

SEC401 – Security Essentials Bootcamp Style

Topics

Network Security and Cloud Essentials

| | |
|--|-----------|
| An Introduction to SEC401 | 1-3-13 |
| Defensible Network Architecture | 1-14-53 |
| Protocols and Packet Analysis | 1-54-107 |
| Virtualization and Cloud Essentials | 1-108-165 |
| Securing Wireless Networks | 1-166-235 |

Defense-in-Depth

| | |
|--|-----------|
| Defense-in-Depth | 2-3-45 |
| Identity & Access Managemnet | 2-46-76 |
| Authentication and Password Securty .. | 2-77-112 |
| Security Frameworks | 2-113-141 |
| Data Loss Prevention | 2-142-181 |
| Mobile Device Security | 2-182-205 |

| | |
|------------|------|
| 3DES | 4-67 |
|------------|------|

Vulnerability Management and Response

| | |
|--|-----------|
| Vulnerability Assessments | 3-3-32 |
| Penetration Testing | 3-33-76 |
| Attacks and Malicious Software | 3-77-128 |
| Web Application Security | 3-129-162 |
| Security Operations and Log Management . | 3-162-200 |
| Digital Forensics and Incident Response | 3-201-239 |

Data Security Technologies

| | |
|--|-----------|
| Cryptography | 4-3-52 |
| Cryptography Algorithms and Deployment . | 4-53-80 |
| Applying Cryptography | 4-81-129 |
| Network Security Devices | 4-130-184 |
| Endpoint Security | 4-185-220 |

| | |
|----------|-----------|
| 5G | 1-229-230 |
|----------|-----------|

Windows and Azure Security

| | |
|--|-----------|
| Windows Security Infrastructure | 5-3-43 |
| Windows as a Service | 5-44-70 |
| Windows Access Controls | 5-71-119 |
| Enforcing Security Policy | 5-120-193 |
| Microsoft Cloud Computing | 5-194-247 |
| Automation, Logging, and Auditing | 5-248-296 |

Linux, AWS, and Mac Security

| | |
|--|-----------|
| Linux Fundamentals | 5-3-66 |
| Linux Security Enhancements and Infrastructure | 5-67-121 |
| Containerized Security | 5-122-143 |
| AWS Fundamentals | 5-144-161 |
| AWS Security Controls | 5-162-178 |
| AWS Hardening | 5-179-200 |
| macOS Security | 5-201-215 |

Workbook

| | |
|-------------------|---------|
| tcpdump | 5-26-37 |
| Wireshark | 5-38-50 |
| Aircrack-ng | 5-51-57 |
| Hashcat | 5-58-69 |

| | |
|-----------------------------------|--------------|
| Cain and Abel | 5-70-94 |
| AppLocker | 5-95-123 |
| Nmap | 5-124-139 |
| Malicious Software | 5-140-147 |
| Command Injection | 5-148-153 |
| hping3 | 5-154-163 |
| Image Steganography | 5-164-184 |
| GNU Privacy Guard (GPG) | 5-184-203 |
| Snort | 5-204-227 |
| Process Hacker | 5-228-244 |
| NTFS Permissions Reporter | 5-245-258 |
| SECEDIT.EXE | 5-259-266 |
| 800-61 | 6-196 |
| 802.11 | 1-171-186 |
| Security | |
| Denial of Service (DoS) | 1-211 |
| Rogue Access Point | 1-209-210 |
| Signal to Noise Ratio (SNR) | 1-211-212 |
| 802.11i | 1-186, 1-197 |
| 802.15 | 1-214 |
| 802.1X | 2-30, 1-210 |

A

| | |
|--|-------------------|
| Abstraction | 1-111 |
| Access Control | 2-47, 2-61, 2-146 |
| Managing and Monitoring Acces | 2-66 |
| Techniques | 2-64-65 |
| Web App | 3-150 |
| Access Control List (ACL) | 5-24, 1-45 |
| Access Management | 2-66 |
| Access Token | 2-60 |
| Account Administration | 2-66 |
| Accountability | 2-48 |
| Active Directory Federation Services (ADFS) .. | 5-206 |
| Adaptive Authentication | 2-109 |
| ADM templates | 5-133 |
| Administrator | 2-68 |
| Advanced Application Shielding | 4-217 |
| Advanced Encryption Standard (AES) | 4-25, 4-68 |
| Algorithm | 4-69-70 |
| Usage | 4-71 |
| Vulnerabliities | 4-71 |
| Advanced Entryption Standard (AES) | 1-197 |
| Adversary Emulation | 3-38 |
| Advnaced Persistent Threat (APT) → Threat Agents | |
| Adware | 3-119 |
| Alert | 3-166 |
| Algroithm | 4-7 |
| AlienVault | 3-186 |
| Allowlist | 3-112 |
| Amazon Web Services (AWS) | 1-147 |
| Anchore | 6-137 |
| Android | |
| Security | 2-186-190 |
| Android vs. iOS | 2-185 |
| Anomaly Analysis | 4-153 |

SEC401 – Security Essentials Bootcamp Style

| | | | |
|---|------------------|--|------------------|
| Ansible | 6-120 | Access Keys | 6-153 |
| Anti-DDoS | 2-14 | Automate Security | 6-192 |
| Anti-malware software | 2-15 | Certificate Manager | 6-195 |
| Anti-Spoofing | 4-139 | CloudFormation | 6-189-191 |
| Antivirus Software | 4-195 | CloudFront | 6-159 |
| Types | 4-196 | Web Application Security | 6-176-177 |
| App Protection Policies (APP) | 5-224 | CloudTrail | 6-172-173 |
| AppArmor | 6-70-71 | CloudWatch | 6-171 |
| Application Analysis | 4-155 | Cognito | 6-150 |
| Application Control | 4-203 | Command Line Interface (CLI) | 6-152 |
| Application control | 2-15 | Components | 6-154-160 |
| Application Control Firewall | 4-198 | Config | 6-159, 6-174 |
| Application Gateway | 4-144 | Data Protection | 6-193-195 |
| Application Insight | 5-236-238 | Key Management Service (KMS) | 6-168-169 |
| Application Security Group (ASG) | 2-36 | Macie | 6-167 |
| Application tier | 1-49 | S3 Bucket Encryption | 6-170 |
| AppLocker | 2-126 | Defenst-in-depth | 6-187-188 |
| Argon2 | 2-84 | Compute | 6-189-190 |
| ARPANET | 1-68, 1-70 | Networking | 6-187-188 |
| Assumed breach | 3-45 | EC2 Image Builder | 6-189 |
| Asymmetric Cryptography | 4-26 | ECR Image Scanning | 6-189 |
| Asymmetric Key Cryptosystems | 4-29 | Elastic Cloud Compute (EC2) | 6-157 |
| Attack Techniques | | Amazon Machine Images (AMIs) | 6-157 |
| Input Attacks | 3-98 | Elastic Container Registry (ECR) | 6-158 |
| Buffer Overflow | 3-101-106 | GuardDuty | 6-175 |
| Cross-Site Scripting (XSS) | 3-110-111 | Hardening | |
| Defenses | 3-112 | Defense-in-depth | 6-187-188 |
| OS Command Injection | 3-99-100 | Strong Identity Foundation | 6-181-184 |
| SQL Injection | 3-107-109 | Traceability | 6-185-186 |
| Attacks | | Well-Architected Framework | 6-180 |
| Current | 3-94 | High Availability (HA) | 6-155 |
| Equifax | 3-86 | Identity and Access Management (IAM) ... | 6-146 |
| Marriott Data Breach | 3-80-85 | Access Analyzer | 6-149 |
| Fallout | 3-84-85 | External Access | 6-149 |
| Impact | 3-83 | Identity Federations | 6-149 |
| SolarWinds | 2-123 | Key Concepts | 6-147-148 |
| WannaCry | 3-87-89 | Incident Response | 6-196-198 |
| Impact | 3-89 | Infrastructure | 6-154 |
| WannCry | | Availability Zones (AZ) | 6-154 |
| Attack Summary | 3-93 | Point of Presences | 6-154 |
| Gaining Access | 3-92 | Regions | 6-154 |
| Root Cause | 3-90 | InfrastructureDeployment Automation | 6-191 |
| Tools | 3-91 | Inspector | 6-189 |
| Audit Reports | 1-142 | Key Management | 6-194 |
| Auditing | 3-166, 5-248 | Key Services | 6-157-160 |
| Australian Signal Directive (ASD) controls | 2-137 | Lambda | 6-159 |
| Authenticaiton | 4-29 | Macie | 6-193 |
| Authentication | 4-15, 2-48, 2-55 | Management Console | 6-151 |
| Types | 2-48, 2-78-79 | Network Security | |
| Web App | 3-147-149 | AWS Shield | 6-165 |
| Authentication Header (AH) | 4-92 | AWS WAF | 6-165-166, 6-176 |
| Authenticator Assurance Levels (AAL) ... | 2-56, 2-109 | Network Access Control Lists (NACLs) . | 6-156, |
| Authorization | 2-48 | 6-163 | |
| Authroization code | 2-60 | Network Firewall | 6-164 |
| Automation | 5-251 | Security Groups (SGs) | 6-156, 6-163 |
| Availability | 2-9-11 | Networking | 6-156 |
| Availability Zones | 1-147 | Objectives | 6-145 |
| AWS | | Organizational Unit (OU) | 6-183 |

SEC401 – Security Essentials Bootcamp Style

| | |
|---|-------------------|
| Relational Database Services (RDS) | 6-160 |
| Resource Access Manager (RAM) | 6-184 |
| Security | |
| Summary | 6-178 |
| Security Hub | 6-175 |
| Simple Storage Server (S3) buckets | 6-157-158 |
| Summary | 6-161, 6-198, 199 |
| System Manager | 6-189 |
| Virtual Private Cloud (VPC) | 6-156 |
| Well Architected Framework | 6-196 |
| Educate | 6-196 |
| Preparation | 6-196 |
| Azure Active Directory | 2-71 |
| Azure Active Directory Domain Services (AADDS) | |
| 5-204 | |
| Azure Virtual Desktop (AVD) | 5-66-67 |
| Management and Requirements | 5-68-69 |
| Pool | 5-68 |
| B | |
| Backups | 2-146 |
| Common Pitfalls | 2-151 |
| Methods | 2-150 |
| Baseline | 2-21-23 |
| Bastion Host | 1-156 |
| bcrypt | 2-84 |
| Birthday Paradox | 4-78 |
| Bit length | 4-32 |
| Blowfish | 4-25 |
| Blue Team | 3-37 |
| Boolean exclusive | 4-17 |
| Buffer Overflow | 3-101-106 |
| C | |
| C2 Frameworks and Implants | 3-68 |
| C2 Matrix | 3-69 |
| Caesar Cipher | 4-18 |
| Cain | 5-31, 5-106 |
| California Consumer Privacy Act (CCPA) .. | 2-155-156 |
| CAP theorem | 2-148 |
| Carrier File | 4-39 |
| Carrier file | 4-43 |
| CDP Information Disclosure → Switch → Attacks | |
| Cellular | 1-229 |
| Centralized User Management | 2-57 |
| Certificate | 4-108-110 |
| Authorities | 4-110 |
| Digital | 4-118 |
| Extensions | 4-118-119 |
| Policies document | 4-118 |
| Revocation | 4-113 |
| Certificate Revocation List (CRL) | 4-115 |
| Certificate Signing Request (CSR) | 4-112 |
| Chain of Custody (CoC) | 3-208-209 |
| CIDR → Classless Inter-Domain Routing (CIDR) | |
| Cipher | 4-7 |
| Cipher block chaining (CBC) | 4-63 |
| Cipher feedback | 4-63 |
| Ciphertext | 4-8 |
| CIS Controls | 2-114 |
| Controls | 2-120-121 |
| Critical Security Controls (CSC) | 2-116-117 |
| Guiding Principles | 2-117-118 |
| Sample Control #2 | 2-122 |
| Measures | 2-126 |
| Summary | 2-119 |
| CIS Controls Cloud Companion Guide | 1-142 |
| Cisco Discovery Protocol (CDP) | 1-36 |
| Claimant | 2-55 |
| Clair | 6-137 |
| Classless Inter-Domain Routing (CIDR) | 1-68 |
| closed-box diagramming → Network → Know Thy | |
| Network → Conceptual Design | |
| Cloud | 1-124 |
| Benefits | 1-127 |
| Logging | 1-160-162 |
| Providers | 1-134-136 |
| Comparison | 1-136 |
| Security | 1-138, 1-160 |
| Services | |
| Types | 1-129 |
| Shared Responsibility | 1-138-140 |
| Types | 1-125 |
| Cloud Computing | |
| Desktop as a Service (DaaS) | 5-198 |
| Infrastructure as a Service (IaaS) | 5-197 |
| Platform as a Service (PaaS) | 5-197 |
| Software as a Service (SaaS) | 5-198 |
| Cloud Security Alliance (CSA) | 1-143-145 |
| Cloud Service Provider (CSP) | 1-129 |
| CMD | |
| whoami.exe /priv | 5-101 |
| Cobalt Strike | 3-68 |
| Collision | 4-30, 4-32, 2-87 |
| Command Injection | 3-99-100 |
| Command Query Responsibility Segregation (CQRS) | |
| 3-158 | |
| Common Event Format (CEF) | 3-170 |
| Common Internet File System (CIFS) | 5-88, 5-162 |
| Common Vulnerability Scoring System (CVSS) .. | 3-23-26 |
| Communication Flow → Network → Know Thy Net- | |
| work | |
| Communication Protocols | 1-58 |
| Computational Complexity | 4-57-58 |
| Conceptual Design → Network → Know Thy Network | |
| Conditional Access | 2-31 |
| Confidentiality | 2-9-11 |
| In Transit | 4-84 |
| Configuration hardening | 2-21 |
| Configuration Management | 2-23-24 |
| Confusion | 2-84 |
| Constant Time | 4-57 |
| Containerization | 1-117 |

SEC401 – Security Essentials Bootcamp Style

| | |
|---|------------------|
| cgroups | 6-129 |
| CIS Benchmarks | 6-138 |
| Docker | 6-131 |
| Images | 6-132 |
| Security | 6-136 |
| Swarm Mode | 6-133 |
| Vulnerability Management | 6-137 |
| Kubernetes | 6-134 |
| Pods | 6-134 |
| Linux | |
| chroot | 6-124-125 |
| LXC | 6-128 |
| LXC vs. Docker | 6-130 |
| namespaces | 6-129 |
| Security | 6-135 |
| Summary | 6-143 |
| Terraform | 6-139-141 |
| Lifecycle | 6-140-141 |
| Security | 6-142 |
| Content Delivery Network (CDN) | 1-35 |
| Context | 2-34 |
| Continuous Integration / Continuous Delivery (CICD) | 1-131 |
| Continuous Backups | 2-150 |
| Controlling Access | 2-62 |
| Cookies | 3-134-136, 3-152 |
| Core Evaluation Test | 2-125 |
| Covenant | 3-68 |
| Creator Owner | 5-79-80 |
| Credentials | 2-51 |
| Certificate | |
| Expiration | 4-114 |
| Criticality 1-19, 3-22, 1-24, 1-29, 1-43, 1-45, 1-52-53 | |
| Cross-Site Scripting (XSS) | 3-110-111 |
| Cryptanalysis | 4-6 |
| Attacks | 4-77-78 |
| Crypto v Stego | 4-40 |
| Cryptographic devices | 2-80 |
| Cryptography | 4-6 |
| Chart | 4-13 |
| Concepts | 4-57-60 |
| Core Components | 4-8 |
| Detecting | 4-41 |
| Goals | 4-15 |
| Authenticaiton | 4-15 |
| Ingetrity | 4-15 |
| Non-repudiation | 4-15 |
| Summary | 4-79 |
| The Challenge | 4-14 |
| Cryptology | 4-6 |
| Cryptosystem | 4-9 |
| Fundamentals | 4-5 |
| Types | 4-24 |
| Asymmetric | 4-26 |
| Symmetric | 4-24, 25 |
| Custom Application-Specific Integrated Circuit (ASIC) 4-176 | |
| CyberArk | 2-71 |

D

| | |
|--------------------------------------|-----------------|
| Data | 1-24 |
| Communication Flow | 1-26 |
| Criticality | 1-24 |
| Storage | 1-24 |
| Data at Rest | 4-100 |
| Data Classification Labels | 2-161 |
| Data Encryption Standard (DES) | 4-63 |
| MitM Attack | 4-66 |
| Not a group | 4-65 |
| Weaknesses | 4-64 |
| Data Exfiltration | 3-57, 2-169-170 |
| Defense | 2-171-172 |
| Data in Transit | 4-83 |
| Data Leakage | 2-143, 2-153 |
| Prevention | 2-154, 2-158 |
| Storing Sensitive Data | 2-159 |
| Data Loss | 2-143-144 |
| Data Loss Prevention (DLP) | 1-26, 2-142 |
| Policies | 2-160 |
| Data Classification Labels | 2-161 |
| Examples | 2-162-163 |
| Strategies | 2-146 |
| Summary | 2-179 |
| Tools | 2-164 |
| Data Normalization | 4-158 |
| Data Parallelism | 2-98 |
| Data Protection | |
| Tokenization | 6-194 |
| Data Recovery | 2-152 |
| Debug Programs | 5-21 |
| Debug traces | 3-166 |
| Decapsulation | 1-62 |
| Decompiler | 3-124 |
| Decryption | 4-8 |
| Defense-in-Depth | |
| Cloud | 2-26-27 |
| Centralized Logging | 2-29 |
| Container Security | 2-29 |
| E-mail Protection | 2-28 |
| Firewall | 2-26-27 |
| IAM | 2-28 |
| IPS/IDS | 2-28 |
| VPN | 2-28 |
| Web Application Firewall (WAF) | 2-26-27 |
| Fixing the Problem | 2-25 |
| Defense-in-Depth (DiD) | 2-5, 1-47 |
| Approaches | 2-16 |
| Information-centric | 2-16, 2-19 |
| Protected enclaves | 2-16, 2-18 |
| Threat vector analysis | 2-16, 2-20 |
| Uniform Proection | 2-16-17 |
| Layers | |
| Application Security | 2-6 |
| Data Security | 2-6 |
| Host Security | 2-6 |
| Network Security | 2-5 |
| Perimeter Security | 2-5 |

SEC401 – Security Essentials Bootcamp Style

| | |
|--|-----------------|
| Strategies | 2-13 |
| Filtering | 2-14-15 |
| Summary | 2-45 |
| Types | |
| Detection | 2-5 |
| Deterrent | 2-5 |
| Prevention | 2-5 |
| Defensible Network Architecture | 1-31 |
| Demilitarized Zone (DMZ) | 1-48, 1-51 |
| Denial of Service (DoS) | |
| 802.11 | 1-211 |
| Denial of Services (DoS) → Router → Attacks | |
| Denylisting | 3-112 |
| Desktop as a Service (DaaS) | 5-66 |
| Development | 3-142 |
| DHCP Manipulation → Switch → Attacks | |
| Differential Backups | 2-150 |
| Diffie-Helman Key Exchange | 4-27 |
| Diffusion | 2-84 |
| Digest | 2-82 |
| Digital Certificates | 4-118 |
| Digital fingerprint | 4-30 |
| Digital Forensics | 3-204 |
| Artifacts | 3-210-211 |
| Filesystem Timestamps | 3-211 |
| Follow the Evidence | 3-207 |
| In Practice | 3-205 |
| Investigative Process | 3-206 |
| Subdisciplines | 3-213 |
| Endpoint | 3-213 |
| Network | 3-213 |
| Reverse Engineering | 3-214 |
| Threat Intelligence | 3-213 |
| Tools | 3-215 |
| Digital Forensics and Incident Response | |
| Summary | 3-237 |
| Digital identity | 2-48 |
| Digital Signature | 4-34 |
| Example | 4-36 |
| Digital Watermarking | 2-177 |
| Directory traversal | 3-150 |
| Disassembler | 3-124 |
| Disaster Recovery | 1-118 |
| Discovery Protocol | 1-36 |
| Discrete Logarithm | 4-60-61 |
| Discretionary Access Control (DAC) | 2-64 |
| Distinguished Name (DN) | 4-112 |
| Distributed Denial of Service (DDoS) | 2-14 |
| Distributed Denial of Services (DDoS) → Router → Attacks | |
| Digital Forensics | |
| Time | 3-212 |
| Document Watermarks | 2-177 |
| Domain Controller | 5-24 |
| Domain Name Service (DNS) | 1-48 |
| DoublePulsar | 3-91 |
| Downgrade Attack | 1-37, 1-205-206 |
| Dragonblood | 1-205 |

| | |
|---|-----------|
| Dragonfly | 1-202-203 |
| DREAD | 3-27 |
| Dynamic Host Configuration Protocol (DHCP) .. | 1-38 |
| Dynamic Trunking Protocol (DTP) | 3-31 |

E

| | |
|---|--------------|
| Elastic Compute Cloud (EC2) | 1-153 |
| Amazon Machine Images (AMIs) | 1-154 |
| Security Groups | 1-155 |
| Elastic Stack | 3-179, 3-186 |
| Electronic codebook (ECB) | 4-63 |
| Elliptic Curve Cryptosystem (ECC) | 4-73 |
| Elliptic Curves | 4-61 |
| Empire | 3-68 |
| Encapsulating Security Payload (ESP) | 4-92-93 |
| Confidentiality | 4-95 |
| Encapsulation | 1-62 |
| EnCase | 3-215 |
| Encryption | 4-7-8 |
| Summary | 34-49-50 |
| Endpoint Detection and Response (EDR) | 2-15 |
| Endpoint Security | |
| Anomalies | 4-192-193 |
| Application Control | 4-203 |
| Baselines | 4-190 |
| Establish | 4-191 |
| Core Components | 4-188 |
| Enhancing | 4-189 |
| File Integrity Checking | 4-199 |
| Steps | 4-200 |
| Firewall | 4-197 |
| Types | 4-198 |
| Log Monitoring | 4-201 |
| Objectives | 4-186 |
| Solutions | 4-194 |
| Enrollment | 2-51 |
| Enterprise Crypto | 4-13 |
| Ephemeral environment | 1-130 |
| Error handling | 3-144 |
| Error-Correction Code (ECC) memory | 2-147 |
| Eternal Blue | 3-91 |
| ETERNALBLUE | 3-29 |
| Event | 3-220 |
| Event of Interest (EOI) | 4-148 |
| Event-triggered computing | 1-130 |
| Evil Twin | 1-209-210 |
| Exfiltration | 1-27 |
| Exploitation | 3-56 |
| Exploitation Framework | 3-66 |
| eXtensible | 1-46 |
| Extensible Authentication Protocol over LAN (EAPOL) | 1-46 |

F

| | |
|--------------------------|------|
| Factoring Integers | 4-59 |
|--------------------------|------|

SEC401 – Security Essentials Bootcamp Style

| | |
|-------------------------------------|-----------------------------|
| Field-Level Encryption | 6-176 |
| File Integrity Checking (FIC) | 4-199 |
| Steps | 4-200 |
| Filesystem Timestamps | 3-211 |
| Finite Fields | 4-60 |
| Firewall | 2-14, 1-48, 49, 1-51, 4-135 |
| Anti-Spoofing | 4-139 |
| Application Control | 4-198 |
| Benefits | 4-136 |
| Default Rule | 4-137 |
| Endpoint | 4-197 |
| Filtering | 4-138 |
| Shortcomings | 4-136 |
| Types | 4-140 |
| Flow Control | 1-85 |
| Fluentd | 3-178 |
| Frequency Analysis | 4-21 |
| Full Disk Encryption | 4-101, 5-107 |
| Full System Imaging | 2-150 |
| Function-as-a-Service (FaaS) | 1-130 |

G

| | |
|---|-----------|
| GDPR | 2-137 |
| General Data Protection Regulation (GDPR) ... | 2-155 |
| Global Catalog Servers | 5-32 |
| GNU Privacy Guard (GPG) | 4-102-103 |
| Key and Passphrase | 4-104 |
| Use | 4-105 |
| Governance, Risk Management and Compliance (GRC) | 1-143 |
| GPU Acceleration | 2-98 |
| Graylog2 | 3-186 |
| Group Policy Object (GPO) | 5-37-39 |

H

| | |
|---|------------|
| Hardening | 2-21, 2-23 |
| Hash Functions | 4-30 |
| Hashcat | 2-103-104 |
| HashiCorp Vault | 2-71 |
| Hasing | 2-81 |
| Headers → Protocol → Headers | |
| Heartbleed | 3-23 |
| Histograms | 4-42 |
| Honeynet | 2-173 |
| Honeypot | 2-173 |
| Honeytoken | 4-160 |
| Host Intrusion Detection System (HIDS) | 4-205 |
| Advantages | 4-207 |
| Challenges | 4-208-209 |
| Developments | 4-210 |
| Network Monitoring | 4-206 |
| Recommendations | 4-210 |
| Host Intrusion Prevention System (HIPS) | 4-212 |
| Advantages | 4-213 |
| Application Behavior Monitoring | 4-215 |

| | |
|--|------------------|
| Challenges | 4-214 |
| Developments | 4-212 |
| Recommendations | 4-216 |
| Summary | 4-218 |
| HTTP → HyperText Transfer Protocol (HTTP) | |
| HTTPS | 4-120 |
| Illustration | 4-122 |
| HTTPS → HyperText Transfer Protocol (HTTPS) ... | |
| Hub | 1-37 |
| HyperText Transfer Protocol Secure (HTTPS) 1-85-86 | |
| HyperText Transfer Protocol (HTTP) | 1-85-86 |
| Hypervisor | 1-111-113, 1-120 |

I

| | |
|---|-------------------|
| ICMP → Network Protocol → Internet Control Mes- sage Protocol (ICMP) | |
| Identity Access Management (IAM) | 2-50 |
| Identity and Access Management (IAM) | |
| AWS | 2-32-33 |
| Azure | 2-31 |
| Cloud | 2-28 |
| On-Premise | 2-30 |
| Identity Assurance Levels (IAL) | 2-51, 2-53, 2-109 |
| Identity Lifecycle | 2-28 |
| Identity Management | 2-47 |
| Identity Proofing | 2-52 |
| IETF | |
| RFC 2401 | 4-91 |
| Incident | 3-220 |
| Incident Handling | 3-219 |
| Common Problems | 3-221 |
| Containment | 3-228 |
| Detection | 3-226 |
| Eradication | 3-229 |
| Identification | 3-226 |
| Key Mistakes | 3-233 |
| Lessons Learned | 3-232 |
| Preparation | 3-224-225 |
| Process | 3-221 |
| Putting it all together | 3-235 |
| Recovery | 3-230 |
| Remediation | 3-231 |
| Taking Notes | 3-234 |
| Triage | 3-226 |
| Verification | 3-226 |
| Incident Response | 3-204 |
| Threat Hunting | 3-236 |
| Incremental Backups | 2-150 |
| INF templates | 5-132-136 |
| Infrastructure as Code (IaC) | 6-192 |
| Infrastructure-as-a-Service (IaaS) | 1-129 |
| Infrastructure-as-Code (IaC) | 1-131 |
| Initial Sequence Number (ISN) | 1-89 |
| Input Attacks | 3-98 |
| Insider Threats | 2-174-175 |
| Institute of Electrical and Electronic Engineers (IEEE) | |
| 1-172 | |

SEC401 – Security Essentials Bootcamp Style

| | |
|---|-----------------------------|
| Integrity | 2-9-11, 4-15, 4-33 |
| Hash | 4-30 |
| Integrity Check Value (ICV) | 4-92-93 |
| Inter-Domain Replication | 5-32 |
| International Data Encryption Algorithm (IDEA) | 4-25 |
| International Organization for Standardization (ISO) | 1-59 |
| International Telecommunication Union (ITU) .. | 1-229 |
| International Telecommunications Union (ITU) .. | 4-118 |
| Internet Gateway (IGW) | 1-149 |
| Internet Key Exchange (IKE) | 4-96 |
| Internet of Things (IoT) | 1-231-232 |
| Internet Protocol (IP) | 1-85 |
| Internet Protocol → Network Protocol (IP) → Inter- net Protocol (IP) | |
| Internet Security Association and Key Management Protocol (ISAKMP) | 4-96 |
| Intractable | 4-29 |
| Intractable Problems | 4-57-58 |
| Intrusion Detection System (IDS) ... | 1-101, 102, 4-146 |
| Alerts | 4-148-149 |
| Data Normalization | 4-158 |
| Is Not | 4-147 |
| Referenced Architecture | 4-181 |
| Wireless | 4-170 |
| Intrusion Pervention System (IPS) | 4-172 |
| Is Not | 4-173 |
| Intrusion Prevention System (IPS) | 2-28 |
| Referenced Architecture | 4-181 |
| Intrusion Detection and Prevention | 2-168 |
| Intrusion Detection System (IDS) | 2-28, 2-168 |
| Host IDS | 2-168 |
| Network IDS | 2-168 |
| IP → Network Protocol (IP) → Internet Protocol (IP) | |
| IP → Network Protocol → Internet Protocol (IP) | |
| IPsec | 1-44, 1-70, 4-91, 5-175-178 |
| Group Policy | 5-177-178 |
| Headers | 4-92 |
| Modes | 4-95 |
| Security Associations | 4-96 |
| IPv4 | 1-55, 1-68-72 |
| Address Space | 1-68, 1-70 |
| Fragmentation | 1-72 |
| Header | 1-71-72 |
| Time-to-live (TTL) | 1-72 |
| IPv6 | 1-55, 1-68-70, 1-74 |
| Address Space | 1-68, 1-70 |
| Header | 1-74 |
| Flow Label | 1-74 |
| Traffic Class | 1-74 |
| Quality of Service (QoS) | 1-70 |
| Translation | 1-76 |
| Tunneling | 1-76 |
| ISO 27000 | 1-142 |
| ISO 27001 | 2-137 |
| ISO → International Organization for Standardization (ISO) | |

J

| | |
|------------------|-------|
| Journaling | 2-147 |
|------------------|-------|

K

| | |
|---------------------------------------|-----------------|
| Kerberos | 5-28, 5-162-163 |
| Example | 5-30 |
| Golden Tickets | 5-29 |
| Key Distribution Centers (KDCs) | 5-28 |
| Risks | 5-29 |
| Kernal | |
| Containerization | 6-129 |
| Key Derivation Function | 2-81-82 |
| Quality | 2-84 |
| Key Exchange | 4-27 |
| Key Length | |
| Comparison | 4-74 |
| Key Stretching | 2-82 |
| Keyed hash | 4-93 |
| Keys | 4-10 |
| Protection | 4-12 |
| Keyspace | 4-10 |
| Know Thy Systems | 1-17 |
| Know your Environment | 1-17 |
| KRACK | 1-198 |

L

| | |
|---|------------|
| LAN Manager (LM) | 2-89 |
| Lateral Movement | 3-57 |
| Lattice-Based Access Control (LBAC) | 2-65 |
| Layer 3 | 1-85 |
| Layer 4 | 1-85 |
| Layer Independence | 1-62 |
| Leased Line | 4-85 |
| Least Significant Bit (LSB) | 4-46, 4-48 |
| Lightweight Directory Access Protocol (LDAP) .. | 5-162-163 |
| Linear Time | 4-57 |
| Linux | 6-12 |
| Commands | |
| grep | 6-54 |
| List active services | 6-55 |
| List services | 6-55 |
| ls | 6-52 |
| netstat | 6-52 |
| ps | 6-52 |
| su | 6-43-44 |
| sudo | 6-43-44 |
| tail | 6-53 |
| Configuration Management Tools | 6-119 |
| Ansible | 6-120 |
| Console | 6-20 |
| Containerization | |
| chroot | 6-124-125 |
| LXC | 6-128 |
| Criticality | 6-6 |

SEC401 – Security Essentials Bootcamp Style

| | | | |
|--|-----------|--|-----------|
| Cron | 6-61 | Lynis | 6-83 |
| daemons | 6-55 | Modprobe | 6-75 |
| Disk Monitoring (df) | 6-25 | OpenSCAP | 6-84-85 |
| Distros | 6-10-11 | SELinux | 6-68-69 |
| File Attributes | 6-29 | SSH Hardening | 6-77 |
| ls -l | 6-29 | SSH MFA | 6-78 |
| File Permissions | 6-30 | SSH/TLS Key Management | 6-79 |
| chmod (change mode) | 6-30 | Summary | 6-121 |
| chown and chgrp | 6-40 | Sysctl Hardening | 6-73-74 |
| flags/bits | 6-31 | Services | 6-55 |
| other bits | 6-32 | Shadow File | 6-47 |
| other bits in absolute mode | 6-33 | Shell | 6-20-21 |
| set-UID | 6-32 | Ststemd | 6-57-60 |
| sticky | 6-32 | SUID/SGID Programs | 6-37 |
| Umask and Chmod | 6-38-39 | Summary | 6-66 |
| Files versus Directories | 6-34-35 | Superuser | 6-42 |
| Filesystem | | swap space | 6-25 |
| Security | 6-26-27 | System Accounts | 6-45 |
| Find command | 6-37 | Terminal | 6-20 |
| Firewalls | 6-111 | Threat hunting | 6-52 |
| Iptables | 6-112-115 | Types | 6-10 |
| Hard Disk Encryption | 6-28 | Unified Key Setup (LUKS) | 6-28 |
| initd | 6-56 | User Accounts and Groups | 6-41 |
| runlevels | 6-56 | UID and GID | 6-41 |
| Logical Filesystem | 6-22 | vs Windows | 6-7-8 |
| Logs | | Vulnerabilities | 6-14-15 |
| auditd | 6-104-110 | World-Writable Directories | 6-36 |
| Centralized Logging | 6-102-103 | LM/NTLM Hashes | 2-89 |
| Key Log Files | 6-87-90 | Log Event Extended Format (LEEF) | 3-170 |
| Logrotate | 6-99-101 | Log file | 3-166 |
| Parsing | 6-54 | Logging | 3-166 |
| Rsyslog | 6-98 | Logical Design → Network → Know Thy Network | |
| Syslog | 6-91-96 | Logical Topology → Topologies | |
| Syslog-NG | 6-97 | LogRhythm | 3-186 |
| Objectives | 6-4 | Logs | |
| Package Management | 6-62 | Agent | 3-168 |
| Advanced Packaging Tool (APT) | 6-64-65 | Aggregation | 3-185 |
| Features | 6-63 | Analysis Tools | 3-178-180 |
| Passwd File | 6-46 | Augmentation | 3-168 |
| Physical Filesystem | 6-23-24 | Azure Monitor | 5-234-238 |
| Partitions | 6-23-24 | Azure Sentinel | 5-239-243 |
| Security | 6-24 | Benefits | 3-199 |
| Pluggable Authentication Modules (PAM) ..6-48-49 | | Centralize | 3-185 |
| Policy Enforcement | | Collection Architecture | 3-169 |
| Passwords | 6-50 | Correlation | 3-185-186 |
| User lockout | 6-51 | Encryption | 3-178 |
| Privilege Elecation | 6-43 | Endpoint | 4-201 |
| Rootkit Detectors | 6-116 | Filtering | 3-173 |
| chkrootkit | 6-118 | Key Points | 3-172 |
| rkhunter | 6-117 | Lack of Accepted Standards | 3-170 |
| Security | | Linux | |
| AppArmor | 6-70-71 | auditd | 6-104-110 |
| AppArmor and SELinux Comparison | 6-72 | Logrotate | 6-99-101 |
| CIS Hardening Guides | 6-82 | Rsyslog | 6-98 |
| Disable Dynamic Loading | 6-76 | Syslog | 6-91-96 |
| Hardening Scripts | 6-80-81 | Syslog-NG | 6-97 |
| InSpec | 6-86 | Management | 3-171 |
| | | Challenges | 3-184 |

SEC401 – Security Essentials Bootcamp Style

| | |
|------------------------|-----------|
| Monitoring | |
| Setup | 3-182-183 |
| Strategy | 3-181 |
| Parsing | 3-168 |
| Ports | 3-168 |
| Pre-processing | 3-178 |
| Pull | 3-169 |
| Push | 3-169 |
| Reports | 3-174-176 |
| Server | 3-168 |
| SIEM | 3-185-186 |
| Summary | 3-200 |
| Tasks | |
| Annual | 3-198 |
| Daily | 3-194 |
| Monthly | 3-196 |
| Quarterly | 3-197 |
| Real-Time | 3-193 |
| Weekly | 3-195 |
| Windows | |
| Configuration | 5-281 |
| Size and Wrapping | 5-290-291 |
| What should be logged? | 5-292-293 |
| Windows Firewall | 5-169 |
| Logstash | 3-186 |

M

| | |
|---------------------------------|------------|
| MAC Flooding → Switch → Attacks | |
| MACB | 3-211 |
| macOS | 6-203 |
| Hardening | 6-212 |
| Malware | 6-214 |
| Security Features | 6-204-211 |
| Summary | 6-215 |
| Vulnerabilities | 6-213 |
| macOS (BSD) | 6-16 |
| Maintaining Access | 3-57 |
| Maintenance | 2-66 |
| Malware | 3-114 |
| Adware and Spyware | 3-119 |
| Analysis | 3-120 |
| Behavior | 3-123 |
| Code Reversing | 3-124 |
| Fully Automated | 3-121 |
| Static | 3-122 |
| Rootkits | 3-118 |
| Trojans | 3-117 |
| Viruses and Worms | 3-115-116 |
| Man in the Middle (MiTM) | 1-35 |
| Management Subnets | 1-156 |
| Mandatory Access Control (MAC) | 2-64 |
| Masquerading AP | 1-209-210 |
| MD4 | 4-30 |
| MD5 | 4-30, 2-87 |
| Media Access Control (MAC) | 1-37 |
| Meltdown and Spectre | 3-30 |
| Members | 2-34 |

| | |
|---|------------------|
| Message | 3-166 |
| Message Digest | 4-30 |
| Message Digest (MD) | 2-87 |
| Message Digest 2 (MD2) | 4-30 |
| Message Integrity Check (MIC) | 1-196 |
| Metasploit | 3-66 |
| Meterpreter | 3-67 |
| Microservice Architecture | 3-158 |
| Attack Surface | 3-159 |
| Microsoft | |
| 365 | 5-200 |
| Azure | 5-199 |
| Cloud Computing | 5-196, 5-199-202 |
| Summary | 5-247 |
| Command Line Tools | 5-258 |
| Defender | 5-212-214 |
| OneDrive | 5-200 |
| Microsoft Azure | |
| Active Directory (AD) | 5-203 |
| Administrative Roles | 5-209-210 |
| Connect tool | 5-205-206 |
| Federation Services | 5-206 |
| Single Sign-On | 5-207-208 |
| Sync | 5-205-206 |
| Active Directory Domain Services (ADDS) | 204 |
| Automation | 5-277-279 |
| Graphical Runbooks | 5-280 |
| Jobs | 5-277 |
| Power Automate | 5-278 |
| Runbook | 5-277 |
| Worker | 5-277 |
| Endpoint Security | 5-211-215 |
| Conditional Access | 5-221-226 |
| Intune | 5-21-220 |
| Microsoft 365 Defender | 5-212-214 |
| Multifactor Authentication | 5-215 |
| Functions | 5-279 |
| Logic Apps | 5-239 |
| Monitor | 5-234-238 |
| Activity Log | 5-238 |
| Agents and Workspaces | 5-236-237 |
| logging | 5-237 |
| metrics | 5-237 |
| telemetry | 5-237 |
| tracing | 5-237 |
| Policy | 5-227-233 |
| Initiative | 5-228-230 |
| Key Vault | 5-231-233 |
| Security Center | 5-244-246 |
| Auto-Provisioning | 5-245 |
| Sentinel | 5-239-243 |
| Data Connectors | 5-240-241 |
| Playbooks | 5-242-243 |
| Tools | 5-272 |
| CLI | 5-273 |
| Cloud Shell | 5-273-276 |
| PowerShell | 5-272 |
| Resource Manager (ARM) Templates | 5-274 |

SEC401 – Security Essentials Bootcamp Style

| | |
|---|--------------------|
| Web Portal | 5-272 |
| Microsoft Azure Active Directory (MAAD) | 5-203 |
| Microsoft Azure Management (MAM) | 5-226 |
| Mimikatz | 5-29, 2-103, 2-106 |
| MISP | 3-190-191 |
| MITRE ATT&CK Framework | 2-116, 2-133-135 |
| Mobile | 1-229 |
| Device Security | 2-182 |
| Malware | 2-200-204 |
| Operating System (OS) | |
| Market Share | 2-184 |
| Problems and Opportunities | 2-195 |
| Summary | 2-205 |
| Threats | 2-196-198 |
| Mobile Device Management (MDM) | 2-198, 5-211 |
| Monitoring | 2-66, 3-166 |
| Web App | 3-154-155 |
| Monolithic Architecture | |
| Security Controls | 3-157 |
| MS17-010 | 3-29 |
| MSTSC.exe | 5-182 |
| Multi-Factor Authentication (MFA) | 2-108 |
| Multi-master Replication | 5-24 |

N

| | |
|---|-----------------|
| NAT → Network Address Translation (NAT) | |
| Nation State Actors → Threat Agents | |
| Need to Know | 2-62 |
| Nessus | 3-55 |
| NetBIOS and WINS | 5-164 |
| Netflow | 3-213 |
| NETSH.exe | 5-172 |
| IPsec | 5-176 |
| Network | |
| Architecture | 1-17 |
| Attacks | 1-29 |
| Authentication | 1-46 |
| Communication | 1-57-58 |
| Design | |
| Segmentation | 1-43 |
| Design Objectives | 1-47 |
| Know Thy Network | |
| Communication Flow | 1-26 |
| Conceptual Design | 1-19 |
| Logical Design | 1-21 |
| Physical Design | 1-22 |
| Valuable Data | 1-24 |
| Security | |
| 802/1X | 1-46 |
| Virtual LAN (VLAN) | 1-45 |
| Software Defined Networking (SDN) | 1-43-44 |
| Network Access Control | 1-46 |
| Network Access Control List (NACL) | 2-18, 1-149-150 |
| Subnets | 1-149-150 |
| Network Address Translation (NAT) | 1-68, 1-149 |
| Gateway | 1-151 |
| Network Architecture | |

| | |
|--|------------------|
| Benefits | 1-52 |
| Network Interface Card (NIC) | 1-101 |
| Network Intrusion Detection System (NIDS) | |
| Advantages | 4-159 |
| Challenges | 4-161 |
| Developments | 4-169-170 |
| Fingerprinting | 4-169 |
| Key Points | 4-168 |
| Packet Inspection | 4-157 |
| Network Intrusion Prevention System (NIPS) | 4-174 |
| Challenges | 4-177 |
| Detail | 4-175-176 |
| Developments | 4-178-179 |
| Passive Analysis | 4-180 |
| Network Intrusion Detection System (NIDS) | 4-150 |
| Analysis Types | 4-150 |
| Network Protocol | 1-55, 1-57 |
| Internet Control Message Protocol (ICMP) | 1-55, 1-79-82 |
| Common Types and Codes | 1-81-82 |
| Header | 1-81 |
| Internet Protocol (IP) | 1-55, 1-67 |
| Transmission Control Protocol (TCP) | 1-55, 1-85-99 |
| Header | 1-90-91 |
| User Datagram Protocol (UDP) | 1-94-97 |
| Header | 1-98-99 |
| Network Security | |
| Big Picture | 4-133 |
| Devices | 4-132 |
| Objectives | 4-131 |
| Referenced Architecture | 4-181 |
| Summary | 4-182 |
| Network Security Group (NSG) | 2-36 |
| Network Security Groups | 2-27 |
| Network Segmentation | |
| AWS | 2-37 |
| Azure | 2-36 |
| GCP | 2-38 |
| On-Premise | 2-35 |
| Network-based Security Control | 1-46 |
| NFC Forum | 1-224 |
| NIC → Network Interface Card (NIC) | |
| NIST 800-53 | 2-137 |
| NIST 800-53R4 | 1-142 |
| NIST 800-63 | 2-53 |
| NIST Framework | 2-114-115, 2-127 |
| Core | 2-128 |
| Functions | 2-127-128 |
| Implementation Tiers | 2-130-131 |
| Profiles | 2-132 |
| Nmap | 3-61-65 |
| OS Identification | 3-65 |
| Non-repudiation | 4-15, 4-29, 4-34 |
| NotPetya | 1-43 |
| NT File System (NTFS) | 5-73-74 |
| Access Control Entry (ACE) | 5-76 |
| Advanced Security Settings | 5-77-78 |

SEC401 – Security Essentials Bootcamp Style

| | |
|------------------------------------|-----------|
| AGULP | 5-83-84 |
| ACLs | 5-76 |
| Logging | 5-287-289 |
| Owners | 5-79 |
| Principle of Least Privilege | 5-81-82 |
| Share ACLs | 5-93-94 |
| Shared Folder Permissions | 5-88-90 |
| NT LAN Manager (NTLM) | 2-90-91 |
| NT LAN Manager (NTML) | 5-31 |
| NTFS | 3-211 |
| NULL algorithm | 4-93 |
| null user session | 5-143 |
| NXLog | 3-178 |

O

| | |
|---|---------------|
| Oakley Key Determination Protocol (Oakley) | 4-96 |
| OAuth | 2-60 |
| On-The-Fly Encryption | 4-101 |
| One-way encryption | 4-30 |
| Online Certificate Status Protocol (OCSP) | 4-116 |
| Open Handset Alliance (OHA) | 2-188-190 |
| Open Systems Interconnect (OSI) | 1-58-59, 1-63 |
| Layer 1(Physical) | 1-60 |
| Layer 2(Data Link) | 1-60 |
| Layer 3(Network) | 1-60 |
| Layer 4(Transport) | 1-60 |
| Layer 5(Session) | 1-60 |
| Layer 6(Presentation) | 1-59 |
| Layer 7(Application) | 1-59 |
| Open Web Application Security Project (OWASP) . | 3-46 |
| Open-Source Intelligence (OSINT) Gathering | 3-53 |
| OpenVAS | 3-55 |
| Operating System (OS) | |
| Best? | 6-17 |
| Hardware | 6-18 |
| Market Share | 6-5 |
| Overview | 6-18 |
| Userland | 6-18 |
| Operating System Identification | 3-65 |
| Opportunistic Attacker → Threat Agents | |
| Opportunistic Wireless Encryption (OWE) . | 1-202-204 |
| Organized Cybercrime → Threat Agents | |
| OSI → Open Systems Interconnect (OSI) | |
| OSSEC | 3-178 |
| OSSIM | 3-179 |
| Output Feedback (OFB) | 4-63 |
| OWASP Top 10 | 3-140-141 |

P

| | |
|--|-------|
| Packet | 1-58 |
| Packet Inspection | 4-157 |
| Packet Misrouting → Router → Attacks | |
| Packet Sniffing → Router → Attacks | |
| Parsing | 3-168 |

| | |
|--|----------------|
| Passive Analysis | 4-180 |
| Password | |
| Compromise | 3-70 |
| Cracking | 2-93-95 |
| Speeding up | 2-93-95 |
| Tools | 2-103 |
| Dumps | 2-92 |
| Hash | 2-84 |
| Policy | 2-99 |
| Reuse and Stuffing | 3-71 |
| Specialized Attacks | |
| Brute-force | 2-96, 2-105 |
| Combinator | 2-104 |
| Dictionary | 2-96, 2-104 |
| Hybrid | 2-96-97, 2-105 |
| Precomputation | 2-96-97, 2-101 |
| Spraying | 3-72 |
| Storage | 2-81 |
| Password Cracking and Denial of Service (DoS) . | 1-207 |
| Password Vault | 2-69-71 |
| PATH | 5-258 |
| Pattern matching | 4-151 |
| PBKDF2 | 2-84-85 |
| PCI | 2-137 |
| Peer review | 3-142 |
| Penetration Testing | 3-33-36, 3-40 |
| Phases | 3-52 |
| Process | 3-51 |
| Rules of Engagement | 3-41 |
| Scoping | 3-42 |
| Summary | 3-74 |
| Tools | 3-60 |
| Types | 3-43 |
| External | 3-44 |
| Internal | 3-45 |
| Other | 3-49 |
| Social Engineering | 3-47-48 |
| Web Application | 3-46 |
| Pepper | 2-82, 2-101 |
| Permutation | 4-16, 4-22 |
| Personal Area Network (PAN) | 1-213-214 |
| Bluetooth | 1-216 |
| Attack: BlueBorne | 1-218-219 |
| Protections | 1-220-221 |
| Special Interest Group (SIG) | 1-216 |
| Near Field Communications (NFC) | 1-224-225 |
| Radio Frequency Identification (RFID) . | 1-226-227 |
| Zigbee | 1-222-223 |
| Phishing | 3-48 |
| Physical Design → Network → Know Thy Network ... | |
| Physical Topology → Topologies | |
| PICERL | 3-220-221 |
| Ping | 1-82 |
| Pivoting | 3-57 |
| Plaintext | 4-8 |
| Platform-as-a-Service (PaaS) | 1-129 |
| Point-to-Point Tunneling Protocol (PPTP) | 5-165 |
| Poisoning | 3-73 |

SEC401 – Security Essentials Bootcamp Style

| | | | |
|--|-----------|--|------------------|
| Policy | 2-34 | Privileged access | 2-68 |
| Policy Enforcement Point (PEP) | 2-69 | Privileged Access Management (PAM) | 2-69-71 |
| Polynomial Time | 4-57 | Privileged Identity Management (PIM) | 2-72 |
| Port Scanning | 3-61 | Procedures → Threat Enumeration | |
| Ports | | Protocol | |
| Numbers | 1-98 | NetBIOS (TCP/UDP/137;UDP/138;TCP/139;TCP/UDP/139-143) | 5-164 |
| TCCP | | Productivity Impact Loss | 1-34 |
| Telnet (23) | 1-86 | Promiscuous mode | 1-101 |
| TCP | | Protected Management Frames (PMF) | 1-203 |
| DNS (53) | 1-86 | Protocol | |
| FTP (21) | 1-86 | DNS (TCP/UDP/53) | 5-164 |
| FTP Data (20) | 1-86 | Headers | 1-62 |
| HTTP (80) | 1-86 | IPsec (UDP/500/4500 for IKE; Protocols 50 and 51 for ESP and AH) | 5-164 |
| HTTPS (443) | 1-86 | Kerberos (TCP/UDP/88) | 5-162-163 |
| SMTP (25) | 1-86 | LDAP (TCP/389/636/3268/3269) | 5-162-163 |
| SSH (22) | 1-86 | RDP (TCP/UDP/3389) | 5-164, 5-187-190 |
| SSL (443) | 4-120 | RPC (TCP/135) | 5-162 |
| TLS (443) | 4-120 | SMB (TCP/139/445) | 5-162 |
| UDP | | SQL Server (TCP/UDP/1433/1434) | 5-164 |
| BOOTP/DHCP (67 and 68) | 1-96-97 | Stack | 1-57-59 |
| DNS (53) | 1-96-97 | Communication | 1-61 |
| NFS (2049) | 1-96-97 | TCP/IP | 1-63-65 |
| NTP (123) | 1-96-97 | Stacks | 1-55 |
| SNMP (161 and 162) | 1-96-97 | Protocol Analysis | 4-155 |
| TFTP (69) | 1-96-97 | Proxy | 1-48-49 |
| Post-Exploitation | 3-57 | Proxy Gateway | 4-144 |
| PowerShell | | Proxy Server | 2-14 |
| Az.KeyVault | 5-232 | Public Key Encryption | 4-26, 4-29 |
| Credential Guard | 5-149 | Public Key Infrastructure (PKI) | 4-107 |
| Detailed | 5-252-257 | Benefits | 4-125 |
| export-csv | 5-256 | Lifecycle | 4-112 |
| format-list | 5-256 | Registration | 4-112-114 |
| fsutil | 5-74 | Operational Goals | 4-112 |
| get-ciminstance | 5-257 | Problems | 4-124 |
| Get-Command -Module NetSecurity | 5-173 | Summary | 4-127 |
| Get-Help | 5-176 | Purple Team | 3-39 |
| get-help | 5-257 | | |
| Get-Help LocalUser | 5-18 | | |
| get-process | 5-256 | | |
| get-scheduledtask | 5-270 | | |
| get-service | 5-257 | | |
| Get-SmbShare | 5-91 | | |
| Get-WindowsFeature | 5-10 | | |
| get-winevent | 5-257 | | |
| Get-WmiObject | 5-264 | | |
| MSTSC.exe | 5-182 | | |
| New-SmbShare | 5-89 | | |
| PATH | 5-258 | | |
| Set-ACL | 5-76 | | |
| Set-ItemProperty | 5-95 | | |
| Show-EventLog | 5-281 | | |
| wf | 5-166 | | |
| whoami | 5-21 | | |
| Pre-shared Key (PSK) | 1-202 | | |
| Principle of Least Privilege . 1-43, 1-52, 2-62, 5-81-82 | | | |
| Printer Dots | 2-177 | | |
| Private Network | 4-84 | | |
| Privilege escalation | 3-57 | | |

Q

| | |
|---|-------|
| QoS → IPv6 → Quality of Service (QoS) | |
| QRadar | 3-186 |
| Quadratic Time | 4-57 |
| Qualys | 5-245 |

R

| | |
|---|-----------|
| RaaS → Ransomware as a Service (RaaS) | |
| RAID configuration | 2-147 |
| Rainbow tables | 2-98 |
| Ransomware | 2-145 |
| Ransomware as a Service (RaaS) | 3-95 |
| Example | 3-96 |
| RC4 | 1-188-190 |
| Read-Only Domain Controller (RODC) | 5-25 |
| Reconnaissance | 3-53 |

SEC401 – Security Essentials Bootcamp Style

| | |
|--|--------------------|
| Red Team | 3-37 |
| Redundancy | 2-146-147 |
| Cloud | 2-146-147 |
| Refresh Token | 2-60 |
| REGEDIT.exe | 5-95 |
| Permissions | 5-98 |
| Security Policy Enforcement | 5-98 |
| Regions | 1-147 |
| Registration Authorities | 4-110 |
| Remote Access | 4-89 |
| Remote Desktop | 5-184 |
| Remote Desktop Protocol (RDP) | 5-187-190 |
| Authentication | 5-188 |
| Group Policy | 5-188 |
| Remote Desktop Services (RDS) | 5-180-181 |
| Best Practices | 5-189 |
| Remote Procedure Call (RPC) | 5-162 |
| Remoted Desktop Protocol (RDP) | 5-164 |
| Reporting | 3-57 |
| Resilient File System (ReFS) | 5-74 |
| Resolution | 2-52 |
| Responder | 3-73 |
| Retransmission | 1-85 |
| Revocation | 2-66 |
| Risk | 2-7-12, 3-22, 1-48 |
| Analysis | 3-28 |
| Assessment | |
| Qualitative | 3-28 |
| Quantitative | 3-28 |
| Customized Calculation | 3-28 |
| Ratings | |
| Dangers | 3-27 |
| Rogue Access Point | 1-206 |
| Role-Based Access Control (RBAC) | 2-34, 2-65 |
| Roles | 2-34 |
| Rootkit | 3-118 |
| ROT-13 | 4-18 |
| Rotation of Duties | 2-62 |
| Router | 1-29, 1-34 |
| Attacks | |
| Denial of Service (DoS) | 1-34 |
| Distributed Denial of Service (DDoS) | 1-34 |
| Packet Misrouting | 1-34 |
| Packet Sniffing | 1-34 |
| Routing Table Poisoning | 1-34 |
| Routing Table Poisoning → Router → Attacks | |
| RSA | 4-34, 4-72 |
| Usage | 4-72 |
| Vulnerabilities | 4-72 |
| Ruleset-Based Access Control | 2-31 |

S

| | |
|--|-----------------|
| Salt | 2-82, 2-101-102 |
| SAML | 2-59 |
| SANS Investigative Forensic Toolkit (SIFT) | 3-216-217 |
| Scanning and Enumeration | 3-54 |
| script | 2-84 |

| | |
|--|----------------------------|
| SEC | 3-178 |
| Secrecy | 4-40 |
| Secrets | 2-79 |
| Secure Channel | 4-26-27 |
| Secure Coding | 3-144 |
| Secure Development Practices | 3-142-144 |
| Secure Hash Algorithm (SHA) | 4-30, 2-88 |
| Secure Hash Standard (SHS) | 4-30 |
| Secure Hashing Algorithm | 4-75 |
| Secure Key Exchange Mechanism (SKEME) | 4-96 |
| Secure Shell (SSH) | 1-85 |
| Hardening | 6-77 |
| Key Management | 6-79 |
| MFA | 6-78 |
| Secure Socket Layer (SSL) | 4-120 |
| Secure Sockets Layer (SSL) | 5-165 |
| Security and Privacy Frameworks | 1-142 |
| Security Associations | 4-96 |
| Security Audit | 3-8 |
| Security Content Automation Protocol (SCAP) | 6-84-85 |
| Security Development Lifecycle (SDL) | 3-27 |
| Security Frameworks | 2-109-110 |
| Other | 2-137 |
| Summary | 2-139 |
| Security Incident Response Simulations (SIRS) | 6-198 |
| Security Information and Event Management (SIEM) | 3-185-186 |
| Security Information Event Mangement (SIEM) | 5-239 |
| Security Orchestration Automated Response (SOAR) | 5-239 |
| Segmentation | 1-45, book148-49 |
| Segmentation → Network → Design | |
| Segmentation Fault | 3-104 |
| SELinux | 6-68-69 |
| Sensitive Data | 2-159 |
| Separation of Duties | 2-62 |
| Server Message Block (SMB) | 3-29, 5-88, 3-89-91, 5-162 |
| Serverless | |
| Security | 1-157-159 |
| Serverless Computing | 1-130 |
| Service Level Agreements (SLAs) | 1-139 |
| Session | 1-85 |
| Hacking | 3-152 |
| Protection | 3-153 |
| Tracking | 3-151-153 |
| SHA | 2-88 |
| SHA256 | 2-84, 2-88 |
| SHA512 | 2-84, 2-88 |
| Shadow Brokers | 3-29 |
| Shared Security Models | 1-138-140 |
| Side-channel attack | 1-207 |
| SIFT Workstation | 3-216-217 |
| Sigma | 3-187-190 |
| Conversion | 3-189 |
| Format | 3-188 |
| Orchestration | 3-191 |

SEC401 – Security Essentials Bootcamp Style

| | |
|---|-----------------|
| Sharing | 3-190 |
| Signal to Noise Ratio (SNR) | 1-211-212 |
| Signature Analysis | 4-151 |
| Rules and Signature Criteria | 4-152 |
| Simultaneous Authentication of Equals (SAE) . | 1-202-203 |
| Single Sign-On (SSO) | 2-57 |
| OAuth 2.0 | 2-57 |
| SAML 2.0 | 2-59 |
| Sliver | 3-68 |
| Sniffer | 1-101-104 |
| BetterCAP | 1-102 |
| Kismet | 1-102 |
| Snort | 1-102 |
| tcpdump | 1-102 |
| Wireshark | 1-102 |
| Sniffing | 1-55, 1-101-104 |
| Snort | 4-163 |
| Advanced Rules | 4-167 |
| Rule Flexibility | 4-164 |
| Simple Rules | 4-166 |
| Writing Rules | 4-165 |
| SOC 2 | 2-137 |
| Software Defined Networking (SDN) | 1-131 |
| Software Defined Networking (SDN) → Network | |
| Software-as-a-Service (SaaS) | 1-129 |
| Software Development Lifecycle (SDLC) | 3-142 |
| SolarWindws | 2-125 |
| Spanning Tree Protocol (STP) | 1-38 |
| Splunk | 3-186 |
| Spoofing | 1-62 |
| Spyware | 3-119 |
| SQL Injection | 3-107-109 |
| SQL Server | 5-164 |
| SSH → Secure Shell (SSH) | |
| SSL | 3-137-138 |
| SSL VPN | 4-97-98 |
| Starefull Firewall | 4-142-143 |
| State | 3-151 |
| Stateful Filtering | 4-140 |
| Stateless Packet Filter | 4-141 |
| Steganography | 4-39 |
| Detecting | 4-48 |
| How it works | 4-43 |
| Types | 4-44 |
| File generation | 4-47 |
| Injection | 4-45 |
| Substitution | 4-46 |
| STP Manipulation → Switch → Attacks | |
| Subnets | 1-150 |
| Subscriber | 2-51 |
| Substitution | 4-16 |
| Arbitrary | 4-20 |
| Rotation | 4-18 |
| Superuser | 2-68 |
| Supplicant | 1-46 |
| Swatch | 3-179 |
| Switch | 1-29 |

| | |
|---|---------|
| Attacks | |
| CDP Information Disclosure | 1-36 |
| DHCP Manipulation | 1-36 |
| MAC Flooding | 1-36 |
| STP Manipulation | 1-36 |
| VLAN Hopping | 1-36 |
| Symmetric Key Cryptography | 4-25 |
| Symmetric stream cipher | 4-13 |
| SYN Flooding | 2-14 |
| Sysinternals | 5-258 |
| Syslog | 3-168 |
| syslog-ng | 3-178 |
| System Access Control List (SACL) | 5-287 |
| Systems Security Layer | 2-21-22 |

T

| | |
|--|------------------|
| Tactics | 2-133 |
| Tactics → Threat Enumeration | |
| TCP → Network Protocol → Transmission Control Protocol (TCP) | |
| TCP/IP | 1-63-65 |
| Communication | 1-65 |
| Layer 4 (Application) | 1-63-65 |
| Layer 4 (Internet (IP)) | 1-63-65 |
| Layer 4 (Network) | 1-63-65 |
| Layer 43(Transport (TCP)) | 1-63-65 |
| Techniques → Threat Enumeration | |
| Temporal Key Integrity Protocol (TKIP) | 1-195 |
| Terraform | 6-139-141, 6-191 |
| Lifecycle | 6-140-141 |
| Security | 6-142 |
| Testing | 3-142 |
| The Birthday Attack | 4-78 |
| Thin Client | 5-182-183 |
| Third-Party Risk Mangement | 2-178 |
| Threat | 2-7 |
| Threat Agents | 1-32 |
| Advanced Persistent Threat (APT) | 1-32 |
| Nation State Actors | 1-32 |
| Opportunistic Attacker | 1-32 |
| Organized Cybercrime | 1-32 |
| Threat Enumeration | 1-31 |
| Procedures | 1-31 |
| Tactics | 1-31 |
| Techniques | 1-31 |
| TTP | 1-31, 1-32 |
| Threat Hunting | 3-236 |
| Threat Intelligence | 1-31 |
| Threat Intelligence (IT) | 3-213 |
| Tiered Architecture | 1-50 |
| Time to Live (TTL) | 1-67 |
| Timing attack | 1-207 |
| TLS | 3-137-138 |
| Tokenization | 6-194 |
| Topologies | |
| Logical | 1-41 |
| Physical | 1-41 |

SEC401 – Security Essentials Bootcamp Style

| | |
|--------------------------------------|--------------|
| Tractable Problems | 4-57-58 |
| Transport Layer Security (TLS) | 4-120, 5-165 |
| Key Management | 6-79 |
| Transposition | 4-22 |
| Trapdoor function | 4-29 |
| Trojan | 3-117 |
| Trust | 1-48 |
| Trust Boundary | 3-157, 3-159 |
| Trusted Platform Module (TPM) | 5-107-114 |
| Options | 5-111-112 |
| TTL → Time to Live (TTL) | |
| TTP | 3-213 |
| TTP → Threat Enumeration | |
| Two-Way Transitive Trusts | 5-33 |
| Type of Service | 1-67 |

U

| | |
|---|-----------|
| UDP → Network Protocol → User Datagram Protocol (UDP) | |
| Unified Extensible Firmware Interface (UEFI) .. | 5-115-116 |
| Universal Naming Convention (UNC) | 5-91 |
| User Activity Monitoring (UAM) | 2-176 |
| User Credential Theft | 2-201 |

V

| | |
|---|-------------------------------|
| Validation | 2-52 |
| Valuable Data → Network → Know Thy Network | |
| Verification | 2-52 |
| Verifier | 2-55 |
| Virtual Desktop Infrastructure (VDI) | 5-66 |
| Virtual LAN (VLAN) → Network → Security | |
| Virtual Local Area Network (VLAN) .. | 2-18, 2-35, 1-38 |
| Virtual Machine (VM) | 1-111-114 |
| Virtual Private Cloud (VPC) | 1-148 |
| Virtual Private Network (VPN) | 4-86 |
| Breakdown | 4-88 |
| Flexibility | 4-87 |
| Security Implications | 4-99 |
| SSL | 4-97-98 |
| Types | 4-89 |
| Virtualization | 1-44, 1-111-122, 1-124, 1-163 |
| Defense | 1-122 |
| Risk | |
| Hypervisor | 1-120 |
| Isolation Violation | 1-121 |
| Security | 1-116 |
| Isolation | 1-117 |
| Malware and Forensic Analyses | 1-119 |
| Virtual Desktop Infrastructure (VID) | 1-118 |
| Virus | 3-115-116 |
| VLAN Hopping → Switch → Attacks | |
| VPC Peering | 1-156 |
| Vulnerability | 2-7, 3-8 |
| Assessment | 3-8-10 |

| | |
|---|------|
| Assessment Framework | |
| Step 1: Engagement Planning | 3-14 |
| Step 2: Intelligence and Threat Modeling .. | 3-15 |
| Step 3: Discovery | 3-16 |
| Step 4: Scanning | 3-17 |
| Step 5: Valication | 3-18 |
| Step 6: Remediation | 3-19 |
| Step 7: Reporting | 3-20 |
| Steps | 3-13 |
| Management | 3-8 |
| Risk | 3-22 |
| Vulnerability Assessments | 3-3 |
| Need at Scale | 3-6 |
| Vulnerability Identification | 3-55 |
| Vulnerability | |
| Assessment Framework | |
| Modules | 3-12 |
| Criticality | 3-22 |
| Vulnreability | |
| Assessment Framework | 3-11 |

W

| | |
|--------------------------------------|---------------|
| WannaCry | 3-29 |
| Web App | |
| Summary | 3-160 |
| Web Application | 1-47 |
| Web Application Firewall (WAF) | 2-27, 3-156 |
| Web Communication Basics | 3-132-133 |
| Who | 1-31, 32 |
| Wi-Fi Alliance | 1-172, 1-192 |
| Wi-Fi Protected Access (WPA) | 1-192-195 |
| Version 2 (WPA2) | 1-197-199 |
| version 3 (WPA3) | 1-200-202 |
| Attacks | 1-205 |
| Windows | |
| Active Directory | 5-24 |
| Authentication Protocols | 5-25-29 |
| Domain Controller | 5-24 |
| Forests and Trusts | 5-32, 5-34-35 |
| Group Policy | 5-25, 5-37-39 |
| Registry | 5-25 |
| Active Directory (AD) | |
| Accounts and Group | 5-85 |
| AGULP | 5-83-84 |
| BitLocker Key | 5-114 |
| Domain Admins | 5-86 |
| Domain Local | 5-87 |
| Enterprise Admins | 5-86 |
| Groups | 5-85-87 |
| Permissions | 5-99-100 |
| BitLocker | 5-107-116 |
| Emergency Recovery | 5-113 |
| UEFI Secure Boot | 5-115 |
| CMD | |
| Tools | 5-259-263 |
| Debugger | 5-106 |
| Firewall | 5-166-173 |

SEC401 – Security Essentials Bootcamp Style

| | | | |
|---|------------|--|------------------|
| IPsec | 5-175-178 | Security Configuration and Analysis (SCA) tool | 5-126-127, 5-130 |
| Mutual Authenticaiton | 5-175 | Security Templates | 5-122-125 |
| Local Accounts | | United States Government Configuration Base- | |
| Manage | 5-18 | line (USGCB) | 5-125 |
| Logging | | User Account Control (UAC) | 5-158-159 |
| Audit Policies | 5-283 | Windows Sandbox for Malware Isolation | 5-160- |
| Configuration | 5-281 | 161 | |
| Security Event IDs | 5-285 | Shared Folder Permissions | 5-88-90 |
| Security Events | 5-283-285 | Hidden and Administrative | 5-91-92 |
| Size and Wrapping | 5-290-291 | Subsystem for Linux (WSL) | 5-267-269 |
| What should be logged? | 5-292-293 | Summary | 5-40-41 |
| Network Configuration Tools | 5-265 | winreg | 5-96-97 |
| PowerShell | 5-252-257 | Workgroups | 5-14-15 |
| Core | 5-254-255 | Benefits | 5-16 |
| Examples | 5-256 | Drawbacks | 5-17 |
| Just Enough Admin (JEA) | 5-253 | More Perfect | 5-22 |
| Network Configuration | 5-266 | Windows Access Controls | 5-71-72 |
| Transcription Logging | 5-253 | Summary | 5-117 |
| Privileges | 5-101-106 | Windows as a Service | 5-44 |
| Backup and Restore | 5-105 | Autopilot | 5-63-65 |
| Debug | 5-106 | Azure Virtual Desktop | 5-66 |
| Take Ownership | 5-104 | End of Support | 5-44 |
| Registry | 5-95 | Fixed Lifecycle Policy | 5-46 |
| Permissions | 5-98 | Modern Lifecycle Policy | 5-47 |
| Remote Registry Service | 5-96-97 | Servicing Channels | 5-48-51 |
| Remote Assistance | 5-184-185 | Configuration | 5-54-55 |
| Remote Desktop | 5-184 | Long-Term | 5-56 |
| Remote Desktop Protocol (RDP) | 5-187-190 | Rings | 5-53 |
| Remote Desktop Services (RDS) | 5-180-181 | Updates | 5-52 |
| Best Practivecs | 5-189 | Windows Insider Program | 5-56-57 |
| Security Access Token (SAT) | 5-21, 5-27 | Summary | 5-70 |
| Security ID Numbers (SID) | 5-19 | Updates | 5-48-50 |
| Security Policy Enforcement | | Windows Server Update Service (WSUS) . | 5-60-62 |
| Account Lockout | 5-142 | Windows Update | 5-58-59 |
| Anonymous Access | 5-142-144 | Windows Event Collector (WEC) | 3-169 |
| AppLocker | 5-154-155 | Windows Event Forwarding (WEF) | 3-169 |
| Center for Internet Security (CIS) | 5-125 | Windows Management Instrumentation (WMI) . | 5-264 |
| Controlled Folder Access | 5-156-157 | Windows Operating Systems | 5-5 |
| Credential Guard | 5-148-149 | Client | 5-6-7 |
| Defense Information Systems Agency Security | | Embedded | 5-11-12 |
| Technical Implementation Guides (DISA | | IoT | 5-11-12 |
| STIG) | 5-125 | Server | 5-8-9 |
| Domain Group Policy Objects | 5-134 | Roles | 5-10 |
| Federal Desktop Cor Configuration (FDCC) . | 5-125 | Windows Subsystem for Linux (WSL) | 6-13 |
| Firewall | 5-166-173 | Windows | |
| GPO Settings Checklist | 5-136-139 | Task Scheduler | 5-270 |
| Group Policy Management Console (GPMC) | | Winlogbeat | 3-178 |
| 5-135 | | Wired Equivalent Privacy (WEP) | 1-188-191 |
| Guest Account | 5-153 | Wireless | 1-166-170 |
| Kerberos and NTLM | 5-145-147 | Pervasiveness | 1-169-170 |
| Key Protocols | 5-162 | Wireless Intrusion Detection System (WIDS) . | 4-170 |
| Local Group Policy Objects | 5-129-133 | Wireless Local Area Network (WLAN) .. | 1-167, 1-172 |
| Microsoft Managment Console (MMC) .. | 5-123 | WMIC.exe | 5-264 |
| Passwords | 5-140-141 | Wookbook | 5-238-239 |
| Protect Admin Accounts | 5-150-152 | Workspace | 5-238-239 |
| REGEDIT.EXE | 5-132 | Worm | 3-115-116 |
| SECEDIT.EXE | 5-128 | | |

SEC401 – Security Essentials Bootcamp Style

X

Z

| | |
|------------|-------|
| X509 | 4-118 |
| XOR | 4-17 |

Y

| | |
|---------------|------|
| YubiKey | 2-80 |
|---------------|------|

| | |
|---|-----------|
| Zero Power High Availability (ZPHA) | 4-175 |
| Zero-Trust | 2-39-44 |
| Adaptive Authentication | 2-109 |
| Log Inspection | 2-44 |
| Variable Trust | 2-42-43 |
| Zeus Trojan | 2-201 |
| Zigbee Alliance | 1-222-223 |
| Zitmo | 2-201 |