

# SEC588 – Cloud Penetration Testing

## Topics

### Architecture, Discovery, & Recon at Scale

Introduction	588.1–9-17
Cloud Assessment Methodology	588.1–18-21
Terms of Serv. & Demarcatoins Points	588.1–22-34
Ngrok	588.1–35-39
Recon at Cloud Scale	588.1–42-54
Discovery Tools & Wordlists	588.1–55-59
IP Addressing & Hosts	588.1–63-77
Mapping URLs	588.1–81-90
Commonspeak2 Wordlists	588.1–91-96
Visualizations During Recon	588.1–100-105
Asset Discovery Frameworks	588.1–106-112
Appendix	588.1–117-128

### Attacking Identity Systems

Mapping Process	588.2–5-12
Authentications & Key Material	588.2–13-19
AWS CLI	588.2–22-28
URL and URIs	588.2–31-37
AWS IAM	588.2–38-48
Azure CLI	588.2–49-53
Username Harvesting in the Cloud	588.2–54-56
Unauthenticated File Shares	588.2–59-62
Introduction to Microsoft Services	588.2–65-68
Microsoft Identity Services	588.2–69-78
Azure AD & RBAC	588.2–79-85
Authentication Standards	588.2–86-105
Golden SAML Attacks	588.2–106-110
Postman for APIs	588.2–111-123

### Attacking & Abusing Cloud Services

Mimikatz & PRT	588.3–5-9
Microsoft Graph	588.3–10-16
AWS IAM Privilege Escalation	588.3–19-28
Introduction to socat	588.3–29-37
AWS Compute	588.3–40-43
Compute Attack Scenarios	588.3–46-51
Amazon KMS	588.3–54-57
Pacu	588.3–58-67
Azure VMs	588.3–70-74
Code Execution on Azure	588.3–77-83

### Vulnerabilities in Cloud-Native Applications

Introduction to Cloud Native Attacks	588.4–4-10
Cloud Native Applications	588.4–11-16
Deployment Pipelines & Attacks	588.4–17-29
Web Application Injections	588.4–32-34
Server-Side Request Forgeries	588.4–35-41
Command Line Injections in Appls	588.4–44-50
Serverless Function with Lambda	588.4–53-60
Serverless Function with Azure	588.4–61-64
Exposed Databases	588.4–67-79
SQLi in a Hosted Environment	588.4–82-95
Containers & Microservices	588.4–98-106
Appendix	588.4–107-111

### Infrastructure Attacks and Red Teaming

Kubernetes & Service Meshes	588.5–4-23
Backdooring Containers	588.5–26-39
Red Team & Exploitation	588.5–42-46
Payloads & Payload Selections	588.5–47-59
Red Team Ops in the Cloud	588.5–62-72
Passwords Attacks	588.5–73-77
Pswd Attack Types & Methodologies	588.5–78-89
Obfuscating Architectures	588.5–92-102

## Categories









### Labs

Attacking with EC2	588.3–52-53
	588.W–118-124
AWS User Enumerations	588.2–29-30
	588.W–59-67
Azure VMs	588.3–75-76
	588.W–137-148
Backdooring CI/CD Pipelines	588.4–30-31
	588.W–159-169
Backdooring Containers	588.5–40-41
	588.W–218-229
Backdoors in Serverless Functions	588.4–65-66
	588.W–185-190
Command Line Injections	588.4–51-52
	588.W–175-184
CTF Challenge	588.W–256-258
Databases & Exposed Ports	588.4–80-81
	588.W–191-199
Domain Discovery Lab	588.1–60-62
	588.W–19-26
Domain Fronting Attacks	588.5–103-104
	588.W–250-255
EC2 Attack Setup	588.3–44-45
	588.W–109-117
Getting Started	588.1–40-41
	588.W–8-18
Gobuster & CommonSpeak2 WLS	588.1–97-99
	588.W–35-44
Heavy & Light Web Shells	588.5–60-61
	588.W–230-242
Hunting for Open File Shares	588.2–63-64
	588.W–75-80
Hunting Key Material	588.2–20-21
	588.W–51-58
Kubernetes & Peirates	588.5–24-25
	588.W–208-217
Microsoft Graph API	588.3–17-18
	588.W–90-100
PACU	588.3–68-69
	588.W–125-136
Password Attacks	588.5–90-91
	588.W–243-249
Port Scans at Scale in the Cloud	588.1–78-80
	588.W–27-34
Postman	588.2–124-125



# SEC588 – Cloud Penetration Testing

.....	588.W-81-89	Flippa 🌐	588.5-96
Running Commands on Azure VMs ..	588.3-84-85	GCC	588.5-49
.....	588.W-149-158	GitLeaks	588.W-54, 56, 58
Scaling Discovery	588.1-113-116	Gobuster	588.1-54, 85-90
.....	588.W-45-50	.....	588.2-60, 77
Socat	588.3-38-39	.....	588.W-40-43, 53
.....	588.W-101-108	GrayHatWarfare Buckets	588.2-12
SQL Injections	588.4-96-97	Hashes.org 🌐	588.5-76
.....	588.W-200-207	HaveIBeenPwned 🌐	588.5-76
SSRF Attack	588.4-42-43	Httpx	588.W-48-49
.....	588.W-170-174	Hydra	588.5-86-88
Username Harvesting & Azure CLI	588.2-57-58	.....	588.W-246-248
.....	588.W-68-74	Intrigue	588.1-108-112
		Ident	588.1-111-112
		.....	588.W-46, 48-49, 76
<b>Tools</b>		IpTables 🚒	588.3-35-36
Apache	588.3-35	John The Ripper	588.W-148
AutoSSH	588.5-27-28	Jq	588.2-11, 27-28, 53
Aws	588.2-11, 24-25, 28	.....	588.W-66, 100
EC2	588.2-25, 28	Kube-Hunter 🚒	588.5-21
.....	588.W-66	Kubeadm 🚒	588.5-10, 13, 22
KMS	588.3-57	Kubectrl	588.5-13, 39
.....	588.W-124	.....	588.W-212-217
Lambda	588.4-55, 58, 60	Secrets	588.5-16
S3	588.2-25	MailSniper	588.W-100
.....	588.5-69	Masscan	588.1-68-74, 77
.....	588.W-65	.....	588.W-27-31
STS	588.W-64	Workflow	588.1-73
Az	588.2-11, 50-51, 70-74	Metasploit 🚒	588.5-29-37, 99-102
AD	588.2-51	msfconsole	588.5-29-34, 51
.....	588.W-71	.....	588.W-226, 228
Disk	588.W-141	msfvenom	588.5-35-37, 99
Login	588.W-70	Meterpreter	588.4-28
Role	588.W-72	.....	588.5-31-36, 51, 98
VM	588.2-50, 53	Mimikatz	588.2-107
.....	588.3-72, 80	.....	588.3-6-9
.....	588.W-72-73, 141, 150-151	.....	588.4-111
AzCopy	588.5-70	Mongo	588.W-196-198
BFG Repo Cleaner	588.W-58	MosDef 🚒	588.5-48, 51
Burp Suite	588.5-86	Nabuu	588.W-48
Certbot	588.5-99-100	Netcat	588.3-30-31
CeWL 🚒	588.5-77	.....	588.4-28-29
China Chopper	588.5-54	Netsh 🚒	588.3-35, 37
Cobalt Strike	588.5-52	NetSPI Microburst	588.1-83
Commonspeak2	588.1-92-95	NfTables 🚒	588.3-35
.....	588.W-21, 35-38	Nginx	588.3-35
Containerd	588.1-123-125	Ngrok	588.1-36-41
CURL	588.5-49	.....	588.4-28
Dism 🚒	588.3-73-74	.....	588.W-15-18, 104
DNSRecon	588.1-54, 57-59	Options	588.1-38
.....	588.W-22-24	Nmap	588.1-75-77, 103-104
Docker	588.1-109, 112, 125-126	.....	588.4-69
.....	588.W-225, 227	.....	588.W-31-33
Build	588.5-37	Ntop	588.1-71
Docker-Compose	588.1-125	Nuclei	588.W-49
Domain Hunter 🚒	588.5-94-95	PACU 🚒	588.3-59-67
env 🚒	588.4-50	Enum	588.3-62
EyeWitness	588.1-103-105	Proxy	588.3-67
.....	588.W-45, 47		

# SEC588 – Cloud Penetration Testing

Recon .....	588.3–62
Patator .....	588.5–86
Peirates  .....	588.5–22-23
PortProxy (Netsh interface)  .....	588.3–35
Postman .....	588.2–112-123
.....	588.W–93-99
Limitations .....	588.2–114
Microsoft Graph Collection .....	588.3–14
Supported Methods .....	588.2–119
PowerCat .....	588.W–151
PowerShell Empire .....	588.W–151
ProxyCannon-NG .....	588.5–65
PW-Inspector .....	588.5–89
Redis-CLI .....	588.W–194
RunC .....	588.1–123, 125
Scanrand .....	588.1–68
Secretsdump.py  .....	588.W–142, 147
Sequelize  .....	588.4–95
set  .....	588.4–50
ShhGit .....	588.W–54, 56
SHIMIT  .....	588.2–105, 109-110
ShuffleDNS .....	588.1–54
.....	588.W–25
Socat .....	588.1–39
.....	588.3–30-34
.....	588.W–101-104
Bash Support .....	588.W–102
SQLmap  .....	588.4–91-94
.....	588.W–202, 206-207
Storage Explorer  .....	588.2–60
.....	588.3–74
.....	588.W–78-80, 138-140
UnicornsCan .....	588.1–68
Wappalyzer .....	588.5–99
Zmap .....	588.1–68

## A

AAA .....	588.2–39
AaaS .....	588.1–27
ABAC .....	588.2–39, 48
Abuse .....	588.2–56, 76, 78
.....	588.3–24
.....	588.4–39
.....	588.5–97
Acceptable Rate .....	588.1–73
Access Control List .....	588.2–42
Access Token .....	588.2–14, 91, 93
.....	588.3–27, 55
Account Attack .....	588.5–84
Account Lockout .....	588.5–80-83
Accuracy .....	588.1–74
ACK .....	588.1–72
ACL .....	588.2–12
ACME .....	588.1–49-50
.....	588.5–100
Active Directory .....	588.2–70, 72
as a Service → ADaaS .....	
Authentication .....	588.2–71
Connector .....	588.2–76
Attacker's View .....	588.2–78
Domain Services .....	588.2–70
Federated Services .....	588.2–70, 73
Active Technique .....	588.1–47
ActiveRecord .....	588.4–86
ADaaS .....	588.1–27
.....	588.2–70, 76
ADFS .....	588.2–39, 70, 73, 77, 105, 108
Administrator Account .....	588.3–80
Administrator Roles .....	588.2–75
Agent .....	588.5–51-54, 101
Akamai (Proxy)  .....	588.5–98
Allow Model .....	588.2–44
Allowances .....	588.1–23
Alpine Linux .....	588.4–50
.....	588.5–49
Amazon DocumentDB .....	588.4–70
Amazon Web Services .....	588.1–17, 20, 28, 50, 67, 82
.....	588.2–11
Certification Manager .....	588.1–50
CLI .....	588.2–11, 14, 23-28
Credentials .....	588.2–24
.....	588.3–27
Options .....	588.2–24-26
Profile .....	588.2–24
ECR .....	588.5–36
EKS .....	588.3–51
IAM .....	588.2–23, 39-48, 67
.....	588.W–65
Administrator  .....	588.2–45
Deny .....	588.2–41
Permissions .....	588.5–67-68
Policy .....	588.2–42-48
Privilege Escalation .....	588.3–20
User Versioning .....	588.3–22-24

# SEC588 – Cloud Penetration Testing

Lambda .....	588.4–55, 110
Constraints .....	588.4–56
Differences with Azure Functions .....	588.4–62
Example 🌐 .....	588.4–109
Language Support .....	588.4–109
Manually .....	588.4–58
Shells .....	588.4–60
Roles .....	588.2–68
List .....	588.4–39
PassRole .....	588.3–25, 47
Start/Stop Instances .....	588.3–49
Root .....	588.2–40–41
SDK .....	588.2–23
Service Names .....	588.2–67
Session Tokens .....	588.3–27–28
Testing Policy .....	588.1–29–30
WAF .....	588.3–66
AMI .....	588.W–114
AMZN Header .....	588.W–48
Anti-Pattern .....	588.2–41
API .....	588.2–10
Gateway .....	588.4–55–56
.....	588.5–53
Exploit .....	588.3–65
Key .....	588.2–14, 39
Server 🌐 .....	588.5–7, 9
App (Windows Functions) .....	588.4–63
Application Mapping .....	588.4–7
Aqua Security .....	588.5–21
ARM .....	588.2–18
ARN .....	588.2–35–37
Artifact Resolution Protocol .....	588.2–103
ASAPI .....	588.4–45
ASN .....	588.1–67
Assertion Query and Request .....	588.2–103
Asset Collection .....	588.1–112
Frameworks .....	588.1–107
Asset Discovery Pipeline .....	588.1–44
.....	588.W–27
Assetnote .....	588.1–92, 96, 107
.....	588.W–35–37
Asymmetric Certificates .....	588.2–100
Atlassian Bamboo .....	588.4–21
Attack Rotation .....	588.5–45, 63
Attack Surface .....	588.2–7, 9
Aurora .....	588.4–84
Auth0 .....	588.2–78, 118
Authentication .....	588.2–14, 122
as a Service → AaaS .....	
Bypass .....	588.5–75
Code Grant .....	588.2–93
Request .....	588.2–103–104
Standards .....	588.2–87
Web .....	588.2–88
System-API .....	588.2–101
Authorization .....	588.2–122
Grant .....	588.2–91
Server .....	588.2–91–92, 127

Automated Rollout and Rollback .....	588.5–5
Autoscaling .....	588.1–128
.....	588.2–7
AV Bypass .....	588.3–50
Azure .....	588.1–20, 28, 67
.....	588.2–11, 36, 66
AD .....	588.2–39, 74, 77
Authentication .....	588.2–71
Connector .....	588.2–78
Domain Services .....	588.2–61, 70, 76–77
Privilege Escalation .....	588.2–85
Roles .....	588.2–75, 80–85, 84
Scope .....	588.2–82
Synchronization .....	588.2–76, 78
Automation .....	588.3–81
Blob .....	588.1–121
CLI .....	588.2–11, 14, 23, 50–52
.....	588.3–80
Compute .....	588.2–77
Files .....	588.2–60–62, 76
.....	588.3–79
Functions .....	588.4–62–64
Differences with AWS Lambda .....	588.4–62
Login .....	588.2–51
Portal .....	588.W–69–70
Resource Manager (RM) .....	588.2–51, 75
Roles .....	588.2–68
Serverless .....	588.4–62
Service Names .....	588.2–67
Storage .....	
Manager .....	588.3–73
Testing Policy .....	588.1–31–34
URL's .....	588.1–83–84
VM .....	588.3–71–74
AzureStack .....	588.2–66


## B

Backdoor .....	588.5–31
Implantation .....	588.3–43, 49, 67, 72–73, 81–82
.....	588.4–20, 23, 26–29
.....	588.5–27
Workflow .....	588.5–37–39
Bad Password Count .....	588.5–79
Banner Grabbing .....	588.1–68, 101
Bash .....	588.3–50
Basic Authentication .....	588.2–88, 122
Bastion Host .....	588.3–43, 49
Beacon .....	588.5–52–53
Bearer Authentication .....	588.2–88, 93, 95, 98, 101
.....	588.5–59
Bearer Token .....	588.2–101
Beijing .....	588.2–41
BGP .....	588.1–67
BigTable .....	588.1–92
Billing Administrator .....	588.2–81, 83
Blind Injection .....	588.4–47
BLOB .....	588.3–57

# SEC588 – Cloud Penetration Testing

Boot Features .....	588.1–119
Box .....	588.1–25
Breach Notification .....	588.2–12
Bridge .....	588.3–42
Brute Force .....	588.4–7
.....	588.5–79-80
BSON .....	588.4–73
Buckets .....	588.1–23, 65
Bug Bounty .....	588.1–23, 107
.....	588.2–9
Build Systems .....	588.4–21-29
Output .....	588.4–27
Busy Box .....	588.5–15

## C


C2 .....	588.5–53, 93
Hardening .....	588.5–58
Implant .....	588.5–52, 101
ca.crt .....	588.5–10
Cassandra .....	588.4–70
Censys .....	588.1–51, 53
Cert Bot .....	588.1–50
Certificate .....	588.1–49
Authority .....	588.1–49-50
Transparency .....	588.1–47-48, 51, 53-54, 57
Certificate Store .....	588.3–7
Certificate-Based Authentication .....	588.2–51, 87
Certification Manager .....	588.1–50
CGI-BIN .....	588.4–45-46
Chrome .....	588.1–48
Chroot .....	588.1–124
.....	588.4–100-101
CI Systems .....	588.4–21
CI/CD .....	588.2–9
.....	588.3–81
.....	588.4–12
Attack .....	588.4–23
Detection .....	588.4–22
CIDR .....	588.1–69
Circle CI .....	588.4–22
Classic Application .....	588.4–99
Classic Subscription Model .....	588.2–75, 83
Cleartext Passwords .....	588.3–6
Client .....	588.2–92, 127
Credentials .....	588.2–93
Client-Side Proxy .....	588.4–10
Cloud Computing .....	588.1–15-16
Types .....	588.1–17
Cloud Controller  .....	588.5–6
Cloud Native Applications .....	588.1–118
.....	588.4–12-16, 36, 106
Injections .....	588.4–48, 86
Properties .....	588.4–12
Cloud Native Attacks .....	588.4–5
CloudAP Service .....	588.3–9
CloudTrail .....	588.2–40
.....	588.3–66

CloudWatch .....	588.2–40, 47
.....	588.3–66
CNAME .....	588.1–45, 56, 65, 83
.....	588.5–98
CNCF .....	588.4–12, 14
.....	588.5–5
Co-Administrator .....	588.2–80, 83
Code Execution .....	588.3–78
Code Flow .....	588.2–93-95
Code Injection .....	588.4–59
Codebuild .....	588.3–63
.....	588.4–21
Collection #1 .....	588.5–76
Command Channel .....	588.5–31, 51, 72
Command Injection .....	588.4–47-50, 60
Primitives .....	588.4–48
Command-and-Control Architecture .....	588.5–53
Hardening .....	588.5–58
Obfuscation .....	588.5–93
Command-and-Control Server .....	588.4–69
.....	588.5–53
?comp=list .....	588.2–60
.....	588.W–78
Compute .....	588.1–119, 128
.....	588.2–68
.....	588.3–41
Attack Scenarios .....	588.3–47
Instance .....	588.2–62
.....	588.3–67
Conditional Access .....	588.2–43, 48
Containerd .....	588.4–12
Containers .....	588.1–26, 118, 122
.....	588.2–8
.....	588.4–99-106
.....	588.5–8
Architectures .....	588.4–101-102
Backdooring .....	588.5–27, 37
Cross-Communication .....	588.4–105
Escape .....	588.1–128
.....	588.4–111
Management System .....	588.1–125
Content Filter .....	588.5–97
Database .....	588.5–94-95
Contributor .....	588.2–80, 83
Cookie Jar .....	588.2–116
CoreOS .....	588.5–7, 49
CouchDB .....	588.1–76
Credential Stuffing .....	588.5–79, 83-84, 86-87
CredentialGuard .....	588.3–6
Credentials .....	588.1–95
.....	588.2–10, 14
CRI-O .....	588.1–124
.....	588.5–8
CRLF .....	588.4–38
Cron .....	588.1–50
Cross-Account Copy .....	588.5–66-67, 70
Cryptography .....	588.5–58, 100
CSE (Azure) .....	588.3–79

# SEC588 – Cloud Penetration Testing

.....	588.W-152-156
CSP .....	588.1-65, 118, 120
.....	588.5-45, 64
Data .....	588.5-69
Mappings .....	588.1-67
Custom Script Extension → CSE .....	
CVE .....	588.1-111
CVS .....	588.4-18
CyberArk .....	588.2-60, 105, 107
.....	588.3-20

## D


DaemonSet 	.....	588.5-38
Data Analysis .....	588.1-20	
.....	588.2-6	
Data Center .....	588.3-48	
Data Collection .....	588.1-20	
.....	588.2-6	
Data Exfiltration .....	588.5-69	
Data Exposure .....	588.4-76	
Data Mining .....	588.1-43	
Data Pivoting .....	588.5-66	
Data Smuggling .....	588.5-71	
Database Protocols .....	588.4-15	
Databases .....	588.4-70	
Databases as a Service → DBaaS .....		
Dataset .....	588.1-43, 53, 92	
.....	588.2-12	
DBaaS .....	588.1-27	
.....	588.4-70	
Managed/Unmanaged .....	588.4-83	
Defender Tip .....	588.2-40	
Delegated Access .....	588.5-67	
Demarcation Points .....	588.1-23-24	
Denial of Service .....	588.1-30, 34	
Deny Model .....	588.2-41	
Deployment .....	588.4-100, 103	
.....	588.5-38-39	
Automation .....	588.3-81	
Pipeline .....	588.4-20-21	
Developer Tools .....	588.4-10	
.....	588.W-57	
Development Pipeline .....	588.4-18	
Dictionary Attack .....	588.5-79, 80-81, 84	
Digital Ocean .....	588.1-17	
.....	588.4-68	
DirectConnect .....	588.3-48, 64	
Directory Bruteforce .....	588.1-87	
Dirty Container .....	588.1-126	
.....	588.5-27, 36-39	
Disclosure Process .....	588.1-128	
Discord .....	588.3-31	
Discovery Tools .....	588.1-56, 109	
DMZ .....	588.2-70	
.....	588.5-101	
DNS .....	588.1-45	
Bruteforce .....	588.1-58, 86	

Filter .....	588.5-97
Lookup .....	588.1-66
DNSdb .....	588.1-52
Docker .....	588.1-26, 109, 111, 118, 123-124
.....	588.2-8
.....	588.4-12, 101-102
Container .....	588.4-104
Datasheet .....	588.1-125
Dockerfile .....	588.4-104
.....	588.5-37
Hub .....	588.1-126
.....	588.5-36
Document Object-Storage .....	588.4-79
Document Type .....	588.4-7-9
Domain Administrator .....	588.2-40, 81
Domain Controller .....	588.2-73, 76-77
Domain Fronting .....	588.4-28
.....	588.5-97-101
Domain/Forest Structure .....	588.2-71
DPAPI .....	588.3-8
Drone .....	588.4-22
Dropbox .....	588.1-25
.....	588.5-71


## E

EBS	588.3-41
Exploit	588.3-65
EC2	588.1-82, 128
	588.2-11, 25, 44
	588.3-41-43
Attacks	588.3-43, 47-51
Conditional Access	588.2-43
Exploit	588.3-65
Instances	588.2-28
Properties	588.3-42
Public IP Address	588.3-47
Security Groups	588.3-42
UserData	588.3-49-51
ECDSA	588.2-16
ECS	588.3-41
	588.5-12
EIP	588.3-42, 47
Elastic Container	588.2-47
Registry → AWS ECR	
Elastic Kurbenetes Services → AWS EKS	
ElasticSearch	588.4-69
ELB	588.1-82
Elevation	588.1-20
Encrypted Command Channel	588.5-31
Encryption	588.5-58
Endpoint Services	588.1-83
Endpoints Controller	588.5-6
Enter-PSSession	588.3-83
Enterprise Administrator	588.2-81
Enumeration	588.3-59
Env File	588.2-17-19
Environment Information	588.4-50

# SEC588 – Cloud Penetration Testing

Environment Variable .....	588.2–15, 18, 24
.....	588.4–25, 63
.....	588.5–14, 16
Etcd  .....	588.5–7, 9
Evasion .....	588.3–66
Expired Domains .....	588.5–94
Exploit Multi Handler .....	588.5–32, 37–38, 101
Exploitation .....	588.1–20
.....	588.4–5
Exposed Databases .....	588.4–68–79
Risks .....	588.4–71
Exposed Secrets .....	588.W–54
Exposed Services .....	588.4–69
ExpressJS .....	588.4–57

## F

F5 .....	588.2–118
Facebook .....	588.1–46, 110
Fastly (Proxy)  .....	588.5–98–99
Federated Identity Service .....	588.2–73
Federation .....	588.2–39, 70, 73, 88, 102
FIFO .....	588.2–61
File Descriptor .....	588.3–32
File Shares .....	588.2–60
File Systems .....	588.1–121, 124
Fingerprinting .....	588.1–111
Tools .....	588.1–109
Firewalling .....	588.2–8
Force.com .....	588.1–24, 26
Foreground Process .....	588.4–28
Forged Key .....	588.2–128
FQDN .....	588.1–49
Function as a Service .....	588.1–118, 127
.....	588.4–54
Fuzzing .....	588.1–88
FWaaS .....	588.1–27

## G

getSubdomain .....	588.1–93
Git .....	588.4–18–19
GitHub .....	588.2–15
Global Administrator .....	588.2–81, 83–85
Golden SAML Attack .....	588.2–105–110
Google Apps .....	588.2–56
Google BigQuery .....	588.1–92
Google Cache .....	588.1–57
Google Cloud .....	588.1–20, 92
Storage .....	588.1–121
Google Enumeration .....	588.1–57
Google Functions .....	588.4–68
Google Tink .....	588.5–58
GovCloud .....	588.2–41
GPG .....	588.2–16
Grep .....	588.1–53
GRPC .....	588.1–124

.....	588.4–16
GSuite .....	588.1–25
GuardDuty .....	588.3–66–67

## H

HackerOne .....	588.4–41
Health Check .....	588.5–21
Heavy Shell .....	588.5–55, 57
Heroku .....	588.W–50
Hibernate .....	588.4–86
HMAC-SHA256 .....	588.2–100
Hogging → Performance Hogging .....	
Hop.php .....	588.5–101
Horizontal Scaling .....	588.5–5
Host Discovery .....	588.1–47–51, 66
.....	588.2–10
Host Header .....	588.1–66
Host Mounts .....	588.5–15
Hostkeys .....	588.5–28
HS256 .....	588.2–100
HSM .....	588.3–56
.htaccess .....	588.W–204
HTTP .....	588.4–15
Gateway .....	588.4–55
Methods .....	588.2–119
Proxy Redirect .....	588.4–45
Request .....	588.4–8–9
REST API .....	588.1–121
Hybrid Workers .....	588.3–81–82
Hyper-V .....	588.3–71
.....	588.4–100, 102

## I

IaaS .....	588.1–17, 119
.....	588.4–6, 83
Attack .....	588.1–27
Attacker's View .....	588.1–128
Testing Policies → Testing Policies .....	
IAM .....	588.1–23
.....	588.2–12
Privilege Escalation .....	588.3–20
IBM Cloud .....	588.1–17
ID Provider .....	588.2–55, 102, 105
Public Certificate .....	588.2–107
ID Token .....	588.2–96
Identity Policy .....	588.2–42, 45
IIS .....	588.2–19
IKEv2 .....	588.3–48
Image Mount .....	588.3–74
IMD .....	588.3–28
Implicit Flow .....	588.2–93
In-Memory Database .....	588.4–70–71
Inetdata .....	588.1–53
Infrastructure Mapping .....	588.4–7
Ingress Access .....	588.1–119



# SEC588 – Cloud Penetration Testing

Initial Foothold .....	588.4-5
.....	588.5-27
Injectons .....	588.4-33-34
Instagram .....	588.1-110
Instance Metadata Service .....	588.3-26-28, 42, 50-51
.....	588.4-39
Token Protections .....	588.4-40
Integrity Check .....	588.2-99
.....	588.5-58
IntelX .....	588.1-52
Invoke-Command 🚩 .....	588.3-83
IP Addressing .....	588.1-64
Space .....	588.2-7
IP Blocking .....	588.2-43
IP Forwarding .....	588.3-36-37
IP Ranges .....	588.1-67
IPC .....	588.4-105
IRC .....	588.3-31

## J

Jail .....	588.4-101, 103
Jailbreak .....	588.3-21
JavaScript .....	588.1-95, 102
.....	588.2-15, 19, 33
.....	588.4-57
Jenkins .....	588.4-20-22
JMESPath .....	588.2-53
Job Control Channel .....	588.5-53
JSON .....	588.2-18, 27, 43
.....	588.3-79
Query .....	588.2-53
JSONC .....	588.2-50
JWT .....	588.2-14, 96, 99-101
.....	588.3-9
Attacker's View .....	588.2-100
Decoding .....	588.W-97
HTTP Header .....	588.3-9

## K

K8s → Kubernetes .....	
Kerberos .....	588.2-71-72
.....	588.3-83
Golden Ticket Attack .....	588.2-107
Kerckhoffs' Principle .....	588.5-58
Kernel .....	588.3-37
API Call .....	588.4-100
Key Exposure Recommendations .....	588.W-58
Key Format .....	588.2-14, 16
Key Management .....	588.3-56
Key Material .....	588.2-14-15, 77
.....	588.3-50, 55
.....	588.5-74
Key Vault .....	588.2-67
Key-Value Store .....	588.4-70-71
.....	588.5-7
KMS .....	588.3-55-57

.....	588.W-112
Features .....	588.3-56
Kubelet 🌟 .....	588.5-8-10, 13
Namespace .....	588.5-10
Rights .....	588.5-18
Kubernetes .....	588.1-118, 122, 124-125
.....	588.2-8
.....	588.4-6, 54
.....	588.5-5-21
API .....	588.5-11, 16
Attacker's View .....	588.5-11
Certificate .....	588.5-10, 18, 20
Config (Default Location) .....	588.5-10
Dashboard UI .....	588.5-17
Features .....	588.5-5
Managed/Unmanaged .....	588.5-12
Master .....	588.5-6, 9
Meterpreter .....	588.5-36-39
Nodes .....	588.5-8
Secrets .....	588.5-10, 16
Vulnerabilities .....	588.5-21
Kudu .....	588.4-63
KVM Hypervisor .....	588.3-41

## L

Lambda .....	588.1-30, 128
.....	588.2-47, 67
.....	588.3-63
.....	588.4-50
Attacks .....	588.4-54-60
Data Decryption .....	588.3-56
Shell .....	588.4-60
Landing Page .....	588.2-56
LANMAN .....	588.3-6, 8
Laravel .....	588.2-19
.....	588.4-86
Lateral Movement .....	588.2-41
.....	588.3-64
.....	588.4-26, 60
.....	588.5-20, 23
LDAP .....	588.2-71-72
Lessons Learned .....	588.1-21
Let's Encrypt .....	588.1-50
.....	588.5-99-100
Lifecycle Management .....	588.4-106
LightSail .....	588.3-41
Exploit .....	588.3-65
LigHTTPD .....	588.4-46
Lighttpd .....	588.1-101
Lightweight Shell .....	588.5-56-57
Link-Local Address .....	588.4-39
Linode .....	588.4-68
Linux Containers .....	588.4-100-101, 103
Linux Kernel .....	588.4-101
Listener .....	588.5-32
Load Balancer .....	588.1-27
.....	588.2-7-8





# SEC588 – Cloud Penetration Testing

.....	588.5-64
Local System .....	588.3-79
Logging .....	588.2-8
Login Hint .....	588.2-97
Loose Access Control .....	588.2-42
Lsadump .....	588.3-8
LSASS .....	588.3-6
.....	588.4-111
Lua .....	588.1-76

## M

Makeshift Router .....	588.3-43
MAM .....	588.1-33
Man-In-The-Middle .....	588.1-48
.....	588.5-74
Managed Container .....	588.4-54
Management Group .....	588.2-82-83
Management Layer .....	588.1-23
Mapping .....	588.1-20
.....	588.2-6-12
.....	588.4-6-7
Client-Side .....	588.4-10
Workflow .....	588.2-8
MariaDB .....	588.4-70
MD4 .....	588.2-78
MDM .....	588.1-33
Memcached .....	588.1-76
.....	588.4-16
Memory Sharing .....	588.4-105
Merkle Hash Tree .....	588.1-48
meta-data/iam/security-credentials .....	588.3-26
Method Type .....	588.4-7
MFA .....	588.2-14, 40, 87
.....	588.W-58
Microservices .....	588.4-12-13, 99, 106
Microsoft Cloud Services .....	588.2-66-68
Microsoft Exchange .....	588.1-49
Microsoft Graph .....	588.2-118, 120
.....	588.3-11-16
API Examples .....	588.3-15-16
Constraints .....	588.3-12
Postman Collection .....	588.3-14
Microsoft Identity Services .....	588.2-70-71
Attacker's View .....	588.2-77
Microsoft Services .....	588.1-84
MIME-Encoding .....	588.2-121
MOD-PHP .....	588.4-45
MongoDB .....	588.1-76
.....	588.4-69-70
Cheat Sheet .....	588.4-79
Port (27001) .....	588.4-73
Query .....	588.4-77-78
Monitoring .....	588.1-82
MX Record .....	588.1-45

## N

Name Identifier Management Protocol .....	588.2-103
Name Identifier Mapping Protocol .....	588.2-103
Namespaces .....	588.1-124
.....	588.4-100-101, 105
NAT .....	588.1-37, 128
.....	588.3-35-36, 42
Net.WebClient  .....	588.3-82
Netcat as a Service .....	588.1-36
Netflix .....	588.4-13
NetSPI .....	588.1-83
Network Bridge .....	588.4-101
Network Components .....	588.1-120
Network Firewall as a Service → FWaaS .....	
Network Forwarding .....	588.5-31
Network IPS/IDS .....	588.5-33
Network Socket .....	588.3-32
.....	588.4-15
NFS .....	588.1-121
NIST SP 500-291 .....	588.1-16
Node Controller  .....	588.5-6
NodeJS .....	588.2-19
Lambda .....	588.4-57
ORM .....	588.4-95
SQL Injection .....	588.4-88-90
Non-Password-Based Authentication .....	588.2-87
NoSQL .....	588.2-61
.....	588.4-70
Injection .....	588.4-72
Notification Form .....	588.1-33
NS Record .....	588.1-45
NSE .....	588.1-74, 76-77
Ntdll.dll / Ntfs.dll .....	588.4-102
NTHash .....	588.2-78
NTLM .....	588.2-71-72
.....	588.3-6

## O

OASIS Group .....	588.2-102
OAuth .....	588.2-51, 71, 88-91, 127
Issues .....	588.2-128
OAuth2 .....	588.2-14, 71, 74, 92
Flow Types .....	588.2-93-94
Code .....	588.2-94-95
Obfuscation .....	588.4-111
.....	588.5-93
OCI .....	588.1-125
Office365 .....	588.1-25
.....	588.2-66, 73, 78, 129
.....	588.5-72
Administrators .....	588.2-84
OIDC → OpenIDConnect .....	
Okta .....	588.2-56, 78, 118
On Premise Roles .....	588.2-68
OneDrive .....	588.1-25
.....	588.3-12, 31
.....	588.5-72
OpenIDConnect .....	588.2-88, 96-98, 103

# SEC588 – Cloud Penetration Testing

Flow .....	588.2–97-98
OpenShift .....	588.1–24, 26
OpenSSH .....	588.2–16
Private Key .....	588.W–198
OpenSSL Connection .....	588.3–32
ORM .....	588.4–86, 95
Orphaned Database .....	588.4–69
Orphaned Disk .....	588.W–73
Orphaned Security Groups .....	588.3–42
OS Fingerprinting .....	588.1–75
OT .....	588.1–105
Owner .....	588.2–80, 83

## P

PaaS .....	588.1–17, 24
Attack .....	588.1–26
PACU Exploit .....	588.3–41, 51
Pass-the-Hash Attack .....	588.3–8-9
Pass-the-PRT Attack .....	588.3–9
Pass-the-Ticket Attack .....	588.3–8
Passive Collection .....	588.1–43
Passive Technique .....	588.1–47-54
PassRole Capability .....	588.3–25, 47
.....	588.W–114
Passthru Authentication .....	588.2–78
Password .....	588.5–74
Attacks .....	588.5–75-89
Types .....	588.5–79
Guessing .....	588.2–55
Hash .....	588.5–75
Synchronization .....	588.2–78
Lists .....	588.5–76
Spraying .....	588.5–79, 82, 84
PAT .....	588.3–36
Payload .....	588.3–64
.....	588.5–31-32
Beacon .....	588.5–52-53
Build .....	588.5–35
Challenges .....	588.5–48
Deployment .....	588.5–50
Design Choices .....	588.5–58-59
Injection .....	588.3–64
Stages .....	588.5–33-35
Traditional .....	588.5–48, 51
PEM .....	588.2–16
.....	588.5–28, 101
Penetration Testing .....	588.5–44, 63
Guidance .....	588.1–23
Methodology .....	588.1–19-21
.....	588.2–6
Pentester Tip .....	588.2–39, 77-78
.....	588.3–72
Performance Hogging .....	588.1–30
Permission Boundary .....	588.2–42, 44
Permission Policy .....	588.2–39
Permission Removal .....	588.2–45
Persistence .....	588.1–21

.....	588.3–59
.....	588.5–55
PF_RING .....	588.1–71
PHP-FPM .....	588.4–45
Pipe .....	588.3–30, 32
Pivot .....	588.1–21, 34
.....	588.2–47
.....	588.3–25, 31, 35, 43, 47-48, 67
.....	588.5–101
Pods ☁ .....	588.1–122
.....	588.5–14-16
Privileged .....	588.5–15, 36-39
Policy Boundary .....	588.2–46
Policy Versioning → AWS IAM User Versioning .....	
Port Forwarding .....	588.3–37
.....	588.5–28, 31
.....	588.W–37
Port Proxy .....	588.3–35
Port Restriction .....	588.2–10
Port Scanner .....	588.1–44, 66, 68
.....	588.2–7
.....	588.W–48
POSIX .....	588.1–121
Post Exploit Recon .....	588.1–21
Post Exploitation .....	588.5–43
PostgreSQL .....	588.4–70
PowerShell .....	588.3–50, 71, 80-82
PPS .....	588.1–71
Premium Drops .....	588.1–53
Prepared Statements .....	588.4–86, 95
Primitive .....	588.1–118, 128
Privacy Law .....	588.2–12
Private Key Check Bypass .....	588.2–100
Privilege Escalation .....	588.2–35
.....	588.3–20-21, 43, 59
.....	588.4–76
.....	588.5–20
Privileged Container .....	588.4–105
Project Sonar .....	588.1–52-53
Proof of Concept .....	588.1–34
.....	588.4–93
Proof of Session Key .....	588.3–9
Proprietary Stack .....	588.4–106
Protocol Buffers .....	588.1–124
Proxy Attacks .....	588.4–34
PRT Attack → Pass-the-PRT Attack .....	
PTR Record .....	588.1–45, 64-65
Public Infrastructure Cloud .....	588.1–118
Python .....	588.1–39
.....	588.3–81


## Q

Qualys .....	588.2–118
--------------	-----------

## R

RAT .....	588.5–50
-----------	----------



# SEC588 – Cloud Penetration Testing

Raw Socket .....	588.5–51
RBAC .....	588.1–122
.....	588.2–39, 44, 51, 67, 74–75, 80, 83
.....	588.3–73
.....	588.5–5, 7, 11
🔵 V1.8+ .....	588.5–18–20
Example .....	588.5–19
RDBM .....	588.4–70
RDP .....	588.3–71, 80
RDS  .....	588.4–84–85
Reader .....	588.2–80, 83
Realm .....	588.2–97
Reconnaissance .....	588.1–20, 43
.....	588.2–6–12
.....	588.3–59
Tip .....	588.3–72
Red Team .....	588.5–43–45, 63
Reddit .....	588.1–92
Redirect .....	588.1–87
Redirection .....	588.3–31, 35–36
Server .....	588.5–53
Redis .....	588.1–76
.....	588.4–16, 69–71
as a Service .....	588.4–71
Port (6379) .....	588.4–73
Refreshed Token .....	588.3–28
Replication Controller 🔵 .....	588.5–6
Resource Owner .....	588.2–92, 127
Password Credentials .....	588.2–93
Resource Policy .....	588.2–42, 45
Resource Server .....	588.2–92, 127
REST .....	588.4–16
<b>Restart-Service</b> 🐞 .....	588.3–83
RESTful API .....	588.2–33, 36, 61, 112–113
.....	588.W–202–206
Revocation Flow .....	588.2–93
RFC 3986 (URI) .....	588.2–33
RFC 5849 (OAuth) .....	588.2–90
RFC 6749 (OAuth2) .....	588.2–90
RFC 7519 (JWT) .....	588.2–99
RFC 8555 (ACME) .....	588.1–50
RFI .....	588.4–36
Roles Comparison .....	588.2–68
Root .....	588.4–23
Route53 .....	588.1–50
Routing (Attack) .....	588.3–43, 48
.....	588.5–64–65
Routing and Switching .....	588.4–106
RPC .....	588.2–72
.....	588.4–15
RSA Private Key .....	588.W–199
RST .....	588.1–72
Ruby on Rails .....	588.4–86
Rules and Permissions .....	588.1–33
Rules of Engagement .....	588.1–23, 31–32, 128
Rumble.run .....	588.1–107
RunCommand .....	588.3–80
.....	588.W–151

## S

S3 Buckets .....	588.1–20, 65, 88, 96, 121
.....	588.2–44
Administration .....	588.2–24
Conditional Access .....	588.2–43
Policy .....	588.5–67
Restrictions .....	588.2–12
SaaS .....	588.1–17
Attack .....	588.1–25
Sailpoint .....	588.2–56, 78
Salesforce .....	588.1–25–26
SAM Database .....	588.3–7–8
SAML .....	588.2–55, 70–71, 74, 88, 102–105
Flow .....	588.2–108, 129
Insertion Message .....	588.2–108
Protocols .....	588.2–103
Token .....	588.2–105
SAN .....	588.1–49–50
Sandbox .....	588.4–103
Escape .....	588.1–33
SASL .....	588.4–69
SCADA .....	588.1–105
Scanning .....	588.1–20
.....	588.2–10
Workflow .....	588.1–77
Scheduler 🔵 .....	588.5–7, 9
SCM .....	588.2–9
.....	588.4–18–19
Scope .....	588.1–23, 128
.....	588.2–9, 77
Scope (OAuth) .....	588.2–91, 97
Screenshot .....	588.1–103, 109
Scripting .....	588.1–119
Scrubbing .....	588.1–47
Secret Exchange .....	588.2–95
Secrets Configuration and Management .....	588.5–5
Secrets Format .....	588.2–16
Secrets Location .....	588.5–14
Secrets Manager .....	588.2–16
Security Bypass .....	588.3–67
Security Credentials .....	588.3–26
Security Isolation Environment .....	588.1–125
SecurityTrails .....	588.1–52
Seed .....	588.1–46
Sekurlsa .....	588.3–8–9
Selenium .....	588.1–103
Self-Healing .....	588.5–5
Self-Signed Certificate .....	588.3–33
Sensitive Information .....	588.3–8
.....	588.4–27, 39
Commit .....	588.4–18
Serial Connection .....	588.3–32
Serverless Computing .....	588.1–118
.....	588.4–54, 110
Serverless Function .....	588.1–33, 128
.....	588.2–8
.....	588.5–64
Attacks .....	588.4–64

# SEC588 – Cloud Penetration Testing

Serverless Infrastructure .....	588.1–33	Discovery .....	588.4–89
Service Administrator .....	588.2–80, 83	Workflow .....	588.4–87
Service Chaining .....	588.4–106	Query .....	588.4–77
Service Control Policy .....	588.2–42, 47	SQLAlchemy .....	588.4–86
Service Mesh .....	588.4–106	SRV Record .....	588.1–57
.....	588.5–13	SSH Keys .....	588.3–65
Service Names Comparison .....	588.2–67	SSH Tunnel .....	588.5–28
Service Orchestration .....	588.1–118, 122	SSM .....	588.3–50
Session Policy .....	588.2–42	SSO .....	588.2–88, 102
Session State Storage .....	588.4–16, 74–75	.....	588.3–9
Set-Item  .....	588.3–83	SSRF .....	588.2–15
SetDefault Policy .....	588.3–24	.....	588.3–51
SG .....	588.2–11	.....	588.4–36–41
Shadow Admins .....	588.3–20	Stand-Alone Database .....	588.4–83
Shared Database .....	588.4–83	Standardized Authorization Implementation ..	588.2–96
Shared File System .....	588.1–27	Standardized Scopes .....	588.2–96
Shared Hosting .....	588.5–54	Stateless/Stateful Application .....	588.5–38
Shared Infrastructure .....	588.2–77	Statically Compiled Binary .....	588.5–49
Shared Responsibility .....	588.1–24	StatufulSets  .....	588.5–38
Shared Service .....	588.1–128	Storage Area .....	588.2–60
SharePoint .....	588.1–25	Storage Blob .....	588.2–8, 61
Shell Access .....	588.1–34	Storage Environments .....	588.2–61
Shell Environments .....	588.4–48	Struts .....	588.4–86
SHM .....	588.4–105	SUID .....	588.3–21
Shodan .....	588.1–52	Supply Chain .....	588.4–23
.....	588.4–69	.....	588.5–27
Shunning .....	588.5–65, 81	Attack .....	588.1–126
Silo Processes .....	588.4–100, 102	Svchost .....	588.3–37
Single Logout Protocol .....	588.2–103	SVN .....	588.4–18
Site-to-Site VPN .....	588.3–48	Swagger API .....	588.W–50
Slack .....	588.3–31	Symmetric Shared Keys .....	588.2–100
SMB .....	588.1–74, 121	SYN .....	588.1–72
.....	588.2–61–62, 76	Synchronization (AD) .....	588.2–76
.....	588.4–15	Sysinternals .....	588.1–31
.....	588.5–66	System Hardening .....	588.3–41
Port (445) .....	588.5–28	System Manager Agent .....	588.3–65
SMTP .....	588.1–74		
Snapshots .....	588.3–65, 74		
SNI (TLS Field) .....	588.5–97		
SOA Bus .....	588.4–15		
Social Engineering .....	588.4–5		
Socket Connector .....	588.3–30		
Socket Redirection .....	588.1–39		
Socket Router .....	588.3–43		
SOCKS4 .....	588.3–32		
Software Portability .....	588.1–118		
Software Router .....	588.3–31		
.....	588.5–48		
Source Control Tools .....	588.4–18		
SP .....	588.2–51–52, 105		
SPA .....	588.2–33		
Spiderfoot .....	588.1–107		
Spin-Down .....	588.4–60		
Spoofing .....	588.1–70		
Spring .....	588.4–86		
SQL .....	588.1–93		
Injection .....	588.4–72, 83, 86–95		
Defenses .....	588.4–95		

T

TBAC .....	588.2–48
TCP Half Open .....	588.1–72
TCP Handshake .....	588.1–70
Technologies .....	588.1–65, 118
Tenant ID .....	588.2–51-52, 109
Tenant/Subscription Model .....	588.2–71, 75
Terms of Service .....	588.1–23
.....	588.4–26, 93
.....	588.5–45, 64
Tesla .....	588.5–17
Testing Policies .....	588.1–28-34
Theoretical Limit (packets/sec) .....	588.1–70
TLS Handshake .....	588.5–97
TLS-Encrypted Channel .....	588.5–51
Token	
Hijacking .....	588.5–75
Token ☸ .....	588.5–10
Controller .....	588.5–6
Token Flow .....	588.2–93

# SEC588 – Cloud Penetration Testing

---

Token-Signing Private Key .....	588.2–107
TOML .....	588.2–18
Traceroute .....	588.1–75
Transitivity (Permissions) .....	588.2–82
Travis CI .....	588.4–21–28
TTL .....	588.4–40
Turnkey Cloud .....	588.5–12

## U


Undocumented Feature .....	588.3–26
Universal Stack .....	588.4–106
Unsecured Resource .....	588.2–12
URI .....	588.2–33–34
URL .....	588.1–82
.....	588.2–34
Bruteforce .....	588.W–43
Encoding .....	588.2–121
URN .....	588.2–34, 104
Useful Strings .....	588.2–18
User Access Administrator .....	588.2–80
User Administrator .....	588.2–81, 83–84
User-Agent .....	588.1–104
.....	588.4–94
Userinfo Endpoint .....	588.2–96
Username .....	588.5–84–85
Harvesting .....	588.2–55

## V

Vagrant .....	588.1–109
Valid Domains .....	588.5–94
VHD .....	588.3–71
.....	588.5–70
Virtual Hosting .....	588.1–66, 85
Virtual Machines .....	588.1–119
.....	588.2–10
.....	588.4–103
Visualization .....	588.1–101
Voldemort DB .....	588.1–76
VPC .....	588.2–66–67
.....	588.3–42
Blocking .....	588.2–43
Flow Logs .....	588.3–66
VPN .....	588.1–120
.....	588.2–9
.....	588.3–48, 64
.....	588.5–65
Vulnerability Discovery .....	588.1–20
Vulnerability Hunting .....	588.5–21
.....	588.W–49
Vulnerability Scanner .....	588.1–111

.....	588.5–21
Vulnerable Function .....	588.4–64

## W

WAF .....	588.2–8
.....	588.4–40, 90, 94
Watcher Task .....	588.3–82
Weak Password .....	588.2–100
Web Browser Secrets .....	588.3–8
Web Redirection .....	588.1–39
Web Server .....	588.3–35
Web Shells .....	588.5–54–57
Web.config .....	588.2–19
WhatsApp .....	588.1–110
Whois XML API .....	588.1–53
Wildcard Enumeration .....	588.1–58
Windows 10 .....	588.5–72
Windows Containers .....	588.4–100, 102, 111
Windows Defender .....	588.4–111
Windows Desktop .....	588.4–100, 102
Windows Functions .....	588.4–62–64
Attacker’s View .....	588.4–63
Attacks .....	588.4–64
Windows Kernel .....	588.4–102
Windows Server Core .....	588.4–50, 102
WinRM .....	588.3–71, 83
Ports (5985/5986) .....	588.3–83
WLAN Passwords .....	588.3–8
Wordlists .....	588.1–56, 92–96
.....	588.2–12
.....	588.5–76–77
.....	588.W–35–37
Worker Node  .....	588.5–9
WSGI .....	588.4–45

## X

X-aws-ec2-metadata-token .....	588.4–40
x-ms-RefreshTokenCredential .....	588.3–9
XML .....	588.2–102–103

## Y

YAML .....	588.2–18
.....	588.5–19, 39
Yml File .....	588.2–17–18

## Z

Zone Transfer .....	588.1–57
---------------------	----------