

699.6 Adversary Emulation Capstone



SANS

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.



Adversary Emulation Capstone

© 2021 James Shewmaker | All Rights Reserved | Version G01_01

Welcome to Day 6 of SANS Security SEC699: Advanced Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection.

James Shewmaker

jshewmaker@sans.org

www.sans.org

Update: G01_01

Course Roadmap

- Introduction & Key Tools
- Initial Access
- Lateral Movement
- Persistence
- Azure AD & Emulation Plans
- **Adversary Emulation Capstone**

SEC699.6

Capstone

Capstone Introduction – Live Events
Capstone Introduction – OnDemand

This page intentionally left blank.

Course Roadmap

- Introduction & Key Tools
- Initial Access
- Lateral Movement
- Persistence
- Azure AD & Emulation Plans
- **Adversary Emulation Capstone**

SEC699.6

Capstone

- Capstone Introduction – Live Events
- Capstone Introduction – OnDemand

This page intentionally left blank.

INTRODUCTION



The SEC699 capstone challenge will cover the **different topics** discussed throughout the course. The goal is to summarize all lessons learned in a hands-on workshop! You will work in teams to try obtaining a **precious coin!**

You will play in **teams of 4 to 5 students**

You will play both a **red team** and **blue team** role

The capstone will run from **09:00** to **14:00**

This page intentionally left blank.

BRIEFING AND INTRODUCTION



So, what is **expected** of you? As you are playing in this capstone, your team will be **both a blue and a red team** at the same time:

You will receive an **organization brief** that explains what your organization is, what your crown jewels are, and what your network environment looks like. **Please carefully read this!**

You will receive a **threat actor brief** that explains what threat actor you are, what industries you typically target, and what attack techniques you typically employ. **Please carefully read this!**

As you will be targeting other teams, it's in your own interest NOT to disclose what threat actor / organization your team was assigned!

This page intentionally left blank.

EXAMPLE ORGANIZATION

About Us

CoalGasOil

Our main business is to process the raw materials coming in into the various plants into a product that can be used by the regular consumer. There are three distinct processing plants:

- ✔ Coal: the coal processing plant receives coals via boat shipments, from there the raw coals are processed into briquettes that can be used for cooking and home heating;
- ✔ Gas: in our gas processing plant the raw natural gas is delivered via a pipeline directly from our supplier, in the gas processing plant we prepare the gas to be suitable for usage by consumers.
- ✔ Oil: in our oil processing plant the raw oil is delivered to us via oil pipelines, we refine the crude oil into various products for the consumer market.

We are operating our plants with state of the art technology, all managed from our HQ.



This page intentionally left blank.

EXAMPLE THREAT ACTOR



APT-28

APT-28 is known as a whole range of other names, including Fancy Bear, STRONTIUM and Sofacy. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT-28 has been active since at least 2004.

TARGET ORGANIZATION

CENSORED



COMMON TECHNIQUES

CENSORED

The above is a **sample threat actor**, with the target organization and techniques censored. 😊

This page intentionally left blank.

HOW CAN YOU SCORE POINTS?

1

Obtain access to the **crown jewels** of the organization you are targeting
Proof: Steal the “crown jewel file” and present it during your presentation

2

Plant your flag on the systems of the target organization
Proof: Every system has a “flag file” that is periodically checked and scored automatically

3

Emulate the techniques you are known for (see threat actor brief)
Proof: Present proof of execution of techniques during your presentation

How about the “blue team” side?
Simple: Detect and kick out the threat actors so they don’t score points. 😊

This page intentionally left blank.

WHAT DOES THE FLAG FILE LOOK LIKE?



The flag file is a text file (with any extension) that can be **anywhere on the system**. The file is the same across the organization though, so once you find it, you know where to find it on all hosts for that organization! When the flag file is not adapted, it includes the following string: **SYSTEM_NOT_OWNED**.

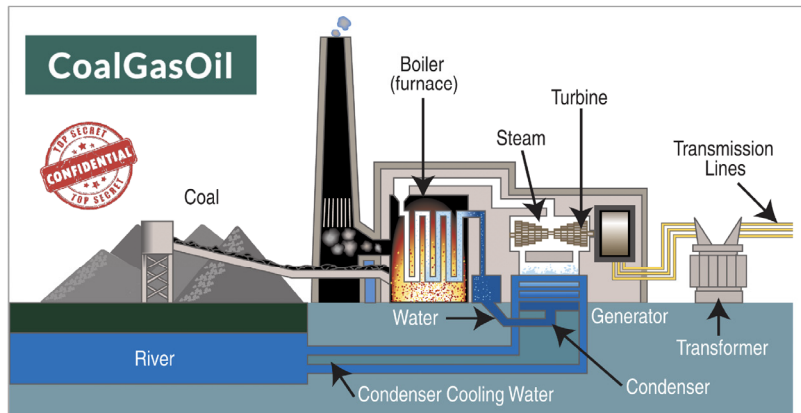
In order to plant your flag, please enter your **team number** (provided by the Instructor). As a defender, **remove** these team numbers when they are set to prevent the other team from scoring. The value of these files is **periodically checked** by the Instructor; thus the longer a number is set, the longer a team scores points!

Finally, it's important to note that **critical systems** (mentioned in the briefings) **generate more points** when compromised!

This page intentionally left blank.

WHAT DO THE CROWN JEWEL FILES LOOK LIKE?

CoalGasOil Plant Diagram



The crown jewels for all organizations are different! They are listed in the briefing document you will receive.

The example on the left is one of the CoalGasOil crown jewels: a **coal plant diagram**!

This page intentionally left blank.

PRESENTATION TO PREPARE



At the end of the capstone, you'll need to do a **15-minute presentation** where you cover both your results as an organization and as a threat actor. Some things you have to cover:

Organization

- Show detections of attack techniques (screenshots of logs)
- Attribute the threat actor to a team in the room

Threat actor

- Present overall attack structure and flow
- Show crown jewel files if you obtained them
- Show screenshots of successful attack techniques

The presentation needs to be submitted by 14:00!

This page intentionally left blank.

HOW DO YOU GET STARTED?



Everyone starts from their personal
CommandoVM (local)

Start doing reconnaissance on your target
organization and try to obtain **an initial
foothold!**

Start building detection logic in order to
detect the adversaries in the environment.
You have access to **Elastic** and
Velociraptor!

This page intentionally left blank.

RULES OF ENGAGEMENT

Some rules of engagement to adhere to:

- As threat actor, your goal is not to be disruptive; refrain from destructive attacks against your target environment
- As threat actor, try to leverage as much as possible the techniques you have been assigned in the emulation plan (it gives you more points)
- As threat actor, do not tamper with the event logging infrastructure put in place (Sysmon, WEF, Elastic,...)
- If, as an organization, you are “locked out” of your environment, you can escalate to the emergency response team (Instructor), who can help take drastic measures to regain control of your environment ☺

That’s about it... We like to keep it creative ☺

**The Instructor has a role as Coordinator and thus coordinates the capstone.
In the event of confusion / argument, the Instructor has the final say!**

This page intentionally left blank.

QUESTIONS?

???

If you have any questions, now is the time to ask them...

This page intentionally left blank.

Course Roadmap

- Introduction & Key Tools
- Initial Access
- Lateral Movement
- Persistence
- Azure AD & Emulation Plans
- **Adversary Emulation Capstone**

SEC699.6

Capstone

- Capstone Introduction – Live Events
- Capstone Introduction – OnDemand

This page intentionally left blank.

SEC699 CTF INTRODUCTION

Welcome to the final exercise of the course. This final exercise is designed to represent the knowledge and skills covered throughout the entire SEC699 course.

You will earn points in three different areas:

- Trivia (Knowledge)
- Blue (Detection)
- Red (Attacks)

There is a new LAB environment specifically for this challenge.

The intended solution is provided in a separate document, containing the word ANSWERS in the filename.

This page intentionally left blank.

SEC699 CTF SCOREBOARD

- The scoreboard is at **<https://ctf.sec699.org/>**
- Register yourself an account to begin
 - USERNAME is a nickname for display
 - EMAIL is also your LOGINID
 - MUST be a valid, usable account
 - VALIDATION link will be sent here
 - PASSWORD complexity is enforced; each requirement changes from yellow to green when satisfied.

CAPTURE THE FLAG

LOGIN REGISTER

REGISTER

USERNAME

EMAIL

CONFIRM EMAIL

PASSWORD

REQUIRED: 10+ CHARACTERS // LOWERCASE // UPPERCASE
// NUMBERS // SPECIAL CHARACTERS 167%

This page intentionally left blank.

SEC699 CTF SCOREBOARD REGISTRATION

- IF any field is invalid, you will need to use a different value
 - Erroneous
 - Already in-use
- Notice the color changes from yellow to green as the PASSWORD complexity rules are satisfied
- Once you complete this form, click on the confirmation link sent to your provided email address

REGISTER

USERNAME
SOME GUY

EMAIL
jshewmaker@sans.org

CONFIRM EMAIL
jshewmaker@sans.org

PASSWORD
.....|

REQUIRED: 10+ CHARACTERS // LOWERCASE // UPPERCASE
// NUMBERS // SPECIAL CHARACTERS 1#7%

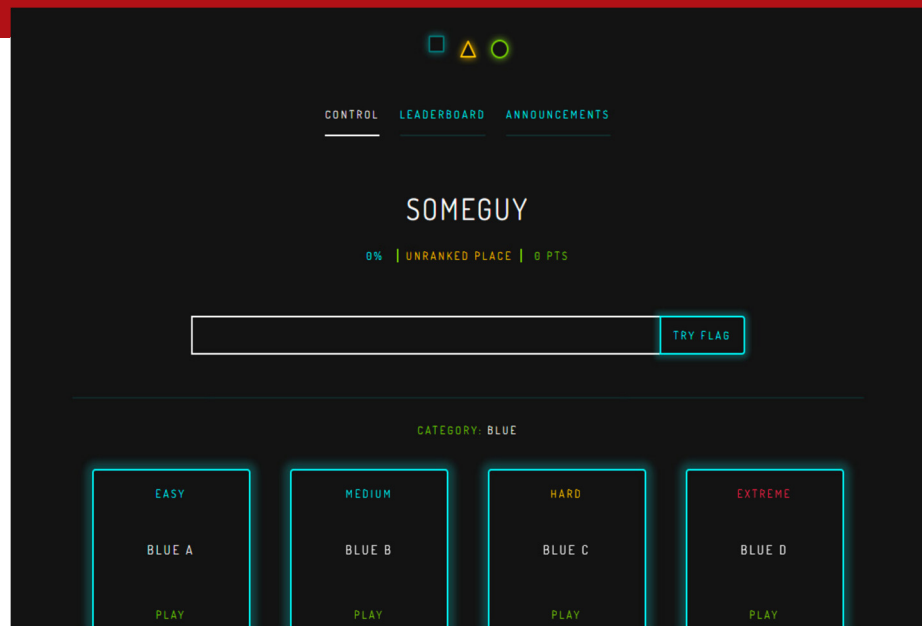
CONFIRM PASSWORD

REGISTER

This page intentionally left blank.

BEGIN!!

- Click any challenge to read the instructions
- Submit any valid flag as you solve each challenge



This page intentionally left blank.

SOLVE!!

- Read the challenge carefully
- Solve the challenge
- Submit a flag in top field
- Click “TRY FLAG”
- IF flag is valid for any challenge
 - success message will show
 - visual indicator on main view will change to green



This page intentionally left blank.

SEC699 CTF WIKI: [HTTPS://CTF-WIKI.SEC699.ORG](https://ctf-wiki.sec699.org)

These challenges are designed to reflect the content in the course, though you may use any tools or resources which you have legal access and permission to use.

The CTF specific wiki is at: <https://ctf-wiki.sec699.org/>

- Instructions to build the BLUE category challenges
- Instructions to build the RED category challenges
- Solutions to the challenges

This page intentionally left blank.

SEC699 CTF TIPS

You may discover easier or alternative solutions different than intended. Take good notes of your work so you can get the most out of your experience.

- Does a challenge seem similar to an exercise?
 - Review the exercise or topic from the course for general tool use and steps
- Are you reading TOO MUCH into a challenge and making it harder?
- Double-check syntax of commands
- Screenshot errors
- Contact your favorite SME for help

This page intentionally left blank.

COURSE RESOURCES AND CONTACT INFORMATION



AUTHOR CONTACT

James Shewmaker
jshewmaker@sans.org



SANS INSTITUTE

11200 Rockville Pike
Suite 200
North Bethesda, MD 20852
301.654.SANS (7267)



PENTEST CONTACT

Stephen Sims
ssims@sans.org



SANS EMAIL

GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org

This page intentionally left blank.

This page intentionally left blank.

Index

A

Access Control Entry (ACE)	3:22, 3:173-178, 4:106, 4:108-129, 4:140-141
Access Tokens	5:62
Active Directory (AD)	1:5, 1:89, 2:64, 2:67, 3:4, 3:16, 3:22, 3:26, 3:30, 3:92, 3:107, 3:118, 3:134, 3:136, 3:145, 3:149, 3:162, 3:164, 3:171-175, 3:183, 3:187, 4:7-9, 4:19, 4:21, 4:23, 4:107-109, 4:111-130, 4:132-134, 4:136-137, 4:147, 5:1, 5:4-20, 5:22, 5:24-38, 5:41-43, 5:47-53, 5:55, 5:58, 5:60-66, 5:68, 5:70-71, 5:73-74
Active Directory Federation Services (ADFS)	5:24, 5:29, 5:32, 5:34-35, 5:43
Address Space Layout Randomization (ASLR)	4:93
Advanced Persistent Threat (APT)	1:43-44, 1:51, 2:9, 2:13, 2:108, 4:51, 5:77-78, 5:87, 5:89-90, 5:101, 5:103
Alternate Data Stream (ADS)	2:84
Amazon Web Services (AWS)	1:7-12, 1:17, 1:26, 5:45
Anomaly-Based Detection	1:106-117
Ansible	1:7, 1:13-20
Anti Malware Scanning Interface (AMSI)	2:18-28, 2:33, 2:35, 3:51, 4:130, 5:92, 5:105
Anti-Malware Scanning Interface (AMSI)	2:18-28, 2:33, 2:35, 3:51, 4:130, 5:92, 5:105
APIs	1:11, 1:74, 1:134, 1:141, 2:18-19, 2:81, 2:90-91, 2:94, 2:119, 2:121-123, 2:126, 2:139-141, 5:7, 5:16, 5:32
AppCert	4:3, 4:58-60, 4:65, 4:67, 4:69, 4:85, 4:149-150
AppCert DLLs	4:3, 4:59
AppCert_DLL Persistence	4:58
AppCertDLLs	4:3, 4:58-59, 4:65, 4:67, 4:69
AppInit	4:3, 4:60-61, 4:65, 4:68-69, 4:149-150
AppInit DLLs	4:3, 4:68
AppInit_DLLs	4:3, 4:60-61, 4:65, 4:68-69
Application Programming Interface (API)	1:68, 1:140-141, 1:147, 2:4, 2:19, 2:21,

	2:23, 2:28, 2:33, 2:38, 2:64, 2:81-82, 2:90-95, 2:102, 2:104-105, 2:111, 2:113, 2:120-124, 2:126, 2:129, 2:139-141, 3:2, 3:51-52, 3:61, 3:121, 4:3, 4:58, 5:7, 5:16, 5:42, 5:56-57, 5:105
Application Whitelisting	1:124, 5:79, 5:105
AppLocker	2:7, 2:38-47, 2:52-54, 2:144, 2:148, 5:80, 5:92, 5:105
Applocker Bypass	2:39, 2:42-44, 2:54
APT-28	1:44, 1:51, 5:77-78, 5:87
APT-34	5:89-90, 5:101
APT3	1:43, 5:89
ArcSight	1:62
ASN.1	3:141
ASReproast	3:137-138, 3:141, 3:143
Atomic Red Team	1:26, 1:101, 1:122-123
ATT&CK	1:4, 1:30, 1:33-37, 1:39-41, 1:43, 1:50, 1:62, 1:68, 1:82, 1:86, 1:96-97, 1:101, 1:122-123, 1:126, 1:132-134, 1:152, 1:157, 1:161, 2:9-10, 2:97, 3:110, 4:106, 5:77-85, 5:89-99, 5:103-110
Attack Surface	1:135, 2:7, 2:60, 2:63-84, 2:86, 2:144, 2:148, 5:79
Attack Surface Reduction (ASR)	2:7, 2:63-84, 2:86, 2:144, 2:148, 5:79
Authentication Packages	3:37-41, 4:62
Autoruns	4:49, 4:54, 4:69, 4:84, 4:150-154, 5:82, 5:98
Azure	1:5, 1:11, 1:17, 1:26, 2:9-11, 3:22, 3:183, 3:188, 5:1, 5:4-20, 5:22, 5:24-39, 5:41-43, 5:47-53, 5:55-66, 5:68, 5:70-71, 5:73-75, 5:95
Azure Active Directory	5:4-9, 5:11, 5:13, 5:17, 5:26, 5:30, 5:35, 5:41, 5:43, 5:47, 5:49, 5:55, 5:58
Azure Active Directory (Azure AD)	5:4-9, 5:11, 5:13, 5:17, 5:26, 5:30, 5:35, 5:41, 5:43, 5:47, 5:49, 5:55, 5:58
Azure AD	1:5, 3:22, 5:1, 5:4-16, 5:18-20, 5:22, 5:24-38, 5:41-43, 5:47-53, 5:55, 5:58, 5:60-66, 5:68, 5:70-71, 5:73-74
Azure AD Graph	5:16
Azure Information Protection	5:17

B

Basic	1:4, 1:15, 1:37, 1:104, 1:130, 1:154, 2:2, 2:37-38, 2:51, 2:54, 2:63, 2:69-70, 2:74, 2:77, 2:89, 2:122, 3:21, 3:23, 3:38, 3:111, 4:74, 5:5-6, 5:45, 5:56
Binaries	1:137, 1:144, 1:146, 2:2, 2:38, 2:42, 2:44, 2:133-134
BloudHound	4:132-133
Bourne Again SHell (bash)	2:15, 4:85
brute-force	3:133, 3:137-138, 5:19

C

C++	1:58, 2:113, 2:123, 3:13, 4:33
CALDERA	1:5, 1:22, 1:26, 1:122, 1:126, 1:132, 1:152-171, 1:173
Celery	1:124
CERT-BDF	1:69
Cisco	1:15-16
Cloud Only Identity	5:24
Cobalt Strike	1:122, 2:98, 2:101, 2:107-108, 2:111
COM hijacking	1:37, 1:44, 4:27, 5:77, 5:103-104, 5:106
COM Object Hijacking	1:5, 2:77, 4:2, 4:27-39, 4:41, 4:150, 5:106
COM Object Linking	4:36-38
COM Search Order Hijacking	4:27, 4:30-35
Command and Control (C&C)	1:135, 5:85
CompilerInput	2:47, 2:49-50
Component Object Model (COM)	1:5, 1:22, 1:37, 1:44, 1:111-117, 2:2, 2:19, 2:42-43, 2:74-77, 4:2, 4:6-7, 4:10-17, 4:27-39, 4:41, 4:150, 5:77, 5:103-104, 5:106
Compromised credentials	5:22
Covenant	1:5, 1:22, 1:122, 1:135-141, 2:97
CreateProcess()	4:58
CreateProcessAsUser()	4:58
CreateProcessWithLoginW()	4:58
CreateProcessWithTokenW()	4:58
Credential Dumping	1:5, 3:3, 3:45-46, 3:51, 3:83, 3:95, 3:103, 3:181, 3:187-188, 5:77, 5:89-90, 5:97, 5:103-104, 5:107
Cscript	1:137, 2:15, 4:85
Cuckoo	1:69

Cyber Kill Chain	1:33
------------------	------

D

Data Aggregation	1:109
DCYNC attack	5:97
Delegation	1:5, 1:146, 3:23, 3:25, 3:118-119, 3:141, 3:145-157, 3:159, 3:161-183, 3:185, 4:20-22
Democratic National Committee (DNC)	5:77
DeTACCT	1:82
Detect Tactics, Techniques & Combat Threats (DeTTECT)	1:82, 1:96-100
Discretionary Access Control List	4:107
Discretionary Access Control List (DACL)	3:173, 4:107-108, 4:116, 4:129
DNS logs	1:57, 1:64
Domain Controller (DC)	1:10, 1:22, 1:26, 3:3, 3:17, 3:23, 3:28, 3:30, 3:38, 3:45, 3:87, 3:92-94, 3:99-100, 3:107, 3:133, 3:137-140, 3:151-154, 3:156, 3:163, 3:165, 3:181, 4:12-15, 4:17, 4:20-21, 4:138, 5:7, 5:13, 5:15, 5:24, 5:26, 5:30, 5:33, 5:35, 5:73, 5:83, 5:97
Domain Functional Level (DFL)	3:142, 4:106
Domain Name Services (DNS)	1:57, 1:64, 1:66, 1:85, 1:111, 1:143-146, 3:116-117, 3:120-121, 5:18
Domain Trust	3:2, 3:187, 4:6, 4:18-19
Duo	5:45
Dynamic-link libraries (DLLs)	1:147, 2:42, 2:62, 2:91, 2:94, 2:107, 2:123, 2:127, 2:129-131, 2:134-136, 3:37, 3:60-61, 3:64, 4:3, 4:28, 4:58-63, 4:65, 4:67-69, 4:80, 4:92-93, 4:97, 4:150

E

ElastAlert	1:61-62, 1:66, 1:71, 1:74
Elastic	1:8, 1:22, 1:57-62, 1:65-66, 1:68, 1:71, 1:74, 1:95, 1:111-118, 1:120, 6:12-13
ElasticSearch	1:58-62, 1:71, 1:74, 1:95, 1:111-118
ElasticSearch, Logstash, and Kibana (ELK)	1:14, 1:58, 1:74
Endpoint Detection and Response (EDR)	1:57, 1:75-80, 1:94, 1:143, 2:7-9, 2:14,

	2:94, 2:97, 2:121-122, 2:126-137, 2:141, 3:5, 3:14, 3:87, 5:72, 5:81
event logs	1:57, 1:73, 1:83, 1:97, 5:97
Event Tracing for Windows (ETW)	1:87-91, 1:94-95, 2:109-110, 2:142, 2:149, 3:13-14, 5:81
Evil Clippy	2:31
EWS Cracker	5:45
Exchange Web Services (EWS)	5:20-21, 5:45

F

Faction C2	1:122, 1:141-142
False Positives	1:64, 1:104-105, 1:108, 2:54, 2:143-144, 3:56, 3:83, 5:75, 5:80
Federated Identity	5:24
Federation Integration (FI)	5:29
firewall logs	1:57, 5:74
Forest	1:22, 3:2, 3:183, 4:6-11, 4:15-22, 4:25, 5:7-8, 5:27-28, 5:90
Full Packet Captures (FPC)	1:57
Fully Qualified Domain Name (FQDN)	1:145

G

Get-AppLockerPolicy	2:39
Golden ticket	3:3, 3:22, 3:43, 3:93, 3:139, 3:156, 3:182-183, 4:17, 4:19, 5:73
Grafana	1:111
Graph Security	5:56-57
GraphFrames	1:74
Group Policies	2:65, 3:17, 3:28, 5:7
GRR Rapid Response (GRR)	1:75-76

H

Hadoop	1:74
Hijacking	1:5, 1:37, 1:44, 2:77, 2:105, 3:171, 3:175, 3:177-178, 4:2, 4:27-39, 4:41, 4:150, 5:77, 5:103-104, 5:106
HKEY_CURRENT_USER (HKCU)	1:107, 1:110, 2:77, 4:27, 4:30-32, 4:34, 4:37, 4:39, 4:79, 4:81, 4:84, 4:86, 4:150,

	5:106
HKEY_LOCAL_MACHINE (HKLM)	1:88, 3:19, 3:88, 3:91, 3:99, 3:101, 4:3, 4:27, 4:30-32, 4:34, 4:39, 4:59, 4:61-63, 4:65, 4:67, 4:69, 4:99, 4:101-102
HTML Application (HTA)	2:53
Hunting ELK (HELK)	1:74

I

Identity Access Management (IAM)	5:58
Indicators Of Compromise (IOCs)	1:30, 1:69
Infection Monkey	1:122, 1:125-131
Infrastructure as a Service (IaaS)	1:68, 5:4
Initial Access	1:5, 1:43-44, 2:6, 5:78-79, 5:90, 5:104
Install-Module	5:11
InstallUtil	1:137, 2:2, 2:42, 2:44-46, 2:54, 2:148-149
InstallUtil.exe	2:2, 2:42, 2:44-46, 2:54

J

Java	1:58, 1:74, 2:53, 2:63-64, 2:83-84, 2:106, 5:56
Java Web Token (JWT)	5:35
JavaScript Object Notation (JSON)	1:58, 1:66, 1:95, 1:161, 4:154, 5:56
JSON Web Token (JWT)	5:35
Juniper	1:15-16
Jupyter	1:72-74

K

Kafka	1:74
Kekeo	3:141
Kerberoast	3:3, 3:24, 3:119, 3:137, 3:141-143, 3:150, 3:187-188, 4:135, 5:78, 5:83
Kerberos	1:5, 1:15, 1:91, 3:3, 3:22-23, 3:37-40, 3:43, 3:45-46, 3:58, 3:87, 3:93, 3:107, 3:118-119, 3:129-142, 3:145-150, 3:154-156, 3:161-162, 3:166-168, 3:179, 3:181-183, 3:188, 4:7-9, 4:12-15, 4:19, 5:7, 5:35-36, 5:38-39, 5:73, 5:83, 5:95
Kibana	1:58, 1:60, 1:66, 1:68, 1:71, 1:74, 1:111

KSQL	1:74
------	------

L

Lateral movement	1:5, 1:43-44, 1:73, 3:1-4, 3:16, 3:36, 3:181, 4:43, 5:73, 5:78, 5:82, 5:84, 5:90, 5:95, 5:97, 5:104, 5:107
Link-Local Multicast Name Resolution (LLMNR)	3:108, 3:120, 3:124-125
LoadAppInit_DLLs	4:61
Local Administration Password Solution (LAPS)	4:137
Local Security Authority (LSA)	3:37, 3:39-41, 3:43-45, 3:53-55, 4:62
Logstash	1:58, 1:60, 1:66, 1:68, 1:71, 1:74
LSASS	1:91, 1:104, 2:94, 2:121, 3:30, 3:36-60, 3:64-83, 3:85, 3:87, 3:95, 3:103, 3:129, 3:187-188, 5:107-108

M

MailSniper	5:20-21
Metasploit	1:122, 1:133-134, 3:43
Microsoft Cloud App Security (MCAS)	5:48
Microsoft Graph	5:16, 5:42, 5:56-57
Mimikatz	1:104-105, 2:24, 3:16, 3:37, 3:42-48, 3:53-54, 3:58, 3:60, 3:65-70, 3:77-79, 3:81-83, 3:92-94, 3:139, 3:141, 3:148, 3:156-157, 3:187, 4:17, 4:19, 4:138, 5:38-39, 5:107-108
MITRE	1:4, 1:26, 1:30, 1:33-41, 1:43, 1:50, 1:62, 1:68, 1:82, 1:86, 1:97, 1:99-101, 1:122-123, 1:132-134, 1:152-171, 2:2-4, 2:9-10, 2:97, 2:103, 2:108, 3:2-3, 3:110, 4:2-4, 4:51, 4:58, 4:60, 4:62-63, 4:73, 4:106, 5:77-85, 5:89-99, 5:103-110
Monkey-MSSQL1	1:129, 1:131
MS-KILE	3:136
MSBuild	1:137, 2:53-54
Mshta	1:137, 2:15, 2:53-54, 4:85
Multi-Factor Authentication (MFA)	2:12, 5:6, 5:16, 5:22, 5:33, 5:45, 5:47-48, 5:53, 5:55, 5:63, 5:66, 5:68-70

Mutual-TLS	1:143
------------	-------

N

Netbios Name Server (NBT-NS)	3:108
No-DACL	4:108
North Atlantic Treaty Organization (NATO)	5:77
NT LAN Manager (NTLM)	1:15, 3:37-40, 3:46, 3:87, 3:93, 3:96, 3:99-101, 3:103, 3:107-109, 3:111-116, 3:120-121, 3:123, 3:136, 3:157, 3:181, 3:188, 4:7-9, 4:12, 5:7, 5:38
NTLM	1:15, 3:37-40, 3:46, 3:87, 3:93, 3:95-103, 3:105, 3:107-121, 3:123, 3:125, 3:127, 3:136, 3:157, 3:181, 3:188, 4:7-9, 4:12, 5:7, 5:38
Null-DACL	4:108

O

OAuth	2:12-13, 3:161-162, 3:164-166, 3:180, 5:7, 5:37, 5:42-44, 5:56
Office Macros	2:81-82, 2:102, 2:119
Okta	5:45
OpenID	5:7, 5:10, 5:41, 5:43-44, 5:56
Organization for Security and Co-Operation in Europe (OSCE)	5:77
OSQuery	1:26, 1:111-117, 4:50, 4:54, 4:100, 4:102, 4:150-151, 4:155, 5:82, 5:98
Ownership Hijacking	3:177-178

P

Parent-child trust	4:6, 4:8, 4:10-11, 4:16
Pass the Hash (PtH)	1:44, 5:96
Pass the Ticket (PtT)	3:3, 5:95
Pass-Through Authentication (PTA)	3:38, 5:13, 5:29, 5:32, 5:35
Password Hash Synchronization (PHS)	5:27, 5:29-32, 5:35
Password Reuse	5:22
Password Spraying	5:15, 5:19-21
Phantom COM Object Hijacking	4:28-29

Phantom COM objects	4:27-29
Ping	5:45
Pivot	1:129, 4:18-21, 4:25, 5:90
playbook	1:7, 1:13-14, 1:16-20, 1:72-73, 1:101
PowerShell	1:15, 1:44, 1:88, 1:95, 1:106-107, 1:109-110, 1:126, 1:134-135, 1:137, 1:153, 1:168-171, 2:3, 2:15, 2:18, 2:20, 2:23-24, 2:26-28, 2:39, 2:46, 2:51, 2:67, 2:84, 2:102, 2:111, 2:115, 2:119-120, 2:131, 2:134, 2:144, 2:148-149, 3:19, 3:43, 3:51, 3:89, 3:149, 3:162, 3:164, 3:172-179, 4:33, 4:35, 4:45, 4:49, 4:85, 4:130, 4:154, 5:7, 5:11, 5:20-21, 5:89-90, 5:92, 5:105
PowerShell (PSI)	1:15, 1:44, 1:88, 1:95, 1:106-107, 1:109-110, 1:126, 1:134-135, 1:137, 1:153, 1:168-171, 2:3, 2:15, 2:18, 2:20, 2:23-24, 2:26-28, 2:39, 2:46, 2:51, 2:67, 2:84, 2:102, 2:111, 2:115, 2:119-120, 2:131, 2:134, 2:144, 2:148-149, 3:19, 3:43, 3:51, 3:89, 3:149, 3:162, 3:164, 3:172-179, 4:33, 4:35, 4:45, 4:49, 4:85, 4:130, 4:154, 5:7, 5:11, 5:20-21, 5:89-90, 5:92, 5:105
PowerShell Empire	1:106, 1:135
PowerShell Remoting	1:15
PowerSploit	3:42, 3:51, 3:172, 4:130
Privilege Account Certificate (PAC)	3:122, 3:129-130, 3:132-136, 3:139, 3:147, 4:13-15, 4:19
Privileged Identity Management (PIM)	5:6, 5:17, 5:66
ProcDump	1:104, 3:42, 3:50, 3:57, 3:69-70
Process Creation	1:85, 1:104, 2:15, 2:54, 2:64, 2:111, 2:119, 2:144, 2:149, 3:30, 3:56, 3:83, 3:103, 3:143, 3:183, 3:187-188, 4:22, 4:43, 4:48, 4:54, 4:66, 4:69, 4:85-86, 4:102, 4:150-151, 5:79-80, 5:93-94, 5:99, 5:105, 5:109-110
Process Environment Block (PEB)	2:99-101, 2:104, 2:109
Property Write-Rights	3:177
PSEXec	1:80, 2:64
PWDump	1:104, 3:60, 3:65
Python	1:13, 1:15-16, 1:58, 1:72, 1:74, 1:94, 1:124, 3:111-115, 3:117, 5:20, 5:45

Q

Qradar

1:62

R

Rabobank	1:82, 1:96-100
Reconnaissance	2:6, 3:119, 5:18, 5:93, 6:12
Red Canary	1:40-41, 1:123
Red Team Automation (RTA)	1:122
Redis	1:124
registry	1:85, 1:88-89, 1:107, 2:42, 2:67, 2:77, 3:19, 3:88, 3:96, 3:99-103, 3:188, 4:2-3, 4:27-31, 4:34, 4:36, 4:39, 4:58-60, 4:62-63, 4:65, 4:67-69, 4:79, 4:81-82, 4:84, 4:86, 4:93, 4:99, 4:101-102, 4:150-152, 5:79, 5:98, 5:109
Regsvr32	1:124, 1:137, 2:15, 2:54, 2:119, 4:85
Remote Procedure Call Service (RPCS)	5:84
RequireSignedAppInit_DLLs	4:61
Resource-Based Constrained Delegation (RBCD)	3:145, 3:170-180, 4:109, 4:138
REST	1:141, 5:7, 5:56-57
RIGHT_DELETE	4:118
RIGHT_DS_CONTROL_ACCESS	4:119
RIGHT_DS_CREATE_CHILD	4:127
RIGHT_DS_DELETE_CHILD	4:126
RIGHT_DS_DELETE_TREE	4:121
RIGHT_DS_LIST_CONTENTS	4:120, 4:125, 4:142
RIGHT_DS_LIST_OBJECT	4:120
RIGHT_DS_READ_PROPERTY	4:123
RIGHT_DS_WRITE_PROPERTY	3:178, 4:122, 4:124
RIGHT_DS_WRITE_PROPERTY (WP)	3:178, 4:122, 4:124
RIGHT_DS_WRITE_PROPERTY_EXTENDED	4:124
RIGHT_GENERIC_ALL	4:114
RIGHT_GENERIC_EXECUTE	4:113
RIGHT_GENERIC_READ	4:111
RIGHT_GENERIC_WRITE	4:112
RIGHT_READ_CONTROL	4:117, 4:140
RIGHT_WRITE_DAC	4:116, 4:129
RIGHT_WRITE_OWNER	3:177, 4:115, 4:129
Role Based Access Control (RBAC)	5:58, 5:60

RSA NetWitness	1:62
Rubeus	3:141, 3:143, 3:148, 3:152-157, 3:166-168, 3:179, 3:181, 3:187, 4:22
Ruler	5:20
rundll32.exe	2:15, 2:52, 4:85, 5:80

S

S4U2proxy	3:145, 3:161-169, 3:181
S4U2self	3:145, 3:161-162, 3:164-169
Sandbox	1:69, 1:108, 2:30, 2:113, 5:79
Sandcat	1:153, 1:165
Secure SHell (SSH)	1:15-16
Security Assertion Markup Language (SAML)	5:7, 5:10, 5:35, 5:37, 5:41, 5:43
Security Center	5:17
Security Descriptor	3:73-76, 3:171, 3:174, 4:106-127, 4:129-144
Security Identifier (SID)	3:134-135, 3:173, 3:175-177, 4:13, 4:19-20, 4:22, 4:107, 4:109, 5:38
Security Information and Event Management (SIEM)	1:46, 1:60-61, 1:66-67, 1:101, 1:103, 5:74
Security Orchestration, Automation and Response (SOAR)	1:57, 1:60
Security Reference Monitor (SRM)	4:128, 4:140-141
Security Support Provider (SSP)	3:37-41, 3:44, 3:46, 3:48, 3:87, 3:96, 4:62
Sentinel	5:57, 5:74-75
SequentialWorkflowActivity	2:47-48
Server Message Block (SMB)	1:128, 1:131, 1:137, 2:6, 3:19, 3:27, 3:30-31, 3:117-118, 3:120, 3:125, 3:150-151, 3:157, 3:187, 5:84, 5:94
Set-ADObject	3:180
Set-Content	2:39
ShellBrowserWindow	2:74-76
ShellShock	1:129, 1:131
SIGMA	1:57, 1:61-68, 1:71, 1:74, 1:82, 1:101, 1:120, 2:15-16, 2:54, 2:144, 3:29-30, 3:57-59, 3:64, 3:66, 3:71-72, 3:82, 3:91, 3:94, 3:102-103, 3:142-143, 3:183, 4:22, 4:51-53, 4:66-68, 4:85, 4:97, 4:102, 5:96, 5:99
SilkETW	1:87, 1:95
SilkService	1:95

Silver ticket	3:139, 5:38-39, 5:73
Single Sign-On (SSO)	3:111, 5:6, 5:10, 5:19, 5:35-39, 5:41
Single-Sign On (SSO)	3:111, 5:19, 5:35-39
Skeleton key	3:139-140
Sliver	1:143-146
SMB Exploit	1:128, 2:6
SOAR	1:57, 1:60
Socket.IO	1:141
Spark	1:74
Spearphishing	1:44, 2:3, 5:78-79, 5:90-91
Splunk	1:26, 1:58-59, 1:62
Spraying Toolkit	5:20
Stockpile	1:161-162, 1:164-165
Synchronized Identity	5:24
syslog	1:57-58
Sysmon	1:26, 1:57, 1:73, 1:82, 1:84-87, 1:93, 1:104, 2:15, 2:54, 2:97, 2:101, 2:139-144, 2:149, 3:5-14, 3:29-30, 3:56-60, 3:64-71, 3:77-79, 3:81, 3:83, 3:91, 3:102-103, 3:143, 3:183, 3:187-188, 4:22, 4:47-48, 4:51-54, 4:66-69, 4:85-86, 4:102, 4:150-151, 5:79-80, 5:84, 5:93-94, 5:99, 5:105, 5:107-110, 6:13
System Access Control List (SACL)	4:107, 4:117

T

Tactics, Techniques & Procedures (TTPs)	1:30, 1:32, 1:42, 1:134
TGS-REP	3:3, 3:129-130, 3:132-136, 3:147, 3:163, 4:14-15, 5:83
TGS-REQ	3:129, 3:133-136, 3:147, 3:163, 4:14-15
TheHive	1:22, 1:57, 1:61, 1:69-71, 1:101
Ticket-Granting Service (TGS)	3:3, 3:129-130, 3:132-136, 3:147, 3:163, 4:14-15, 5:83
Ticket-Granting Ticket (TGT)	3:3, 3:38, 3:129, 3:131-136, 3:139, 3:146-148, 3:150-156, 3:161, 3:163, 4:13-14, 4:21-22, 5:83, 5:95
Tree-Root	4:6, 4:8, 4:10-11, 4:16
Tree-root trust	4:6, 4:10-11, 4:16
Trust direction	4:7
Trust transitivity	4:7-8
Turla	5:103-104, 5:112

U

Uber Metta 1:122, 1:124

V

Vault	1:20, 5:61-62
VECTR	1:22, 1:47-53, 1:55
Velocidex Query Language (VQL)	1:75, 1:77, 1:80
Velociraptor	1:57, 1:75-80, 6:12
VirusTotal	4:152-153
Visual Basic for Applications (VBA)	2:2, 2:19, 2:30-33, 2:35, 2:67, 2:81-82, 2:102, 2:119, 3:111, 4:73, 4:75-76, 4:86
VMWare	1:17, 1:26

W

WCE	1:104, 3:60, 3:65-66
web proxy logs	1:57, 5:91
Whitelisting	1:124, 2:54, 3:72, 5:79, 5:105
Windows Defender Application Control (WDAC)	5:92
Windows Defender ATP	1:62
Windows Management Instrumentation (WMI)	2:64, 2:142, 4:2, 4:43-54, 4:56, 4:149-150, 4:155, 5:78, 5:84
Windows Remote Management (WinRM)	1:15
Windows Script Host (WSH)	5:105
WinExec()	4:58
Wmic	1:137, 2:15, 2:119, 4:85
WriteDacl	4:108, 4:129
WriteOwner	4:108, 4:129
WS-Federation	5:43
Wscript	1:137, 2:15, 2:77, 2:144, 4:85

X

X.509	1:143
-------	-------

Y

YAML Ain't Markup Language (YAML)	1:13-14, 1:17-18, 1:20, 1:64, 1:66, 1:78, 1:96, 1:98, 1:124, 1:161-162, 1:164
Yelp	1:61, 1:71
Yet Another Markup Language (YAML)	1:13-14, 1:17-18, 1:20, 1:64, 1:66, 1:78, 1:96, 1:98, 1:124, 1:161-162, 1:164