Cybersecurity Cheatsheet

Essential operations for protecting systems and data from cyber threats

This cheatsheet provides a quick reference to fundamental cybersecurity concepts, tools, and best practices, ideal for beginners and IT professionals to effectively secure systems and defend against cyber attacks.

Threat Identification

Recognize and analyze security threats

Security Assessment

Evaluate system vulnerabilities

System Hardening

Secure systems and applications

Incident Response

Handle security breaches effectively

Monitoring & Detection

Continuously watch for threats

System Security Fundamentals

User Account Management

Control access to systems and data.

```
# Add a new user
sudo adduser username
# Set password policy
sudo passwd -l username
# Grant sudo privileges
sudo usermod -aG sudo username
# View user information
id username
# List all users
cat /etc/passwd
```

File Permissions & Security

Configure secure file and directory access.

```
# Change file permissions (read, write, execute)
chmod 644 file.txt
# Change ownership
chown user:group file.txt
# Set permissions recursively
chmod -R 755 directory/
# View file permissions
ls -la
```

Network Security Configuration

Secure network connections and services.

```
# Configure firewall (UFW)
sudo ufw enable
sudo ufw allow 22/tcp
sudo ufw deny 23/tcp
# Check open ports
netstat -tuln
sudo ss -tuln
```

System Updates & Patches

Keep systems updated with latest security patches.

```
# Update package lists (Ubuntu/Debian)
sudo apt update
# Upgrade all packages
sudo apt upgrade
# Automatic security updates
sudo apt install unattended-upgrades
```

Service Management

Control and monitor system services.

```
# Stop unnecessary services
sudo systemctl stop service_name
sudo systemctl disable service_name
# Check service status
sudo systemctl status ssh
# View running services
systemctl list-units --type=service --state=running
```

Log Monitoring

Monitor system logs for security events.

```
# View authentication logs
sudo tail -f /var/log/auth.log
# Check system logs
sudo journalctl -f
# Search for failed logins
grep "Failed password" /var/log/auth.log
```

Password Security & Authentication

Implement strong authentication mechanisms and password policies.

01

Strong Password Creation

Generate and manage secure passwords following best practices.

```
# Generate strong password
openssl rand -base64 32
# Password strength requirements:
# - Minimum 12 characters
# - Mix of uppercase, lowercase, numbers, symbols
# - No dictionary words or personal info
# - Unique for each account
```

02

Multi-Factor Authentication (MFA)

Add additional authentication layers beyond passwords.

```
# Install Google Authenticator
sudo apt install libpam-google-authenticator
# Configure MFA for SSH
google-authenticator
# Enable in SSH config
sudo nano /etc/pam.d/sshd
# Add: auth required pam_google_authenticator.so
```

03

Password Management

Use password managers and secure storage practices.

```
# Install password manager (KeePassXC)
sudo apt install keepassxc
# Best practices:
# - Use unique passwords for each service
# - Enable auto-lock features
# - Regular password rotation for critical accounts
# - Secure backup of password database
```

Network Security & Monitoring

Port Scanning & Discovery

Identify open ports and running services.

```
# Basic port scan with Nmap
nmap -sT target_ip
# Service version detection
nmap -sV target_ip
# Comprehensive scan
nmap -A target_ip
# Scan specific ports
nmap -p 22,80,443 target_ip
# Scan range of IPs
nmap 192.168.1.1-254
```

Network Traffic Analysis

Monitor and analyze network communications.

```
# Capture packets with tcpdump
sudo tcpdump -i eth0
# Save to file
sudo tcpdump -w capture.pcap
# Filter specific traffic
sudo tcpdump host 192.168.1.1
# Monitor specific port
sudo tcpdump port 80
```

Firewall Configuration

Control incoming and outgoing network traffic.

```
# UFW (Uncomplicated Firewall)
sudo ufw status
sudo ufw allow ssh
sudo ufw deny 23
# iptables rules
sudo iptables -L
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

SSL/TLS Certificate Management

Implement secure communications with encryption.

```
# Generate self-signed certificate
openssl req -x509 -newkey rsa:4096 -keyout key.pem -
out cert.pem -days 365
# Check certificate details
openssl x509 -in cert.pem -text -noout
# Test SSL connection
openssl s_client -connect example.com:443
```

Vulnerability Assessment

System Vulnerability Scanning

Identify security weaknesses in systems and applications.

```
# Install Nessus scanner
# Download from tenable.com
sudo dpkg -i Nessus-X.X.X-ubuntu1404_amd64.deb
# Start Nessus service
sudo systemctl start nessusd
# Access web interface at https://localhost:8834

# Using OpenVAS (free alternative)
sudo apt install openvas
sudo gvm-setup
```

Web Application Security Testing

Test web applications for common vulnerabilities.

```
# Using Nikto web scanner
nikto -h http://target.com
# Directory enumeration
dirb http://target.com
# SQL injection testing
sqlmap -u "http://target.com/page.php?id=1" --dbs
```

Security Auditing Tools

Comprehensive security assessment utilities.

```
# Lynis security audit
sudo apt install lynis
sudo lynis audit system
# Check for rootkits
sudo apt install chkrootkit
sudo chkrootkit
# File integrity monitoring
sudo apt install aide
sudo aideinit
```

Configuration Security

Verify secure system and application configurations.

```
# SSH security check
ssh-audit target_ip
# SSL configuration test
testssl.sh https://target.com
# Check file permissions on sensitive files
ls -la /etc/shadow /etc/passwd /etc/group
```

Incident Response & Forensics

Log Analysis & Investigation

Analyze system logs to identify security incidents.

```
# Search for suspicious activities
grep -i "failed\|error\|denied" /var/log/auth.log
# Count failed login attempts
grep "Failed password" /var/log/auth.log | wc -l
# Find unique IP addresses in logs
awk '/Failed password/ {print $11}' /var/log/auth.log |
sort | uniq -c
# Monitor live log activity
tail -f /var/log/syslog
```

Network Forensics

Investigate network-based security incidents.

```
# Analyze network traffic with Wireshark
# Install: sudo apt install wireshark
# Capture live traffic
sudo wireshark
# Analyze captured files
wireshark capture.pcap
# Command-line analysis with tshark
tshark -r capture.pcap -Y "http.request"
```

System Forensics

Preserve and analyze digital evidence.

```
# Create disk image
sudo dd if=/dev/sda of=/mnt/evidence/disk_image.dd
bs=4096
# Calculate file hashes for integrity
md5sum important_file.txt
sha256sum important_file.txt
# Search for specific file content
grep -r "password" /home/user/
# List recently modified files
find /home -mtime -7 -type f
```

Incident Documentation

Properly document security incidents for analysis.

```
# Incident response checklist:
# 1. Isolate affected systems
# 2. Preserve evidence
# 3. Document timeline of events
# 4. Identify attack vectors
# 5. Assess damage and data exposure
# 6. Implement containment measures
# 7. Plan recovery procedures
```

Threat Intelligence

Gather and analyze information about current and emerging security threats.

OSINT (Open Source Intelligence)

Collect publicly available threat information.

```
# Search for domain information
whois example.com
# DNS lookup
dig example.com
nslookup example.com
# Find subdomains
sublist3r -d example.com
# Check reputation databases
# VirusTotal, URLVoid, AbuseIPDB
```

Threat Hunting Tools

Proactively search for threats in your environment.

```
# IOC (Indicators of Compromise) search
grep -r "suspicious_hash" /var/log/
# Check for malicious IPs
grep "192.168.1.100" /var/log/auth.log
# File hash comparison
find /tmp -type f -exec sha256sum {} \;
```

Threat Feeds & Intelligence

Stay updated with latest threat information.

```
# Popular threat intelligence sources:
# - MISP (Malware Information Sharing Platform)
# - STIX/TAXII feeds
# - Commercial feeds (CrowdStrike, FireEye)
# - Government feeds (US-CERT, CISA)

# Example: Check IP against threat feeds
curl -s "https://api.threatintel.com/check?ip=1.2.3.4"
```

Threat Modeling

Identify and assess potential security threats.

```
# STRIDE threat model categories:
# - Spoofing (identity)
# - Tampering (data)
# - Repudiation (actions)
# - Information Disclosure
# - Denial of Service
# - Elevation of Privilege
```

Encryption & Data Protection

Implement strong encryption to protect sensitive data.

File & Disk Encryption

Encrypt files and storage devices to protect data at rest.

```
# Encrypt a file with GPG
gpg -c sensitive_file.txt
# Decrypt file
gpg sensitive_file.txt.gpg
# Full disk encryption with LUKS
sudo cryptsetup luksFormat /dev/sdb
sudo cryptsetup luksOpen /dev/sdb encrypted_drive
```

Network Encryption

Secure network communications with encryption protocols.

```
# Generate SSH keys
ssh-keygen -t rsa -b 4096
# Set up SSH key authentication
ssh-copy-id user@server
# VPN setup with OpenVPN
sudo apt install openvpn
sudo openvpn --config client.ovpn
```

Certificate Management

Manage digital certificates for secure communications.

```
# Create certificate authority
openssl genrsa -out ca-key.pem 4096
openssl req -new -x509 -key ca-key.pem -out ca.pem
# Generate server certificate
openssl genrsa -out server-key.pem 4096
openssl req -new -key server-key.pem -out server.csr
# Sign certificate with CA
openssl x509 -req -in server.csr -CA ca.pem -CAkey ca-
key.pem -out server.pem
```

Data Loss Prevention

Prevent unauthorized data exfiltration and leakage.

```
# Monitor file access
sudo apt install auditd
# Configure audit rules
sudo auditctl -w /etc/passwd -p wa -k passwd_changes
# Search audit logs
sudo ausearch -k passwd_changes
```

Security Automation & Orchestration

Automate security tasks and response procedures.

Security Scanning Automation

Schedule regular security scans and assessments.

```
# Automated Nmap scanning script
#!/bin/bash
DATE=$(date +%Y-%m-%d)
nmap -sS -O 192.168.1.0/24 > /var/log/nmap-scan-$DATE.log
# Schedule with cron
0 2 * * * /path/to/security-scan.sh

# Automated vulnerability scanning
#!/bin/bash
nikto -h $1 -o /var/log/nikto-$(date +%Y%m%d).txt
```

Incident Response Automation

Automate initial incident response procedures.

```
# Automated threat response script
#!/bin/bash
SUSPICIOUS_IP=$1
# Block IP at firewall
sudo ufw deny from $SUSPICIOUS_IP
# Log the action
echo "$(date): Blocked suspicious IP $SUSPICIOUS_IP" >> /var/log/security-actions.log
# Send alert
echo "Blocked suspicious IP: $SUSPICIOUS_IP" | mail -s "IP Blocked" security@company.com
```

Log Monitoring Scripts

Automate log analysis and alerting.

```
# Failed login monitoring
#!/bin/bash
FAILED_LOGINS=$(grep "Failed password" /var/log/auth.log | tail -n 100 | wc -l)
if [ $FAILED_LOGINS -gt 10 ]; then
    echo "High number of failed logins detected: $FAILED_LOGINS" | mail -s "Security Alert" admin@company.com
fi
```

Configuration Management

Maintain secure system configurations.

```
# Ansible security playbook example
---
- name: Harden SSH configuration
 hosts: all
 tasks:
 - name: Disable root login
 lineinfile:
 path: /etc/ssh/sshd_config
 line: 'PermitRootLogin no'
 - name: Restart SSH service
 service:
 name: sshd
 state: restarted
```

Compliance & Risk Management

Security Policy Implementation

Implement and maintain security policies and procedures.

```
# Password policy enforcement (PAM)
sudo nano /etc/pam.d/common-password
# Add: password required pam_pwquality.so minlen=12
# Account lockout policy
sudo nano /etc/pam.d/common-auth
# Add: auth required pam_tally2.so deny=5
unlock_time=900
```

Risk Assessment Tools

Evaluate and quantify security risks.

```
# Risk matrix calculation:
# Risk = Likelihood × Impact
# Low (1-3), Medium (4-6), High (7-9)

# Vulnerability prioritization
# CVSS Score calculation
# Base Score = Impact × Exploitability
```

Audit & Compliance Checking

Verify compliance with security standards and regulations.

```
# CIS (Center for Internet Security) benchmark tools
sudo apt install cis-cat-lite
# Run CIS assessment
./CIS-CAT.sh -a -s
```

Documentation & Reporting

Maintain proper security documentation and reporting.

```
# Security incident report template:
# - Date and time of incident
# - Systems affected
# - Attack vectors identified
# - Data compromised
# - Actions taken
# - Lessons learned
# - Remediation plan
```

Security Tools Installation

Install and configure essential cybersecurity tools.

Package Managers

Install tools using system package managers.

```
# Ubuntu/Debian
sudo apt update
sudo apt install nmap wireshark
tcpdump
# CentOS/RHEL
sudo yum install nmap
wireshark tcpdump
# Arch Linux
sudo pacman -S nmap
wireshark-qt tcpdump
```

Security Distributions

Specialized Linux distributions for security professionals.

```
# Kali Linux - Penetration
testing
# Download from:
https://www.kali.org/
# Parrot Security OS
# Download from:
https://www.parrotsec.org/
# BlackArch Linux
# Download from:
https://blackarch.org/
```

Tool Verification

Verify tool installation and basic configuration.

```
# Check tool versions
nmap --version
wireshark --version
# Basic functionality test
nmap 127.0.0.1
# Configure tool paths
export
PATH=$PATH:/opt/tools/bin
echo 'export
PATH=$PATH:/opt/tools/bin' >>
~/.bashrc
```

Security Configuration Best Practices

Apply security hardening configurations across systems and applications.

System Hardening

Secure operating system configurations.

```
# Disable unnecessary services
sudo systemctl disable telnet
sudo systemctl disable ftp
# Set secure file permissions
sudo chmod 600 /etc/ssh/sshd_config
sudo chmod 644 /etc/passwd
# Configure system limits
echo "* hard core 0" >> /etc/security/limits.conf
```

Network Security Settings

Implement secure network configurations.

```
# Disable IP forwarding (if not a router)
echo "net.ipv4.ip_forward = 0" >> /etc/sysctl.conf
# Enable SYN cookies
echo "net.ipv4.tcp_syncookies = 1" >> /etc/sysctl.conf
# Disable ICMP redirects
echo "net.ipv4.conf.all.accept_redirects = 0" >>
/etc/sysctl.conf
```

Application Security

Secure application and service configurations.

```
# Apache security headers
Header always set X-Content-Type-Options nosniff
Header always set X-Frame-Options DENY
Header always set X-XSS-Protection "1; mode=block"
# Nginx security configuration
add_header X-Frame-Options DENY;
add_header X-Content-Type-Options nosniff;
```

Backup & Recovery Security

Implement secure backup and disaster recovery procedures.

```
# Encrypted backups with rsync
rsync -av --password-file=/etc/rsyncd.secrets /data/
backup@server::backups/
# Test backup integrity
tar -tzf backup.tar.gz > /dev/null && echo "Backup OK"
# Automated backup verification
#!/bin/bash
find /backups -name "*.tar.gz" -exec tar -tzf {} \; >
/dev/null
```

Advanced Security Techniques

Implement advanced security measures and defense strategies.

Intrusion Detection Systems

Deploy and configure IDS/IPS for threat detection.

```
# Install Suricata IDS
sudo apt install suricata
# Configure rules
sudo nano /etc/suricata/suricata.yaml
# Update rules
sudo suricata-update
# Start Suricata
sudo systemctl start suricata
# Monitor alerts
tail -f /var/log/suricata/fast.log
```

Security Information and Event Management (SIEM)

Centralize and analyze security logs and events.

```
# ELK Stack (Elasticsearch, Logstash, Kibana)
# Install Elasticsearch
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
sudo apt update && sudo apt install elasticsearch
```

Security Awareness & Training

Social Engineering Defense

Recognize and prevent social engineering attacks.

```
# Phishing identification techniques:
# - Check sender email carefully
# - Verify links before clicking (hover)
# - Look for spelling/grammar errors
# - Be suspicious of urgent requests
# - Verify requests through separate channel

# Email security headers to check:
# SPF, DKIM, DMARC records
```

Security Culture Development

Build a security-aware organizational culture.

```
# Security awareness program elements:
# - Regular training sessions
# - Phishing simulation tests
# - Security policy updates
# - Incident reporting procedures
# - Recognition for good security practices

# Metrics to track:
# - Training completion rates
# - Phishing simulation click rates
# - Security incident reporting
```

Reference: This cheatsheet covers essential cybersecurity commands, tools, and best practices for protecting systems and data from modern cyber threats in both personal and enterprise environments.