.DS-6	6.2.16 6.2.17		HWAM: Hardware Asset Management SWAM: Software Asset Management	A.12.5 A.12.6
Critical Security Control #3: Continuous Vulnerability Assessment and Remediation	CA-2: Security Assessments CA-7: Continuous Monitoring RA-5: Vulnerability Scanning SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring SI-7: Software, Firmware, and Information Integrity	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.MI-3	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.AN-5 RS.MI-3	6.2.16 6.2.17	3.2c	VUL: Vulnerability Management	A.12.6 A.14.2
Critical Security Control #4: Controlled Use of Administrative Privileges	AC-2: Account Management AC-6: Least Privilege AC-17: Remote Access AC-19: Access Control for Mobile Devices CA-7: Continuous Monitoring IA-2: Identification and Authentication (Organizational Users) IA-4: Identifier Management IA-5: Authenticator Management SI-4: Information System Monitoring	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3	5.15 6.2.7 6.2.16 6.2.17			A.9.1 A.9.2.2 - A A.9.3 A.9.4.1 - A
Critical Security Control #5: Secure Configurations for Hardware and Software	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-7: Least Functionality CM-8: Information System Component Inventory CM-9: Configuration Management Plan CM-11: User-Installed Software MA-4: Nonlocal Maintenance RA-5: Vulnerability Scanning SA-4: Acquisition Process SC-15: Collaborative Computing Devices SC-34: Non-Modifiable Executable Programs SI-2: Flaw Remediation	PR.IP-1	PR.IP-1	6.2.16 6.2.17		CSM: Configuration Settings Management	A.14.2 A.14.2 A.18.2

Summary | NIST 800-53 rev4 | NIST CSF 1.1 | NIST CSF 1.0 | NIST 800-82 rev2 | NIST SMB Guide | DHS CDM Program | ISO 27002-2013 | ISO 27002-2005 | IEC 62443-3-3-2013 | NIST 800-171 | NSA MNT

Ready

BLACK HILLS Information Security — CELEBRATING 10 YEARS — 2008-2018

To the Future!

AuditScripts

Security Control Category Coverage Analysis (v1.0g)

Security Control Category	Common Control Count	CIS Control (v7.1) Count	NIST CSF (v1.1) Count	NIST CSF (v1.0) Count	ISO 27002:2013 Count	NIST 800-171 Count	NIST Privacy (v1.0)
Security Program Governance	60	17%	32%	30%	25%	8%	28%
Auditing and Reporting	53	15%	15%	6%	21%	8%	11%
Security Program Operations	38	21%	95%	95%	87%	34%	45%
Asset Inventory and Control	18	94%	17%	17%	22%	22%	22%
System Protection	55	76%	20%	20%	7%	38%	11%
System Monitoring	23	65%	30%	30%	22%	57%	30%
Identity and Access Management	51	41%	25%	22%	43%	67%	37%
Network Device Protection	7	71%	14%	0%	0%	0%	0%
Boundary Protection	35	63%	11%	11%	6%	29%	6%
Internal Network Protection	16	94%	19%	19%	25%	25%	19%
Secure Software Development	18	44%	17%	11%	72%	0%	17%
Data Privacy	15	0%	0%	0%	0%	7%	107%

To the Future!

AuditScripts

Common Control Library (v1.0g)

Control Reference ID #	Control Description	CIS Control (v7.1)	NIST CSF (v1.1)	NIST CSF (v1.0)	ISO 27002:2013	NIST 800-171	NIST Privacy (v1.0)	Australian DSD35	CMMC (v1)
GOV-01	Create an information assurance charter that articulates the organization's commitment to data protection and its goals towards the confidentiality, integrity and availability of data.		ID.BE-3 PR.DS-4 PR.PT-5	ID.BE-3 PR.DS-4	A.12.1.3 A.17.2.1		ID.BE-P2 PR.DS-P4		
GOV-02	Establish the authority of a committee to define the organization's information assurance program strategy and administer the program.								
GOV-03	Define the key stakeholders that will serve as members of the organization's information Assurance program committee.								
GOV-04	Establish that an senior executive leadership representative with authority will always be a member of this organization's committee.								
GOV-05	Define additional leadership roles and responsibilities for the organization's information security program and committee.								
GOV-06	Ensure that the organization's information security program committee is composed of key stakeholders from a cross-section of the organization, not simply technology workforce members.		ID.RM-1	ID.RM-1					
GOV-07	Ensure that the organization's information assurance program charter defines the organization's approach to addressing cyber security risk.		ID.RM-1 ID.RM-2 ID.RM-3 ID.GV-4 ID.RA-4	ID.RM-1 ID.RM-2 ID.RM-3 ID.GV-4 ID.RA-4			ID.DE-P1 GV.PO-P6 GV.RM-P1 GV.RM-P2 GV.RM-P3		
GOV-08	Ensure that the organization's information assurance program charter defines the specific regulatory requirements, contractual requirements, and standards that the organization's assurance program shall achieve.		ID.BE-2 ID.GV-3 ID.RM-3	ID.BE-2 ID.GV-3 ID.RM-3	A.18.1.1 A.18.1.2		GV.PO-P5		

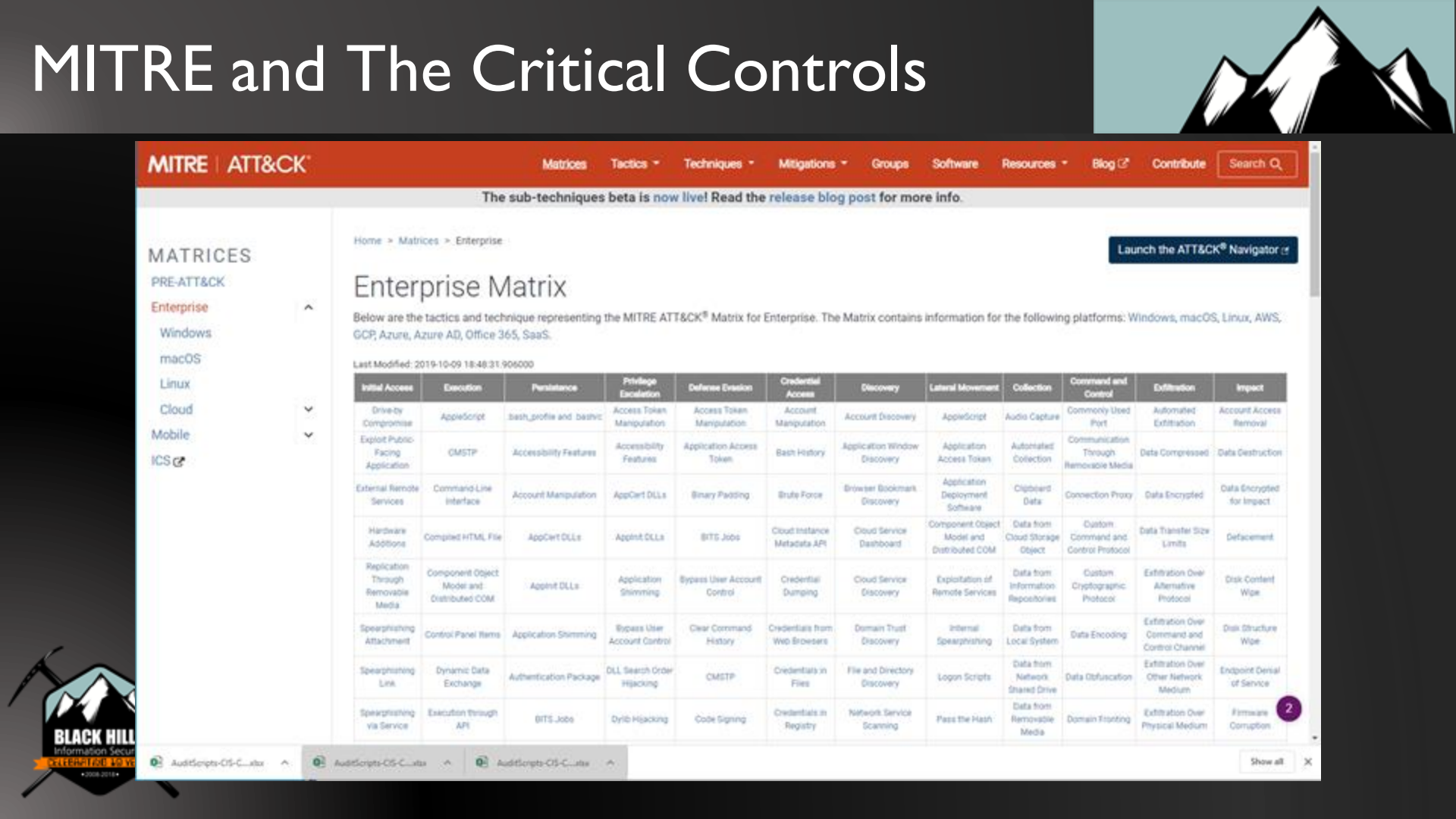
To the Future!

AuditScripts

Security Control System Coverage Analysis (v1.0g)

Governance and Operations Controls	Common Control Count	CIS Control (v7.1) Count	NIST CSF (v1.1) Count	NIST CSF (v1.0) Count	ISO 27002:2013 Count	NIST 800-171 Count	NIST Privacy (v1.0)
Technical Infrastructure Controls	**Common Control Count**	**CIS Control (v7.1) Count**	**NIST CSF (v1.1) Count**	**NIST CSF (v1.0) Count**	**ISO 27002:2013 Count**	**NIST 800-171 Count**	**NIST Privacy (v1.0)**
Asset Inventory and Discovery System	6	5	2	2	2	0	4
Software Inventory and Discovery System	6	6	1	1	0	0	0
Application Control System	6	6	0	0	2	4	0
Patch Management System	3	2	0	0	0	0	0
Vulnerability Management System	9	10	5	5	0	3	2
Configuration Management System	21	14	2	2	0	6	2
Endpoint Protection System	12	8	2	2	2	5	0
Removable Media Protection System	5	3	1	1	1	6	1
Backup and Recovery System	5	5	1	1	1	1	1
Log Management System	20	14	6	6	5	13	5
File Integrity Management System	3	1	1	1	0	0	2
Identity Management System	16	10	3	1	9	13	2
Data Inventory System	12	3	4	4	3	3	9
Access Management System	10	2	5	5	9	11	6
Privileged Account Management System	13	6	1	1	1	7	2
Network Device Management System	7	5	1	0	0	0	0
Boundary Filtering System	11	11	2	2	0	3	1
Remote Access System	11	1	2	2	1	7	1
Web Filtering System	8	7	0	0	0	0	0
Email Filtering System	5	3	0	0	1	0	0
Network Segmentation and Control System	8	9	3	3	4	1	3
Wireless Access System	8	6	0	0	0	3	0

MITRE and The Critical Controls



MITRE and The Critical Controls

AuditScripts MITRE ATTACK to CIS Controls Mapping – v7.1a.xlsx — Open with

AuditScripts &CK Enterprise Techniques Mapped to the CIS Controls (v7.1a)

Category	ID	Technique Title	Technique Description	Johns call
Initial Access	T1189	Drive-by Compromise	A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:	CSC(17.0) CSC(8.0)
Initial Access	T1190	Exploit Public-Facing Application	The use of software, data, or commands to take advantage of a weakness in an internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), and any other applications with Internet accessible open sockets, such as web servers and related services. Depending on the flaw being exploited this may include Exploitation for Defense Evasion.	CSC(3.0) CSC(18.0)
Initial Access	T1200	Hardware Additions	Computer accessories, computers, or networking hardware may be introduced into a system as a vector to gain execution. While public references of usage by APT groups are scarce, many penetration testers leverage hardware additions for initial access. Commercial and open source products are leveraged with capabilities such as passive network tapping, man-in-the-middle encryption breaking, Leystroke injection, Kernel memory reading via DMA, adding new wireless access to an existing network, and others.	CSC(2.0)
Initial Access	T1091	Replication Through Removable Media	Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.	CSC(8.8)
Initial Access	T1193	Spearphishing Attachment	Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.	CSC(7.0) CSC(8.8)
Initial Access	T1192	Spearphishing Link	Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.	CSC(7.0) CSC(8.8)
Initial Access	T1194	Spearphishing via Service	Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels.	CSC(7.0) CSC(8.8)
Initial Access	T1195	Supply Chain Compromise	Supply chain compromise is the manipulation of products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including:	CSC(18.0)
Initial Access	T1199	Trusted Relationship	Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.	CSC(9.4)
Initial Access	T1078	Valid Accounts	Adversaries may steal the credentials of a specific user or service account using Credential Access techniques or capture credentials earlier in their reconnaissance process through social engineering for means of gaining Initial Access.	CSC(6.0)
Execution	T1155	AppleScript	macOS and OS X applications send AppleEvent messages to each other for interprocess communications (IPC). These messages can be easily scripted with AppleScript for local or remote IPC. Osascript executes AppleScript and any other Open Scripting Architecture (OSA) language scripts. A list of OSA languages installed on a system can be found by using the osalang program.	CSC(5.0) CSC(8.8)

Password Cracking

- Hashcat is king
- Get some GPUs
- Yes. Bigger is better
- More GPUs better cracking
- However, having multiple rigs is also very important
- Cthulhu <- Big
- Squidward, cuttlefish <- Small
- Take old cards and build small crackers

Hashcat

Hash Types (-m)

RAW HASH	
900	MD4
0	MD5
5100	Half MD5
100	SHA1
1300	SHA-224
1400	SHA-256
10800	SHA-384
1700	SHA-512
5000	SHA-3 (Keccak)
600	BLAKE2b-512
10100	SipHash
6000	RIPEMD-160
6100	Whirlpool
6900	GOST R 34.11-94
11700	GOST R 34.11-2012 (Streebog) 256-bit
11800	GOST R 34.11-2012 (Streebog) 512-bit
RAW HASH + SALT / ITERATION **	
10	md5($pass.$salt)
20	md5($salt.$pass)
30	md5(utf16le($pass).$salt)
40	md5($salt.utf16le($pass))
3800	md5($salt.$pass.$salt)
3710	md5($salt.md5($pass))
4010	md5($salt.md5($salt.$pass))
4110	md5($salt.md5($pass.$salt))
2600	md5(md5($pass))
3910	md5(md5($pass).md5($salt))
4300	md5(strtoupper(md5($pass)))
4400	md5(sha1($pass))
110	sha1($pass.$salt)
120	sha1($salt.$pass)
130	sha1(utf16le($pass).$salt)
140	sha1($salt.utf16le($pass))
4500	sha1(sha1($pass))
4520	sha1($salt.sha1($pass))
4700	sha1(md5($pass))
4900	sha1($salt.$pass.$salt)
14400	sha1(CX)
1410	sha256($pass.$salt)
1420	sha256($salt.$pass)
1430	sha256(utf16le($pass).$salt)
1440	sha256($salt.utf16le($pass))
1710	sha512($pass.$salt)
1720	sha512($salt.$pass)
1730	sha512(utf16le($pass).$salt)
1740	sha512($salt.utf16le($pass))
***RAW HASH, AUTHENTICATED ***	
50	HMAC-MD5 (key = $pass)
60	HMAC-MD5 (key = $salt)
150	HMAC-SHA1 (key = $pass)
160	HMAC-SHA1 (key = $salt)
1450	HMAC-SHA256 (key = $pass)
1460	HMAC-SHA256 (key = $salt)
1750	HMAC-SHA512 (key = $pass)
1760	HMAC-SHA512 (key = $salt)
*** RAW CIPHER, KNOWN-ATTACK ***	
1731	**MSSQL (2012, 2014)**
200	MySQL323
300	**MySQL4.1/MySQL5**
3100	Oracle H: Type (Oracle 7+)
112	Oracle S: Type (Oracle 11+)
12300	Oracle T: Type (Oracle 12+)
8000	Sybase ASE
*** HTTP, SMTP, LDAP, FTP ***	
141	Episerver 6.x < .NET 4
1441	Episerver 6.x >= .NET 4
1600	**Apache $apr1$ MD5, md5apr1, MD5 ARP**
12600	ColdFusion 10+
1421	hMailServer
101	nsldap, SHA-1(Base64), Netscape LDAP SHA
111	nsldaps, SSHA-1(Base64), Netscape LDAP SSHA
1411	SSHA-256(Base64), LDAP {SSHA256}
1711	SSHA-512(Base64), LDAP {SSHA512}
16400	CRAM-MD5 Dovecot
15000	FileZilla Server >= 0.9.55
*** CHECKSUM ***	
11500	CRC32
*** OPERATING SYSTEMS ***	
3000	**LM**
1000	**NTLM**
1100	**Domain Cached Credentials (DCC), MS Cache**
2100	**Domain Cached Credentials 2 (DCC2), MS Cache 2**
15300	DPAPI masterkey file v1
15900	DPAPI masterkey file v2
12800	MS-AzureSync PBKDF2-HMAC-SHA256
1500	descrypt, DES (Unix), Traditional DES
12400	BSDi Crypt, Extended DES
500	md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5)
3200	bcrypt $2*$, Blowfish (Unix)
7400	sha256crypt 5, SHA256 (Unix)
1800	ha512crypt 6, SHA512 (Unix)
122	macOS v10.4, MacOS v10.5, MacOS v10.6
1722	macOS v10.7
7100	**macOS v10.8+ (PBKDF2-SHA512)**
6300	AIX {smd5}
6700	AIX {ssha1}
6400	AIX {ssha256}
6500	AIX {ssha512}
2400	Cisco-PIX MD5
2410	Cisco-ASA MD5
500	Cisco-IOS 1 (MD5)
5700	Cisco-IOS type 4 (SHA256)
9200	Cisco-IOS 8 (PBKDF2-SHA256)
9300	**Cisco-IOS 9 (scrypt)**
22	Juniper NetScreen/SSG (ScreenOS)
501	Juniper IVE
15100	Juniper/NetBSD sha1crypt
7000	**FortiGate (FortiOS)**
5800	Samsung Android Password/PIN
13800	Windows Phone 8+ PIN/password
8100	Citrix NetScaler
8500	RACF
7200	GRUB 2
9900	Radmin2

Attack Modes

-a 0	Straight	[hash] [dictionary]
-a 1	Combination	[hash] [dictionary] [dictionary]
-a 3	Brute-Force	[hash] [mask]
-a 6	Hybrid Wordlist + Mask	[hash] [dictionary] [mask]
-a 7	Hybrid Mask + Wordlist	[hash] [dictionary] [mask]

Character Sets (Default) [?]

?l	abcdefghijklmnopqrstuvwxyz	[26]
?u	ABCDEFGHIJKLMNOPQRSTUVWXYZ	[26]
?d	0123456789	[10]
?h	0123456789abcdef	[16]
?H	0123456789ABCDEF	[16]
?s	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~	[33]
?a	?l?u?d?s	[95]
?b	0x00 - 0xff	[255]

Device Types (-D)

-D 1	CPU
-D 2	GPU
-D 3	FPGA, DSP, Co-Proc

Options

-m [#]	Hash Type (mode)
-a [#]	Attack Mode
-r [file]	Rules file
-V	Version
--status	Keep screen updated
-b	Benchmark
--runtime [#]	Abort after x seconds
--session [text]	Set session name (resumeable)
--restore	Restore/Resume session
-o [filename]	Define output/potfile
--username	Ignore username field in hashfile
--potfile-disable	Ignore potfile and do not write
-d [#]	Specify an OpenCL Device
-D [#]	Specify an OpenCL Device type
-I	List OpenCL Devices & Types
-O	Optimized Kernel, Passwords <32 char
-i	Increment (brute force)
--increment-min [#]	Start increment at [#] of chars
--increment-max [#]	Stop increment at [#[of chars

hashcat-utils

Cap2hccapx (.pcap to WPA/WPA2)

./cap2hccapx.bin input.pcap output.hccapx [essid]

ct3_to_ntlm (mschap to ntlm)

./ct3_to_ntlm.bin 8-byte-ct3-in-hex 8-byte-salt-in-hex [24bESS]

Hashcat 4.10 Cheat Sheet v.2018.1b

@BHInfoSecurity @Krelkci

https://www.blackhillsinfosec.com

https://hashcat.net/hashcat/

https://github.com/hashcat/hashcat

Common Dictionary Repos

CrackStation: https://crackstation.net/

Lots of others: https://wiki.skullsecurity.org/Passwords

Custom: cewl -d3 -w wordlist.txt -v http://domain.tld

Hash Sources to Hash Type

Inveigh NetNTLMv1	5500
Inveigh NetNTLMv2	5600
Mimikatz/LSAdump	1000
esedbexport/secretsdump.py ntds.dit (LM)	3000
esdbexport/secretsdump.py ntds.dit (NTLM)	1000
airmon-ng (WPA/WPA2)	2500
	2501

Common Hash Types

MD4	90
MD5	0
NTLM	1000
NetNTLMv1	5500
NetNTLMv2	5600
mscache1 (xp, w2k3)	1100
mscache2 (v, w7, w8, w10,w2k8+)	2100
LanManager	3000
SHA512	1700
Kerberos REQ	7500
Kerberos TGS-REP	13100
Wordpress	400
WPA	2500
WPA PMK	2501

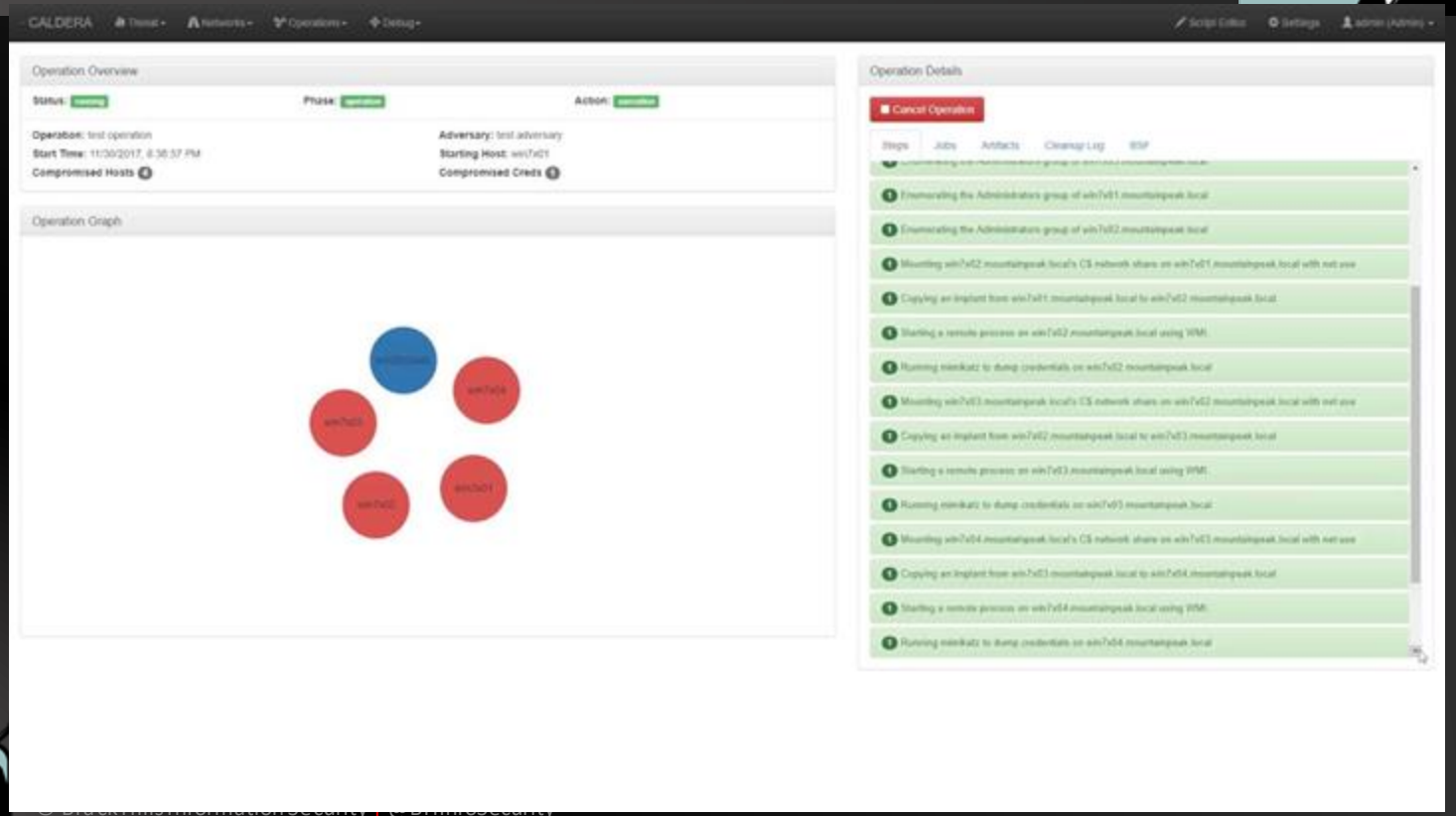
https://www.blackhillsinfosec.com/hashcat-4-10-cheat-sheet-v-1-2018-1/

Threat Emulation

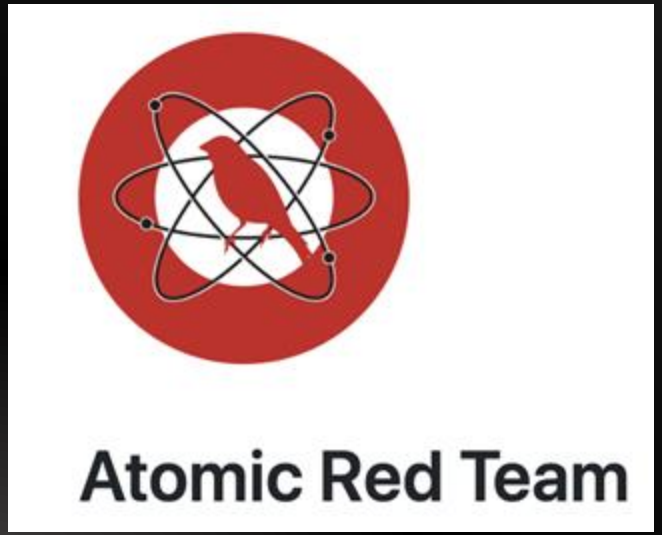
- Don’t just think of vulnerabilities as missing patches and misconfigurations on systems
- Think post exploitation
- What happens after an attacker gains access to a system
- There are a number of free tools that will automate parts of this process
- Currently, would take a bit of tuning and trial and error
- The collected data is invaluable

Question:
What is the Difference Between Emulation and Simulation?
Who cares?

Open Source Tool Example: Caldera



Open Source Tool Example: Atomic Red Team



Execute All Attacks for a Given Technique

```
Invoke-AtomicTest T1117
```

Speficy a Process Timeout

```
Invoke-AtomicTest T1117 -TimeoutSeconds 15
```

If the attack commands do not exit (return) within in the specified `-TimeoutSeconds`, the process and it's children will be forcefully terminated. The default value of `-TimeoutSeconds` is 120. This allows the `Invoke-AtomicTest` script to move on to the next test.

Execute All Tests

This is not recommended but you can execute all Atomic tests in your atomics folder with the follwing:

```
Invoke-AtomicTest All
```

Execute All Tests from a Specific Directory

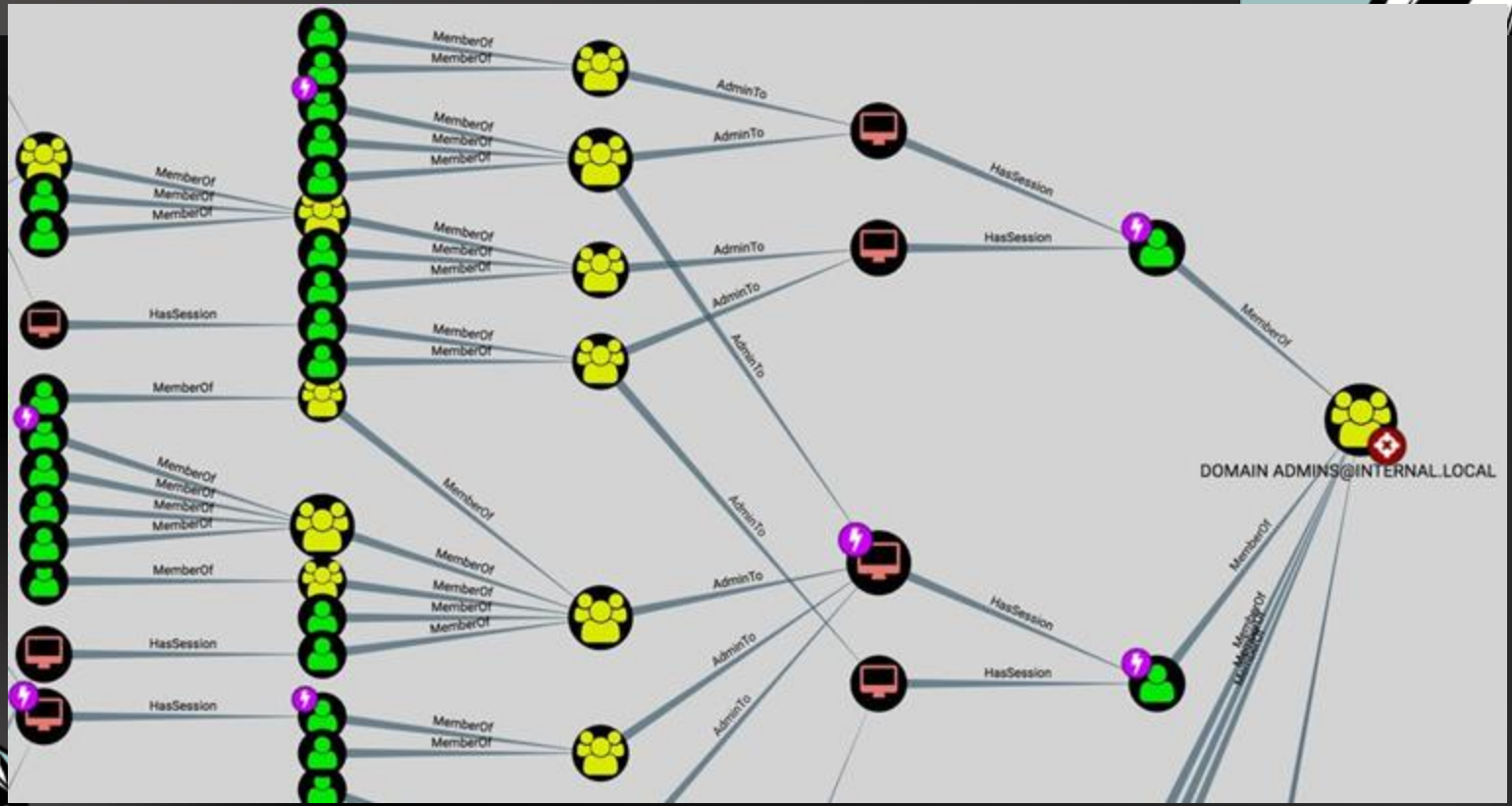
Specify a custom path to your atomics folder, example C:\AtomicRedTeam\atomics

```
Invoke-AtomicTest All -PathToAtomicsFolder C:\AtomicRedTeam\atomics
```

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1117 -TestNumbers 1 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: Regsvr32 T1117
Atomic Test Name: Regsvr32 local COM scriptlet execution
Atomic Test Number: 1
Description: Regsvr32.exe is a command-line program used to register and unregister OLE controls.
Upon execution, calc.exe will be launched.
Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
regsvr32.exe /s /u /i:#{filename} scrobj.dll
Command (with inputs):
regsvr32.exe /s /u /i:C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct scrobj.dll
Dependencies:
Description: Regsvr32.exe must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1117
\src\RegSvr32.sct)
Check Prereq Command:
if (Test-Path #{filename}) {exit 0} else {exit 1}
Check Prereq Command (with inputs):
if (Test-Path C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct) {exit 0} else {exit 1}
Get Prereq Command:
New-Item -Type Directory (split-path #{filename}) -ErrorAction ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/Reg
Svr32.sct" -OutFile "#{filename}"
Get Prereq Command (with inputs):
New-Item -Type Directory (split-path C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct) -ErrorAction
 ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/Reg
Svr32.sct" -OutFile "C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct"
[!!!!!!!!END TEST!!!!!!!]
```

Open Source Tool Example: Bloodhound



Threat Emulation Warning

- One of the traps of the MITRE framework and threat emulation is we train our systems to detect specific attacks
- Most of the attacks in Atomic Red Team and MITRE are representations of classes of attacks
- We are seeing vendors simply detect those attacks
  - More on this later!
- A few modifications and you can easily bypass detection

Commercial Offerings

ATTACKIQ

SCYTHE

XM CYBER

Everyone's a Winner!

MITRE ENGENUITY | ATT&CK Evaluations

Enterprise ICS Managed Services Trials Resources

Home > Using Attack Evaluations

GETTING STARTED

Using ATT&CK Evaluations

Who We Are

MITRE Engenuity evaluates cybersecurity products using an open methodology based on the ATT&CK® knowledge base.
Our goals are to improve organizations against known adversary behaviors by:

Empowering end-users with objective insights into how to use participating security products

Providing transparency around the true capabilities of participating security products

Driving participants to **Enhance** their capabilities

These evaluations are not a competitive analysis. We show the detections we observed without providing a "winner." Because there is no singular way for analyzing, ranking, or rating the solutions, we instead show how each vendor approaches threat de within the context of ATT&CK.

Our evaluation methodologies are publicly available, and the results are publicly released. We continue to evolve and extend our methodologies and content to ensure a fair, transparent, and useful evaluation process.

Interpreting Our Results

Making sense of ATT&CK Evaluation results can be challenging. Each participant has their own take on the results, and every user has their own criteria for success. Fortunately, to accompany the raw results, we also have tools and resources that can h use and understand the data.

User Guide

This guide helps you understand how to use the evaluation results to assess security products and select an endpoint threat detection tool. In this guide, we address using ATT&CK Evaluations to inform two of the key questions:

- Does this tool detect known threats to your organization (i.e., ATT&CK technique coverage)?
- How does the tool present the data to your analysts (i.e., Graphical User Interface)?"

This post helps you understand the nuance required to utilize ATT&CK Evaluation data. It explores why so many participants declare themselves the winner, as well as common pitfalls people make when analyzing the information, including the thought that ATT&CK Evaluations can answer every question, and overgeneralizing the results.

Or not?

README.md

attack-eval-scoring

This project represented my attempts at analyzing the results of round 1 of the MITRE Enterprise ATT&CK Evaluation. With the release of round 2 results, please check out my new project: https://github.com/joshzelonis/EnterpriseAPT29Eval

For my initial blog post on the subject, check out: https://go.forrester.com/blogs/measuring-vendor-efficacy-using-the-mitre-attck-evaluation/

simple_score.py

In parsing the results, I found 56 ATT&CK techniques were measured with 136 procedures for doing so. This is a quick script for applying the scale on a procedure (or per step) basis. There were many instances where there were multiple detections for a single procedure/step which would skew any counting method that did not take this into effect.

coverage.py

This script generates two key metrics for understanding vendor performance. The first of which is a coverage score which gives insight into the percentage of ATT&CK techniques the solution was able to generate any type of detection against. This can be viewed as a high water mark for how the product could be used to generate detections. The second metric is a correlation metric which is the percentage of detections that had a tainted modifier. This is useful for understanding how the product reduces work for SOC analysts.

kill_chain_analysis.py

There were 10 different stages of attack measured from initial compromise to execution of persistence across two scenarios. One may argue that the most critical capability is being able to alert on an aversary at each stage of an intrusion. This script analyzes and breaks out how each vendor performed at each stage of these scenarios on the same 1-3-5 scale used by simple_score.py

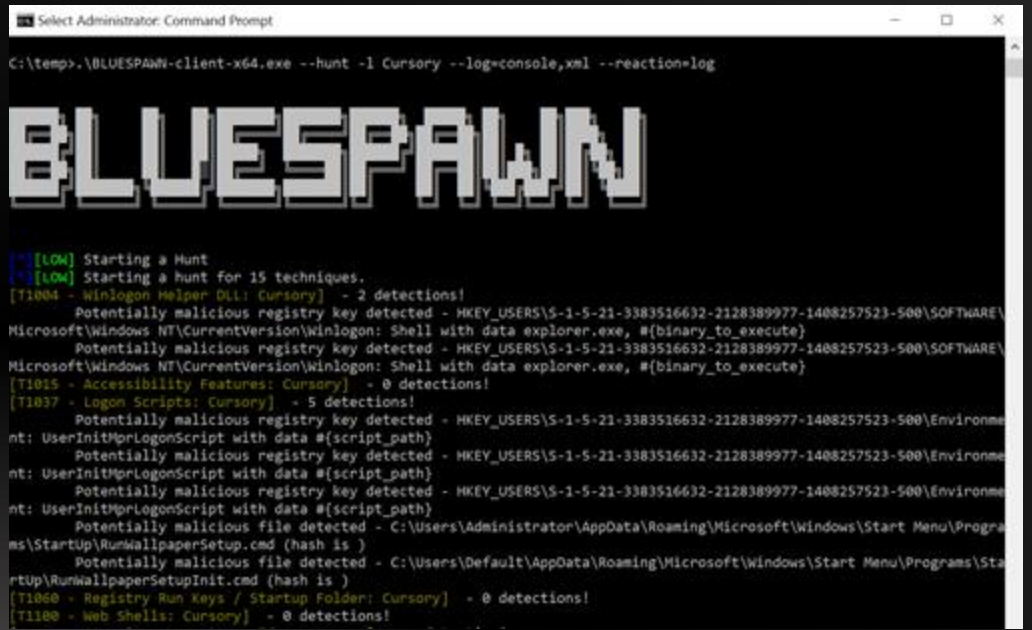
“Simple” Score

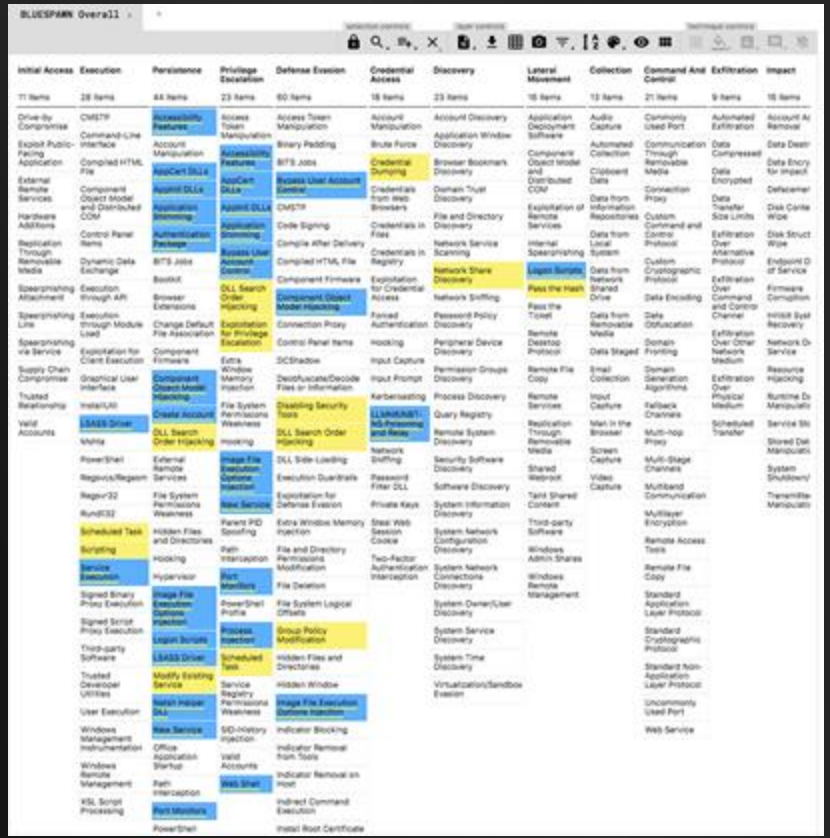
```
john@pop-os:~/attack-eval-scoring$ python3 simple_score.py
./data/McAfee.1.APT3.1_Results.json - 268
./data/CarbonBlack.1.APT3.1_Results.json - 259
./data/Cybereason.1.APT3.1_Results.json - 285
./data/Microsoft.1.APT3.1_Results.json - 195
./data/PaloAltoNetworks.1.APT3.1_Results.json - 329
./data/GoSecure.1.APT3.1_Results.json - 108
./data/RSA.1.APT3.1_Results.json - 78
./data/F-Secure.1.APT3.1_Results.json - 376
./data/Endgame.1.APT3.1_Results.json - 225
./data/FireEye.1.APT3.1_Results.json - 288
./data/CrowdStrike.1.APT3.1_Results.json - 269
./data/SentinelOne.1.APT3.1_Results.json - 123
```

Misses

```
john@pop-os:~/attack-eval-scoring$ python3 total_misses.py
./data/McAfee.1.APT3.1_Results.json - 38
./data/CarbonBlack.1.APT3.1_Results.json - 34
./data/Cybereason.1.APT3.1_Results.json - 24
./data/Microsoft.1.APT3.1_Results.json - 23
./data/PaloAltoNetworks.1.APT3.1_Results.json - 9
./data/GoSecure.1.APT3.1_Results.json - 28
./data/RSA.1.APT3.1_Results.json - 49
./data/F-Secure.1.APT3.1_Results.json - 14
./data/Endgame.1.APT3.1_Results.json - 14
./data/FireEye.1.APT3.1_Results.json - 32
./data/CrowdStrike.1.APT3.1_Results.json - 22
./data/SentinelOne.1.APT3.1_Results.json - 35
```

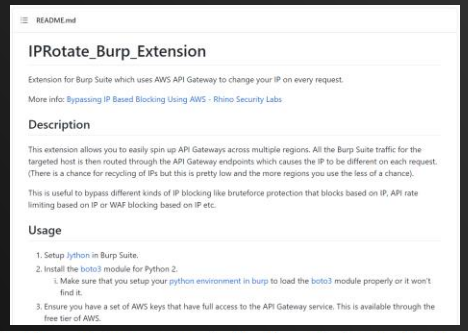
Optional LAB: EDR with Bluespawn





Infrastructure

- Get a cloud provider
  - We use Digital Ocean
  - And Amazon
  - ***And Azure***…
- Automation is key
- You will be bouncing attacks
- You will need Phishing infrastructure
  - Azure helps
- Buy lots of old and categorized domains
- Buy them now


README.md

IPRotate_Burp_Extension

Extension for Burp Suite which uses AWS API Gateway to change your IP on every request.

More info: Bypassing IP Based Blocking Using AWS - Rhino Security Labs

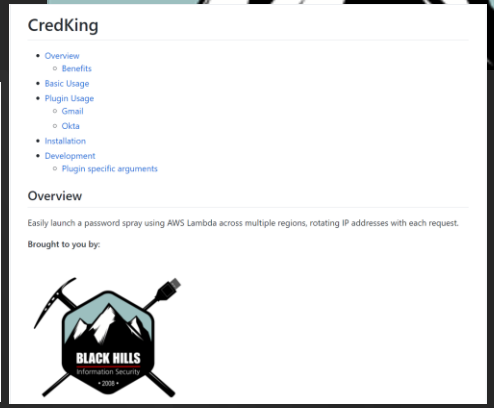
Description

This extension allows you to easily spin up API Gateways across multiple regions. All the Burp Suite traffic for the targeted host is then routed through the API Gateway endpoints which causes the IP to be different on each request. (There is a chance for recycling of IPs but this is pretty low and the more regions you use the less of a chance).

This is useful to bypass different kinds of IP blocking like bruteforce protection that blocks based on IP, API rate limiting based on IP or WAF blocking based on IP etc.

Usage

1. Setup Jython in Burp Suite.
2. Install the boto3 module for Python 2.
   i. Make sure that you setup your python environment in burp to load the boto3 module properly or it won't find it.
3. Ensure you have a set of AWS keys that have full access to the API Gateway service. This is available through the free tier of AWS.


CredKing

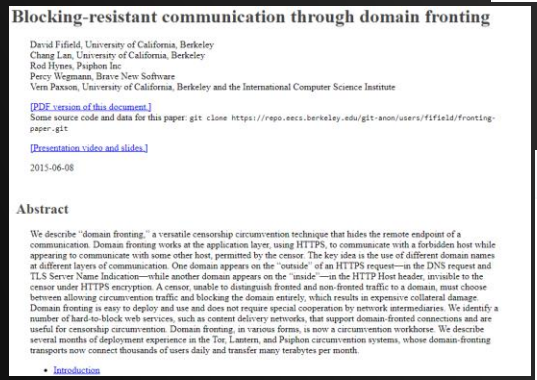
- Overview
  - Benefits
- Basic Usage
- Plugin Usage
  - Gmail
  - Okta
- Installation
- Development
  - Plugin specific arguments

Overview

Easily launch a password spray using AWS Lambda across multiple regions, rotating IP addresses with each request.

Brought to you by:

BLACK HILLS Information Security


Blocking-resistant communication through domain fronting

David Fifield, University of California, Berkeley
Chang Lan, University of California, Berkeley
Rod Hynes, Psiphon Inc
Percy Wegmann, Brave New Software
Vern Paxson, University of California, Berkeley and the International Computer Science Institute

[PDF version of this document.]
Some source code and data for this paper: `git clone https://repo.eecs.berkeley.edu/git-anon/users/fifield/fronting-paper.git`

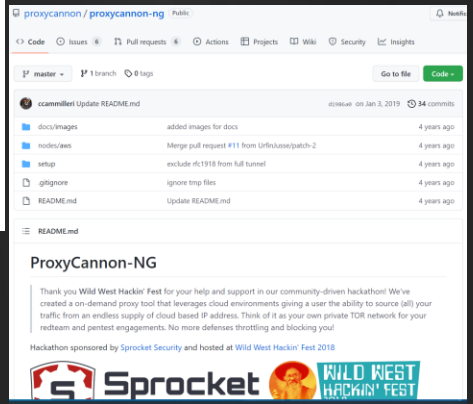
[Presentation video and slides.]

2015-06-08

Abstract

We describe "domain fronting," a versatile censorship circumvention technique that hides the remote endpoint of a communication. Domain fronting works at the application layer, using HTTPS, to communicate with a forbidden host while appearing to communicate with some other host, permitted by the censor. The key idea is the use of different domain names at different layers of communication. One domain appears on the "outside" of an HTTPS request—in the DNS request and TLS Server Name Indication—while another domain appears on the "inside"—in the HTTP Host header, invisible to the censor under HTTPS encryption. A censor, unable to distinguish fronted and non-fronted traffic to a domain, must choose between allowing circumvention traffic and blocking the domain entirely, which results in expensive collateral damage. Domain fronting is easy to deploy and use and does not require special cooperation by network intermediaries. We identify a number of hard-to-block web services, such as content delivery networks, that support domain-fronted connections and are useful for censorship circumvention. Domain fronting, in various forms, is now a circumvention workhorse. We describe several months of deployment experience in the Tor, Lantern, and Psiphon circumvention systems, whose domain-fronting transports now connect thousands of users daily and transfer many terabytes per month.

- Introduction


proxycannon / proxycannon-ng

Code | Issues 6 | Pull requests 6 | Actions | Projects | Wiki | Security | Insights

master | 1 branch | 0 tags | Go to file | Code

ccammilleri Update README.md on Jan 3, 2019 34 commits

docs/images	added images for docs	4 years ago
nodes/aws	Merge pull request #11 from Urfin/usse/patch-2	4 years ago
setup	exclude rfc1918 from full tunnel	4 years ago
.gitignore	ignore tmp files	4 years ago
README.md	Update README.md	4 years ago

README.md

ProxyCannon-NG

Thank you Wild West Hackin' Fest for your help and support in our community-driven hackathon! We've created a on-demand proxy tool that leverages cloud environments giving a user the ability to source (all) your traffic from an endless supply of cloud based IP address. Think of it as your own private TOR network for your redteam and pentest engagements. No more defenses throttling and blocking you!

Hackathon sponsored by Sprocket Security and hosted at Wild West Hackin' Fest 2018

Sprocket | WILD WEST HACKIN' FEST

BLACK HILLS Information Security

When Things Go Wrong

- And they will
- Lose, but don't lose the lesson
- I have shared a lot of stories
- A little about SANS
- Everything can be improved
- Everything
- How to prepare
- How to react
- How to spin
- How to turn a negative into a positive

Backdoors and Breaches

Yep....

HTTP AS EXFIL

The attackers use HTTP as an exfil method. This is usually used in conjunction with some type of stego. For example, VSAgent uses base64 encoded __VIEWSTATE as an exfil field.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Metasploit Reverse HTTP Payloads
VSAgent
Prismatica

https://www.blackhillsinfosec.com/504-vsagent-usage-instructions

https://github.com/Project-Prismatica/Prismatica

HTTPS AS EXFIL

This is pretty basic: the attackers use HTTPS. Lots and lots of malware uses this. For example, Meterpreter has used this technique for a long time. It can be used in conjunction with other stego techniques.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Metasploit Reverse HTTPS Payloads
SILENTTRINITY

HTTPS

https://www.metasploit.com

https://attack.mitre.org/techniques/T1032

https://github.com/byt3bl33d3r/SILENTTRINITY

DNS AS C2

The attackers use DNS as a C2 channel.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

dnscat2

https://www.blackhillsinfosec.com/bypassing-cylance-part-2-using-dnscat2

Windows Background Intelligent Transfer Service (BITS)

The attackers use BITS, another protocol that is often ignored.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

CE-

M$

https://github.com/deruke/tools

Gmail, Tumblr, Salesforce, Twitter as C2

The attackers route traffic through third-party services. Many services, like Gmail, are ignored completely by many security tools.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Gcat
Sneaky Creeper

https://github.com/byt3bl33d3r/gcat

https://github.com/DakotaNelson/sneaky-creeper

Domain Fronting as C2

The attackers use Domain Fronting to bounce their traffic off of legitimate systems.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Cobalt Strike

https://www.cobaltstrike.com

https://www.blackhillsinfosec.com/bypass-web-proxy-filtering

Things Not In B&B

- https://www.thec2matrix.com/
- https://www.digitalocean.com/community/tutorials/how-to-use-certbot-standalone-mode-to-retrieve-let-s-encrypt-ssl-certificates-on-ubuntu-16-04
- https://www.blackhillsinfosec.com/using-cloudfront-to-relay-cobalt-strike-traffic/
- https://github.com/killswitch-GUI/CobaltStrike-ToolKit/blob/master/HTTPsC2DoneRight.sh
- https://fortynorthsecurity.com/blog/introducing-c2concealer/

Things Not In B&B

- https://urlfiltering.paloaltonetworks.com/
- https://www.digicert.com/kb/ssl-support/ssl-enabling-perfect-forward-secrecy.htm
- https://github.com/api0cradle/Powershell-ICMP
- https://github.com/breenmachine/dnsftp
- https://github.com/Arno0x/DNSExfiltrator

PHISH

The attackers send a malicious email targeting users. Because users are super easy to attack. Feel free to add a narrative of a CEO getting phished. Or maybe the Help Desk!

DETECTION

Firewall Log Review
Endpoint Security Protection Analysis

TOOLS

evilginx
GoPhish
CredSniper

https://www.blackhillsinfosec.com/how-to-phish-for-geniuses

https://www.blackhillsinfosec.com/offensive-spf-how-to-automate-anti-phishing-reconnaissance-using-sender-policy-framework

Web Server Compromise

The attackers take over an external web server. They use it to pivot to your internal network.

DETECTION

Server Analysis
SIEM Log Analysis
NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Zed Attack Proxy
sqlmap
Burp Proxy

https://www.zaproxy.org

https://portswigger.net/burp

https://www.blackhillsinfosec.com/using-simple-burp-macros-to-automate-testing

External Cloud Access

The attackers gain access to your cloud resources. They use this access to pivot.

DETECTION

SIEM Log Analysis

TOOLS

SprayingToolkit
CredKing
FireProx

https://github.com/byt3bl33d3r/SprayingToolkit

https://github.com/ustayready/CredKing

https://github.com/ustayready/fireprox

Insider Threat

An internal disgruntled user exfiltrates information from your network.

DETECTION

User and Entity Behavior Analytics
DLP (Ha! Ha! Kidding. DLP never works.)
Working with HR

TOOLS

Being considered a Full Time Expenditure (FTE)
Long Hours
Addiction

https://americanaddictioncenters.org

Password Spray

The attackers gain access to your internal network by spraying commonly used passwords (like SeasonYear) against your organization.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Firewall Log Review

TOOLS

SprayingToolkit
FireProx
Hydra
DomainPasswordSpray

https://github.com/byt3bl33d3r/SprayingToolkit

https://github.com/ustayready/fireprox

https://github.com/dafthack/DomainPasswordSpray

Trusted Relationship

A trusted third party who has access to your network is compromised. The attackers use this to pivot to your internal resources.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics

TOOLS

An unfortunate and unfounded trust in humanity and business partners who are complete strangers.

Social Engineering

The attackers use social engineering to trick a user into running malware.

DETECTION

Endpoint Security Protection Analysis
User Awareness Training

TOOLS

Phone
A goal and a dream of evil
People trusting people

https://youtu.be/rnmcRTnTNC8

https://youtu.be/FvhkKwHjUVg

Bring Your Own (Exploited) Device

Your organization allows users to bring in their own devices. Or, another way to put it, they bring in their own exploited devices. The attackers use these devices to compromise your organization.

DETECTION

Firewall Log Review
NetFlow, Zeek/Bro, RITA Analysis

TOOLS

The completely asinine belief that somehow allowing people to bring their own devices in is a worthy cost savings.

https://www.blackhillsinfosec.com/pentesting-dropbox-on-steroids

Exploitable External Service

An external service has a misconfiguration or a publicly available exploit. The attackers take advantage of this to attack and pivot to internal resources.

DETECTION

Firewall Log Review
Server Analysis

TOOLS

Metasploit
Failed Patching Process
Unauthorized System Stood Up by Employee

https://www.metasploit.com

Credential Stuffing

The attackers take advantage of third-party breaches to identify and use IDs and passwords against your organization.

DETECTION

Server Analysis
User and Entity Behavior Analytics

TOOLS

Burp
Hydra
Users registering for services with their work email addresses.

https://github.com/ustayready/fireprox
https://github.com/dafthack/DomainPasswordSpray
https://github.com/byt3bl33d3r/SprayingToolkit
https://portswigger.net/burp

INTERNAL PASSWORD SPRAY

The attackers start a password spray against the rest of the organization from a compromised system.

DETECTION

User and Entity Behavior Analytics
SIEM Log Analysis

TOOLS

Domain Password Spray

https://github.com/dafthack/DomainPasswordSpray

https://www.blackhillsinfosec.com/webcast-attack-tactics-5-zero-to-hero-attack

KERBEROASTING

The attackers use a "feature" of SPNs to extract and crack service passwords.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Honey Services
Internal Segmentation

TOOLS

GetUserSPNs.py from Impacket
Hashcat for Cracking

https://www.blackhillsinfosec.com/running-hashcat-on-ubuntu-18-04-server-with-1080ti

https://github.com/SecureAuthCorp/impacket/blob/master/examples/GetUserSPNs.py

Broadcast/Multicast Protocol Poisoning

For years, LANMAN was the worst thing in Windows. Then LLMNR said "Stand Back and Hold My Beer!" Basically, LLMNR lets a host ask for name resolution from any system on the same network. The attackers perform Broadcast/Multicast protocol poisoning on your Active Directory Network.

DETECTION

CredDefense Toolkit
User and Entity Behavior Analytics
Firewall Log Review

TOOLS

Responder attacks LLMNR, NBT-NS, and mDNS.

https://github.com/lgandx/Responder

https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to

Weaponizing Active Directory

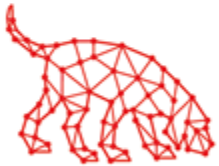
The attackers map trust relationships and user/group privileges in your Active Directory Network.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Internal Segmentation

TOOLS

BloodHound
DeathStar
CrackMapExec



https://github.com/BloodHoundAD/BloodHound

https://github.com/byt3bl33d3r/DeathStar

https://github.com/byt3bl33d3r/CrackMapExec

https://www.blackhillsinfosec.com/webcast-weaponizing-active-directory

Credential Stuffing

Valid Active Directory credentials have been discovered on open shares and files within your environment. These are used by the attackers.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Internal Segmentation

TOOLS

ADExplorer.exe
Invoke-ShareFinder
Invoke-FileFinder
Find-InterestingFile
MailSniper

https://www.blackhillsinfosec.com/domain-goodness-learned-love-ad-explorer

https://www.blackhillsinfosec.com/abusing-exchange-mailbox-permissions-mailsniper

New Service Creation

The attackers create and load their malware using a service with SYSTEM privileges. Or, they just create a new service.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis

TOOLS

Metasploit getsystem and other Post-Exploitation Scripts.

https://www.metasploit.com

Local Privilege Escalation

The attackers use a vulnerability in local software to gain administrative access.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis

TOOLS

PowerSploit's PowerUp
Meterpreter Post-Exploitation Scripts

https://www.blackhillsinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions-av

Things Not In B&B

- rpcclient –U [username] [domain controller IP] --option=’ldap page size’=[integer] -c “enumdomusers” | cut –d ‘[‘ -f 2 | cut –d ‘]’ -f 1 > users.txt

https://github.com/dafthack/DomainPasswordSpray

- https://github.com/sense-of-security/ADRecon/blob/master/ADRecon.ps1

Things Not In B&B

- `az login --allow-no-subscriptions --use-device-code`
- `az ad user list --filter “AccountEnabled eq true” > Users.txt`

- GitHub - dirkjanm/ROADtools: The Azure AD exploration framework.

Things Not In B&B

- https://github.com/dafthack/MSOLSpray

  https://github.com/arch4ngel/BruteLoops

- https://github.com/dafthack/MailSniper

Things Not In B&B

- Invoke-ShareFinder -CheckShareAccess -Verbose -Threads 20 | Out-File -Encoding ascii interesting_shares.txtInvoke-FileFinder -ShareList .\interesting_shares.txt -Verbose -Threads 20 -OutFile sensitive_files.csv

- `Invoke-AllChecks | Out-File -Encoding ASCII LocalPrivilegeEscalationChecks.txt`
- `Copy – PowerSploit PowerUp`

Things Not In B&B

- # Metasploit - Add a route. Adjust the IP and subnet accordingly
- route add 10.0.0.0 255.0.0.0 3
- use auxiliary/scanner/smb/smb_login
- set rhosts 10.116.112.0/24
- set smbuser Administrator
- set smbpass <32CharHash:32CharHash>
- set smbdomain
- set threads 10
- run

Things Not In B&B

- Get ntds.dit

- Use the PowerSploit Powerview module called UserHunter. It will find systems where the current user has administrative access and where a Domain Administrator is logged in. You can run a command shell as different users and repeat this to look for more systems.
- Invoke-UserHunter

Malicious Service/Just Malware

The attackers add a service that starts every time the system starts.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Metasploit Persistence
autoruns.exe
msconfig.exe
SILENTTRINITY

https://github.com/byt3bl33d3r/SILENTTRINITY

DLL Attacks

The attackers hijack the order in which DLLs are loaded. This is usually done through insecure directory/file permissions.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

PowerSploit
InvisiMole

https://www.blackhillsinfosec.com/digging-deeper-vulnerable-windows-services

Malicious Driver

The attackers load a malicious driver into the operating system.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Pasam	ROCKBOOT
Wingbird	Alureon
SeaDuke	

https://en.wikipedia.org/wiki/Alureon

New User Added

Easy, the attackers add a new user to the local computer.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Metasploit
Cobalt Strike

https://www.metasploit.com

https://www.cobaltstrike.com

Application Shimming

The attackers use the Application Compatibility Toolkit to trick applications into not seeing the ports, directories, files, and services the attackers want to hide.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Windows Assessment and Deployment Kit (ADK)

https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install

https://attack.mitre.org/techniques/T1138

Malicious Browser Plugins

The attackers install plugins in the browser. This can be used as part of C2 and persistence. The browser is the new endpoint.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
Web Proxy (Firewall Log Review)
NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Grammarly is a Keylogger
graniet/chromebackdoor

https://www.kaspersky.com/blog/browser-extensions-security/20886

https://github.com/graniet/chromebackdoor

Logon Scripts

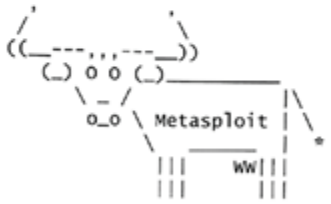
The attackers install a script that triggers when a user logs on.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Meterpreter Persistence



https://www.metasploit.com

Evil Firmware

The attackers update the firmware of Network Cards, Video Cards, and BIOS or UEFI... with Evil! All of these are very difficult to detect and very difficult to update.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
Prayers to an Engaged and Merciful God

TOOLS

Hacking Team UEFI Rootkit
BadBIOS (... maybe.)

https://threatpost.com/uefi-rootkit-sednit/140420

Accessibility Features

The attackers hijack Accessibility Features like Sticky Keys and Onscreen Keyboard.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis

TOOLS

Bash Bunny
USB Rubber Ducky

https://shop.hak5.org

Things Not In B&B

- https://github.com/optiv/ScareCrow
- https://github.com/Tylous/SourcePoint
- https://github.com/pathtofile/PPLRunner
- https://github.com/xforcered/InvisibilityCloak/blob/main/WWHF_2022_Presentation/Applying_the_InvisibilityCloak_WWHF_2022.pdf
- https://github.com/optiv/Mangle
- https://github.com/h4wkst3r/InvisibilityCloak
- https://github.com/GhostPack/Seatbelt