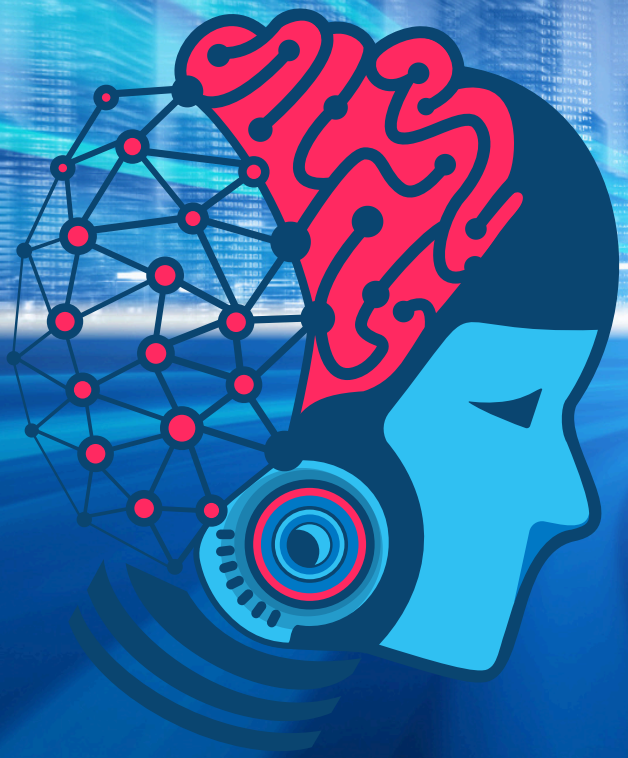
200 ChatGPT Prompts For Cybersecurity Pros

Red Team | Blue Team | Awareness | Threat Intel & more



Master AI for Security Operations

PORT::ZERO
CYBER SOLUTIONS
Protect Against Cyber Threats

How To Use This Guide

- Copy and paste these prompts to turn ChatGPT into your AI cybersecurity assistant.
- Utilize the prompts for real-world tasks like CTF prep, lab creation, policy preparation, cyber awareness training, etc.
- Prompts may require refinement. Avoid disclosing sensitive data.

Pro Tip:
Chain prompts together for deeper analysis: Start with detection logic, follow up with '*write alert logic for this*,' finish with '*draft incident response steps*'.

Table of Contents

Blue Team Defense & Detection

Windows Endpoint Triage Checklist

Act as a Tier 1 SOC analyst. Create a Windows endpoint triage checklist for detecting signs of malware infection, including memory, process, and service checks.

Detecting Lateral Movement

Generate a detection strategy to identify lateral movement techniques in a small enterprise network using Windows Event Logs and Sysmon.

Blue Team Defense & Detection

Suspicious PowerShell Monitoring

Write a Wazuh rule or Sigma signature that detects encoded PowerShell command execution on a monitored Windows host.

DNS Tunneling Detection

Describe how to detect DNS tunneling in outbound traffic logs using frequency analysis and unusual subdomain patterns.

Blue Team Defense & Detection

Host Isolation SOP

Create a Standard Operating Procedure (SOP) for isolating a compromised host in a hybrid network environment using EDR or manual intervention.

USB Device Alerting

Draft an alert for a SIEM to detect unauthorized USB device insertions on critical endpoints, including alert thresholds and response actions.

Blue Team Defense & Detection

Brute Force Login Detection

Develop a correlation rule for identifying brute force login attempts in Windows Event Logs. Set parameters for time range, user lockouts, and alert escalation.

Malware Sandbox Integration

Guide me on integrating a malware sandbox (like Cuckoo or ANY.RUN) into a blue team workflow for dynamic analysis and IOC extraction.

Blue Team Defense & Detection

Firewall Log Review Checklist

Create a weekly checklist for manually reviewing firewall logs, focusing on identifying unusual outbound connections, port scanning, or blocked access attempts.

Ransomware Behavior Signatures

List key behavioral indicators of ransomware in system logs or EDR telemetry. Include file renaming patterns, mass file access, and registry edits.

Blue Team Defense & Detection

Detecting Suspicious Scheduled Tasks

Write a detection rule or workflow to identify suspicious scheduled tasks or new entries in the Windows Task Scheduler created outside of IT-approved tools.

Credential Dumping Hunt

Generate a threat-hunting plan to detect Mimikatz or other credential-dumping tools using Sysmon logs, memory analysis, and PowerShell telemetry.

Blue Team Defense & Detection

Beaconing Detection Logic

Explain how to detect C2 beaconing behavior in outbound traffic logs. Include patterns like jittered intervals, small repetitive packets, and DGA domains.

Privileged Account Abuse Monitoring

Design an alerting strategy for detecting unusual activity by privileged accounts, such as off-hours logins, access to HR folders, or bulk file deletions.

Blue Team Defense & Detection

Insecure RDP Exposure Hunt

Guide me through scanning internal and external networks for insecure RDP configurations, and write a SIEM rule to alert on unencrypted RDP traffic.

Detection Gap Analysis

Create a checklist for performing a detection gap analysis in an EDR or SIEM platform. Include categories for MITRE coverage, visibility, and false negatives.

Blue Team Defense & Detection

Anomoly-Based Detection Baseline

Draft a prompt to baseline normal user logon activity in a small business AD environment so ChatGPT can later help detect logon anomalies.

Removable Media Policy Enforcement

Write a detection rule for Wazuh or a PowerShell script to alert when a USB device is mounted on a system outside of approved hours.

Blue Team Defense & Detection

Local Admin Enumeration

Create a detection strategy that identifies systems where domain users have been added to local admin groups without a ticket or approval trail.

Deceptive File Execution Traps

Explain how to use decoy files (canary files) to detect unauthorized file access attempts on sensitive shared folders. Include SIEM integration steps.

Red Team & Offensive Security

Phishing Pretext Creation

Generate a phishing email targeting employees of a tech startup. The pretext should involve fake HR onboarding documents and include a believable subject line and email body.

Initial Access Simulation

Simulate an initial access scenario using a Word document with macros. Include the command, payload type, and evasion tactic.

Red Team & Offensive Security

Payload Obfuscation Techniques

List five PowerShell obfuscation techniques used to bypass common endpoint detection tools and explain how each works.

C2 Infrastructure Plan

Design a basic command and control (C2) infrastructure setup using Cobalt Strike or Mythic C2 for a red team engagement, including OPSEC tips.

Red Team & Offensive Security

Privilege Escalation Enumeration

Simulate privilege escalation enumeration on a compromised Windows 10/11 machine. List the top five tools and commands used.

Web App Recon Flow

Create a red team recon workflow for targeting a web application. Include steps for subdomain discovery, WAF detection, and endpoint fuzzing.

Red Team & Offensive Security

NTLM Hash Capture Lab

Design a lab in VirtualBox that allows safe capture of NTLM hashes via Responder in a simulated Windows environment. Include network configuration tips.

Active Directory Attack Path

Describe a full attack path from initial compromise to Domain Admin in an AD environment. Include tools and techniques at each phase.

Red Team & Offensive Security

Exfiltration Simulation

Create a scenario where sensitive files are exfiltrated over DNS. Detail how the data is encoded and exfiltrated in chunks using a custom script.

TTP Mapping for Red Team Ops

Map a red team engagement's tools and techniques to MITRE ATT&CK. Include persistence, lateral movement, and exfiltration techniques.

Red Team & Offensive Security

Living Off the Land Simulation

Simulate an attack using only Living off the Land Binaries (LOLBins) on a Windows 10/11 machine. List each binary used for initial access, persistence, and exfiltration.

WebShell Detection Evasion

Write a prompt for generating a stealthy PHP or ASP webshell payload that avoids traditional signatures, then explain how a blue team might still detect it.

Red Team & Offensive Security

Custom Wordlist Generator

Create a prompt that builds a targeted wordlist for password cracking based on a company's social media posts, employee names, and common business terms.

AV Evasion Strategy

Simulate the process of modifying a known payload (e.g. reverse shell) to bypass antivirus detection using encoding, packing, and command obfuscation techniques.

Red Team & Offensive Security

Physical Red Team Recon Workflow

Generate a physical recon plan for assessing a target office's physical security posture before a penetration test. Include pretext development and camera mapping.

Covert Data Exfil via Slack

Simulate an exfiltration method where sensitive data is encoded and sent through a corporate Slack webhook. Include payload and bypass considerations.

Red Team & Offensive Security

Initial Compromise via Excel Macro

Generate an Excel VBA macro payload that executes PowerShell on open. Explain each line of code and suggest an OPSEC-safe delivery method.

Attack Path Mapping in AD

Guide me through identifying a privilege escalation path in Active Directory using BloodHound data. Include the use of shortest path queries and node interpretation.

Red Team & Offensive Security

DNS C2 Tunneling Lab

Design a practice lab for setting up DNS-based C2 using tools like DNScat2 or Iodine. Include attacker/server setup and how to simulate realistic traffic.

Offensive Prompt Chain

Create a 3-step chained prompt sequence that helps automate red team tasks: (1) generate pretext, (2) build payload, (3) identify OPSEC risks.

OSINT & Reconnaissance

Email Enumeration Workflow

Create a workflow to enumerate employee emails from the domain <*insert domain*> using OSINT tools and techniques. Include at least one passive and one active method.

LinkedIn Intelligence Gathering

Act as an OSINT analyst. Guide me step-by-step on how to extract job roles, tech stack hints, and infrastructure clues from a company's public LinkedIn profiles.

OSINT & Reconnaissance

Metadata Extraction Lab

Set up a virtual OSINT lab for extracting metadata from image and document files. Include tools for EXIF analysis and PDF structure review.

Subdomain Discovery Strategy

Generate a list of tools and steps for discovering subdomains of a given target. Include passive enumeration, brute-forcing, and DNS history lookup.

OSINT & Reconnaissance

Google Dorking for Recon

Write 5 custom Google Dork queries to help identify exposed documents, login pages, and misconfigured directories for a target company.

GitHub Leak Hunting

Guide me on how to search GitHub repositories for accidentally leaked credentials or sensitive config files tied to a company domain.

OSINT & Reconnaissance

Social Media Profiling

Generate an OSINT checklist for profiling a target individual using Facebook, Twitter/X, Instagram, and TikTok. Focus on habits, location clues, and device info.

WHOIS & DNS Footprinting

Provide a prompt sequence to gather WHOIS records, DNS zone data, registrar details, and name server relationships for a given domain.

OSINT & Reconnaissance

Dark Web Footprint Discovery

Explain how to use Tor + OSINT tools to discover whether a company's brand or data has been mentioned on known dark web forums.

OSINT Report Template

Create a one-page OSINT report template that summarizes key findings, intel sources, and risk insights for a corporate client.

OSINT & Reconnaissance

Employee Name Pivot via Breach Data

Create a workflow to identify employee usernames and emails by cross-referencing breach data (like HaveIBeenPwned) with LinkedIn information.

Google Maps Recon for Physical Security

Design a reconnaissance workflow using Google Maps, Street View, and satellite imagery to assess a physical site's security controls such as badge readers, entrances, and cameras.

OSINT & Reconnaissance

Maltego Graph Planning

Design a Maltego graph for recon on a target company, starting with the domain and expanding into DNS records, employee data, and linked social accounts.

GitLab & Bitbucket Intelligence

Generate a prompt sequence for discovering exposed repositories or sensitive files in GitLab and Bitbucket using advanced search and dorking techniques.

OSINT & Reconnaissance

Company Tech Stack Fingerprinting

Guide me through fingerprinting a company's tech stack using tools like BuiltWith, Netcraft, and passive DNS to infer providers, frameworks, and potential vulnerabilities.

OSINT Workflow Using Shodan

Create a complete OSINT scan workflow using Shodan to identify publicly exposed assets for a given domain. Include filters for CVEs and outdated services.

OSINT & Reconnaissance

Social Media Geolocation Clues

Explain how to extract geolocation data from Instagram or TikTok content to build a physical movement profile of a target individual.

OSINT Pivoting Plan

You have a domain and a single email address. Guide me through techniques to uncover connected assets, accounts, and organizations.

OSINT & Reconnaissance

Whois Privacy Workaround Techniques

Outline legal OSINT techniques for uncovering useful metadata from domains that use WHOIS privacy protection. Include registrar tracking and certificate transparency logs.

News & Press Release Recon

Use corporate press releases and news sources to identify potential targets, infrastructure changes, or acquisitions that could inform future attack vectors.

Network Security & Tool Mastery

Nmap Scan Breakdown

Break down the function of each flag in this Nmap command: *nmap -sS -sV -T4 -A -p- -Pn 192.168.1.1.* Explain in simple language for a beginner analyst.

Nmap Command Deep Dive

Break down and explain each part of the following Nmap command: *nmap -sS -sV -p- -T4 -Pn -oN fullscan.txt 10.10.10.0/24*. Include what each flag does, the scan behavior, and OPSEC concerns.

Network Security & Tool Mastery

Wireshark Filter Cheat Sheet

Create a Wireshark display filter cheat sheet with 10 useful filters for investigating suspicious network activity on Windows endpoints.

Firewall Ruleset Review Template

Create a 1-page template to audit firewall rules on a perimeter device. Include field for source/destination, ports, protocol, justification, and last verified date.

Network Security & Tool Mastery

tcpdump Quick Guide

Provide a tcpdump command reference for capturing: (1) HTTP traffic, (2) specific IP addresses, and (3) traffic on port 443. Add explanations for each.

Wireshark Packet Analysis Scenario

You are reviewing a Wireshark capture that includes suspicious outbound DNS requests. Guide me on identifying potential data exfiltration behavior and show how to filter using display filters.

Network Security & Tool Mastery

Network Segmentation Plan

Generate a basic network segmentation plan for a small business with finance, HR, and IT departments using VLANs and firewalls.

TCP Handshake Walkthrough

Explain how the TCP three-way handshake works step-by-step. Then, demonstrate how it appears in a Wireshark capture, including typical flags (SYN, ACK, etc.).

Network Security & Tool Mastery

VPN Tunnel Troubleshooting

List common issues that can break or degrade VPN tunnels, and explain how to use network diagnostics tools to troubleshoot each issue.

IDS vs IPS Comparison

Create a table comparing IDS and IPS across the following attributes: detection method, response capability, deployment mode, pros, cons, and real-world use cases.

Network Security & Tool Mastery

Detecting Port Scans

Design a detection rule for identifying TCP SYN scans in firewall or IDS logs. Explain why SYN scans are preferred by attackers.

Packet Crafting Lab

Guide me in building a lab environment to practice packet crafting using tools like Scapy or Hping3. Include install steps, test scenarios, and analysis tips.

Network Security & Tool Mastery

Proxy vs VPN Analysis

Compare proxies and VPNs in terms of encryption, anonymity, threat modeling, and typical use cases. Include a table format if possible.

VPN Protocol Breakdown

Compare OpenVPN, IPSec, WireGuard, and L2TP across speed, encryption strength, setup complexity, mobile support, and use cases.

Network Security & Tool Mastery

Netstat Investigation Workflow

Write a step-by-step guide to investigate suspicious outbound connections using *netstat, nslookup, and whois* from a Windows machine.

Port Scanning Detection Tactics

List 5 detection techniques to identify stealthy port scans (like FIN, NULL, or XMAS scans) on a monitored network. Include log and behavioral indicators.

Network Security & Tool Mastery

Log4j Exploit Detection Logic

Create a Snort or Suricata rule to detect HTTP traffic attempting the Log4Shell (Log4j) exploit. Add an explanation of how it works.

Netcat for Network Troubleshooting

Demonstrate how to use Netcat (nc) for basic port listening, banner grabbing, and file transfer between two systems. Include both client and server commands.

Network Security & Tool Mastery

Firewall Rule Audit Checklist

Build a 10-point checklist for auditing firewall rules in a hybrid network environment, focusing on least privilege, logging, and alerting.

Network Segmentation Audit Checklist

Draft a 10-point checklist for auditing segmentation in an enterprise environment. Focus on VLANs, access control, traffic restrictions, and monitoring placement.

Log Analysis & SIEM/EDR Use

Brute-Force Detection Rule

Write a Sigma rule that detects 5+ failed login attempts followed by a successful login from the same IP address within a 10-minute window on a Windows Server.

Windows Event Log Breakdown

List the top 10 most important Windows Event IDs to monitor for security-related incidents, along with a short description of what each event means.

Log Analysis & SIEM/EDR Use

Failed Logins by Time of Day

Create a Splunk query that visualizes failed login attempts by time of day. Group results by username and source IP.

EDR Alert Analysis Playbook

Develop a step-by-step triage playbook for responding to an EDR alert about suspicious PowerShell activity on a domain-joined workstation.

Log Analysis & SIEM/EDR Use

Linux Syslog Log Hunt

You suspect a malicious user is hiding commands on a Linux server. Write a Linux command sequence to search */var/log* for suspicious *sudo, SSH,* and *cron* activity.

Detecting Data Exfiltration via FTP

Generate a SIEM correlation rule to detect large outbound FTP transfers from internal hosts to unknown external IPs.

Log Analysis & SIEM/EDR Use

Event Log Forwarding Architecture

Design a basic Windows Event Forwarding (WEF) architecture for a small company with 10 workstations and 1 SIEM server.

Unusual User Behavior Detection

You're building a detection rule for a user logging into a workstation they've never used before. Write the logic and threshold that could trigger an alert without causing false positives.

Log Analysis & SIEM/EDR Use

Ransomware IOC Matching

Create a workflow for ingesting threat intel reports and matching IOCs (IPs, hashes, domains) against your organization's current logs.

SIEM False Positive Reduction Plan

Generate a plan to reduce false positives in a SIEM environment without losing valuable visibility. Include examples like whitelist tuning, alert suppression, and behavioral tuning.

Log Analysis & SIEM/EDR Use

MITRE Technique Mapping via Logs

Given a log sample showing PowerShell execution with encoded commands, use MITRE ATT&CK to identify the technique ID, description, and detection method.

Red Team Simulation Detection

Create a detection checklist for simulated attacks using tools like Cobalt Strike or Sliver. What log sources and fields should be monitored to detect beaconing and lateral movement?

Log Analysis & SIEM/EDR Use

SOC Alert Fatigue Analysis

Design a prompt for evaluating SOC alert fatigue by analyzing false positives, ticket resolution time, and analyst workload from log and ticketing data.

Time-Based Attack Correlation

Write a correlation rule for detecting potential staging behavior where a user downloads a ZIP file and accesses an unusual set of internal resources within the next 15 minutes.

Log Analysis & SIEM/EDR Use

Detecting Off-Hours Activity

Build a SIEM rule that alerts on any login attempts or file access during non-business hours. Include logic to suppress known approved jobs or maintenance windows.

USB Device Behavior Baseline

Guide me through establishing a baseline of normal USB usage across an environment and generating a deviation alert using EDR or SIEM logic.

Log Analysis & SIEM/EDR Use

Suspicious Parent-Child Process Chains

List Windows process chains that may indicate malicious activity (e.g. *winword.exe* > *powershell.exe*) and generate a detection logic for spotting them in EDR logs.

Anomaly Detection Using UEBA

Generate a use case for implementing a User and Entity Behavior Analytics (UEBA) model in a SIEM to flag deviations in logon locations, access times, and resource usage.

Log Analysis & SIEM/EDR Use

Shadow IT Detection via Proxy Logs

Create a log analysis workflow for detecting unauthorized or shadow IT tools in proxy/web traffic logs, such as remote desktop software or cloud storage not whitelisted.

Threat Intelligence-Enriched Alerts

Write a logic example that enriches SIEM alerts with threat intelligence feeds (e.g. VirusTotal or AbuseIPDB) to automatically prioritize high-confidence IP matches.

Vulnerabilities & Threat Intel

CVE Breakdown for Execs

Explain <CVE-20XX-XXXXX> to a non-technical executive. Focus on the business risk, attack vector, and urgency to patch.

Vulnerability Risk Scoring Table

Create a CVSS-based scoring table to prioritize patching across five systems based on severity, exposure, and asset criticality.

Vulnerabilities & Threat Intel

Zero-Day Alert Response

Simulate a situation where a zero-day is released targeting Exchange servers. Generate an internal alert and IR team checklist to assess exposure.

Exploit Prediction Workflow

Draft a workflow to predict which recently disclosed vulnerabilities are most likely to be exploited based on threat actor chatter, exploit POCs, and vendor delay.

Vulnerabilities & Threat Intel

Threat Intel Report Summary

You've received a 10-page threat intel report from a vendor. Summarize it into a 1-page executive brief with action items and relevant IOCs.

IOC Correlation Script

Write a script or step-by-step prompt to correlate IP, URL, domain, and file hash IOCs against your firewall, DNS, and EDR logs.

Vulnerabilities & Threat Intel

Exploit Walkthrough (Lab Format)

Create a guided lab for safely exploiting a known vulnerability (e.g. EternalBlue or Log4Shell) in a virtual lab. Include setup and rollback options.

Threat Actor Profile Builder

Build a profile on the APT group ‘Lazarus’ based on publicly available MITRE and threat intel reports. Include targets, tools, and known TTPs.

Vulnerabilities & Threat Intel

Patch Management Audit Checklist

Generate a 10-point checklist for auditing patch management practices in an organization with both Windows and Linux systems.

Threat Intel Feeds vs SIEM Usefulness

Compare five popular threat intelligence feeds in terms of data quality, integration support, and SIEM compatibility. Include recommendations for SMBs.

Vulnerabilities & Threat Intel

Vulnerability Disclosure Policy Draft

Generate a public-facing Vulnerability Disclosure Policy (VDP) that encourages ethical hackers to report bugs responsibly, including scope, contact, and safe harbor language.

Predictive Threat Intel Planning

Guide me through building a predictive threat intelligence model using recent CVEs, geopolitical context, and threat actor patterns to forecast likely attack targets.

Vulnerabilities & Threat Intel

Exploit PoC Vetting Checklist

Create a checklist for analyzing public Proof-of-Concept (PoC) exploits to determine if they are safe, reliable, and legitimate before internal testing.

CVE Patch Prioritization by Asset Risk

Generate a patch prioritization matrix based on CVSS score, exploit availability, asset criticality, and exposure to the internet.

Vulnerabilities & Threat Intel

Dark Web Vulnerability Sale Monitoring

Simulate a threat intelligence process for identifying when a newly discovered CVE is being discussed or sold on dark web forums or marketplaces.

Third-Party Vulnerability Risk Matrix

Write a prompt to assess a company's third-party vendor exposure based on recently disclosed vulnerabilities affecting those vendors' software or infrastructure.

Vulnerabilities & Threat Intel

Threat Actor-CVE Mapping

Generate a table linking specific threat actors (e.g. APT29, FIN7) to the CVEs they most commonly exploit, using MITRE or threat report data.

ICS/SCADA Vulnerability Report

Create a vulnerability report template tailored to industrial control systems (ICS), including affected OT software, CVEs, patch status, and operational risk.

Vulnerabilities & Threat Intel

NVD Feed Automation

Write a prompt to ingest NIST NVD RSS feed updates and summarize the 3 most critical vulnerabilities discovered in the past 24 hours.

Threat Modeling from a Known CVE

Use CVE-2021-44228 (Log4Shell) to build a threat model in STRIDE format. Include attacker goals, affected assets, and possible mitigations.

Home Lab Setup & CTF Training

VirtualBox Lab Build

Guide me step-by-step on how to create a cybersecurity home lab using VirtualBox with a Windows Server domain controller, Windows 10/11 client, and a Kali Linux attacker box.

Vulnerable Web App Setup

Create a tutorial for installing DVWA (Damn Vulnerable Web App) inside a Docker container for local penetration testing practice.

Home Lab Setup & CTF Training

Active Directory Attack Simulation

Design a practice lab to simulate an AD attack chain using BloodHound and SharpHound. Include network setup, AD user creation, and permissions.

Capture-the-Flag Challenge Generator

Generate a beginner-friendly CTF-style challenge involving password cracking, hidden text, or base64 decoding. Include flag validation instructions.

Home Lab Setup & CTF Training

Linux Privilege Escalation Playground

Provide a walkthrough to set up a Linux VM vulnerable to privilege escalation using weak sudo permissions and SUID binaries. Include a warning about ethical use.

Packet Capture Practice Lab

Build a packet capture lab with Wireshark that simulates DNS, HTTP, and SSH traffic. Include instructions to create suspicious traffic for analysis.

Home Lab Setup & CTF Training

Blue Team Detection Lab

Design a Wazuh SIEM training lab to detect brute-force logins, USB usage, and basic malware behavior on Windows endpoints.

BurpSuite Interception Drill

Create a BurpSuite lab scenario for intercepting and modifying POST requests on a vulnerable login form. Include target setup and practice objective.

Home Lab Setup & CTF Training

CTF Team Strategy Prompts

Generate a list of pre-game prompts a CTF team can use to divide roles, plan recon, identify likely categories, and track progress.

OSCP Prep Prompt Pack

Build a prompt sequence to simulate OSCP-style enumeration, exploitation, and privilege escalation on a practice machine. Include logic branching and hints.

Home Lab Setup & CTF Training

Build a Red vs Blue Live Fire Lab

Design a home lab where one machine plays the role of an attacker using Kali Linux and the other plays a blue team defender with Wazuh SIEM. Include objectives for both teams.

Credential Harvesting Simulation

Create a step-by-step lab to simulate credential harvesting using Evilginx or Gophish. Include setup, bait creation, and how to detect the activity.

Home Lab Setup & CTF Training

Build Your Own CTF Platform

Guide me in setting up a self-hosted CTF platform like CTFd or FBCTF. Include steps to host it locally and upload my own challenge sets.

Simulate a Malware Outbreak

Design a lab scenario where malware spreads laterally across a Windows workgroup. Simulate detection with Sysmon and mitigation via Group Policy.

Home Lab Setup & CTF Training

Chain-of-Exploitation Challenge

Generate a CTF-style challenge that requires a user to chain three exploits (e.g. *misconfigured S3 buckets > exposed credentials > RCE*). Include hints and a flag location.

CTF Category Planning

Act as a CTF event planner. Suggest 3 beginner, 3 intermediate, and 3 advanced challenges across the categories of Crypto, Web, Reverse Engineering, and Forensics.

Home Lab Setup & CTF Training

Ransomware Simulation

Build a ransomware simulation lab that uses a harmless script to encrypt files on a test VM. Include before/after system state and log collection instructions.

Simulate a Phishing Click Trail

Create a phishing lab using a fake login portal hosted on a local server. Simulate the click-through experience and log collection for blue team review.

Home Lab Setup & CTF Training

Capture the Flag Walkthrough Script

Write a guided walkthrough script for a basic Linux CTF box from TryHackMe or HackTheBox. Include enumeration, exploitation, and privesc explanations.

Add Log Forwarding to Your Lab

Guide me on configuring all my lab machines (Linux and Windows) to forward logs to a central SIEM (like Wazuh or Graylog). Include event types and transport methods.

Cyber Awareness & Education

Phishing Awareness Email Template

Write a monthly awareness email for employees about phishing red flags. Include a short story-based example and five quick prevention tips.

Social Engineering Quiz Generator

Create a 10-question multiple-choice quiz on social engineering tactics including phishing, vishing, and smishing.

Cyber Awareness & Education

Poster Slogan Generator

Generate five catchy cybersecurity awareness poster slogans for a school or small business setting. Make them memorable and motivational.

Cybersecurity Awareness Calendar

Draft a 12-month cybersecurity awareness content calendar with monthly themes, such as password hygiene, safe browsing, and data privacy.

Cyber Awareness & Education

Awareness Training Script

Write a 5-minute cybersecurity awareness training script for non-technical employees covering strong passwords, phishing, and device hygiene.

USB Baiting Scenario

Describe a realistic workplace scenario that explains how a malicious USB device could be used in a baiting attack. Include takeaway lessons.

Cyber Awareness & Education

Secure Remote Work Checklist

Create a checklist for remote workers to stay cyber-safe while using public Wi-Fi, personal devices, or working from home.

Quiz on Ransomware Basics

Generate a 10-question quiz about ransomware for a basic employee awareness course. Include an answer key.

Cyber Awareness & Education

Cyber Roleplay Trainer

Act as a suspicious caller trying to socially engineer an employee into revealing company credentials. Afterward, provide coaching on what went wrong.

Awareness Workshop Plan

Design a 60-minute cybersecurity awareness workshop agenda for small businesses. Include objectives, activities, and key takeaways.

Cyber Awareness & Education

Deepfake Awareness Training

Write a 5-minute training script that explains deepfakes and how they could be used in business email compromise (BEC) or CEO fraud scenarios. Include tips for identifying synthetic media.

Executive Cyber Briefing Prep

Generate a short, non-technical cybersecurity briefing for executives that covers recent risks, regulatory impact, and personal protection habits.

Cyber Awareness & Education

Mobile Device Security Poster

Design content for a printable poster that gives employees 5 tips to keep their personal and work phones secure from malware and phishing apps.

Cyber Hygiene for New Employees

Create a cybersecurity onboarding checklist for new hires that covers passwords, device use, data handling, and phishing recognition.

Cyber Awareness & Education

AI-Generated Awareness Assistant

Create a prompt sequence that lets HR or IT automatically generate a weekly awareness email with recent threats and safety tips.

IoT Device Security Awareness

Write a newsletter snippet warning employees about the risks of smart devices (e.g. Alexa, smart TVs, Wi-Fi plugs) on home and work networks.

Cyber Awareness & Education

Simulated Phishing Response Drill

Design a training prompt for running a simulated phishing email exercise and tracking employee response behaviors. Include debriefing questions.

Gamified Cyber Awareness Quiz

Generate a 10-question, gamified cybersecurity quiz for employees. Add a fun scoring system and category hints (e.g. passwords, phishing, public Wi-Fi).

Cyber Awareness & Education

Cyber Awareness for Remote Teams

Create a short awareness training agenda for fully remote employees that covers safe cloud usage, VPN expectations, and device hygiene.

Generational Cybersecurity Tips

Write 5 cybersecurity awareness tips each for Baby Boomers, GenX, Millennials, and GenZ. Tailor the language and examples to each generation's habits.

Policies & Compliance

Acceptable Use Policy Generator

Write a company-wide Acceptable Use Policy (AUP) for a 50-person organization with remote workers. Include sections on internet use, email, and removable media.

Data Classification Policy Draft

Create a basic data classification policy template with four tiers of sensitivity: Public, Internal, Confidential, and Restricted.

Policies & Compliance

Cybersecurity Policy Outline

Generate a high-level outline for a company-wide cybersecurity policy that includes access control, data protection, incident response, and training.

Vendor Risk Management Checklist

Write a 10-question checklist for evaluating third-party vendors from a cybersecurity and compliance perspective.

Policies & Compliance

BYOD Policy Template

Draft a Bring Your Own Device (BYOD) policy for a hybrid company. Cover access controls, acceptable apps, monitoring, and employee responsibilities.

Password Policy Generator

Write a password policy that meets NIST 800-63b guidelines and is easy for non-technical users to understand.

Policies & Compliance

Compliance Framework Comparison

Compare the goals and structure of NIST CSF, ISO 27001, and CIS Controls. Use a table format for side-by-side review.

Policy Review Tracker

Create a template for tracking cybersecurity policy review cycles, including last update, owner, next review date, and status.

Policies & Compliance

Privacy Policy Generator (GDPR Aligned)

Write a privacy policy for a U.S.-based company that serves European customers. Include language that aligns with GDPR requirements.

Incident Response Policy Draft

Generate a first draft of a company incident response policy based on NIST 800-61. Include roles, notification steps, and phases of response.

Policies & Compliance

Cyber Roles & Responsibilities Matrix

Generate a RACI matrix for cybersecurity within a small to mid-sized organization. Include roles like IT Admin, CISO, Compliance Officer, and Incident Response Lead.

AI Use Policy for Employees

Draft a company-wide AI use policy that governs employee use of tools like ChatGPT or Copilot. Include acceptable use, data protection, and intellectual property concerns.

Policies & Compliance

Audit-Readiness Checklist

Create a 15-point checklist to prepare a company for a third-party cybersecurity audit. Include documentation review, asset inventories, and access logs.

Third-Party Risk Assessment Template

Write a standard risk assessment form template to evaluate cybersecurity risks from vendors and service providers. Include risk scoring and remediation tracking.

Policies & Compliance

Encryption Policy Statement

Draft an organizational policy that defines acceptable encryption standards for data at rest and in transit, including use cases for AES-256, TLS 1.2+, and VPN requirements.

Incident Documentation Template

Generate a fillable template for documenting a cybersecurity incident, including discovery time, systems affected, initial triage, communications, and resolution.

Policies & Compliance

Remote Work Compliance Policy

Write a compliance policy for remote and hybrid employees that covers device security, VPN usage, physical workspace privacy, and reporting procedures.

Data Retention Policy Generator

Create a flexible data retention policy for an organization handling both employee records and customer PII. Include tiered timelines based on data type.

Policies & Compliance

Internal Audit Follow-Up Process

Write a short workflow that defines how to track, assign, and validate follow-up actions resulting from internal cybersecurity audit findings.

Compliance Policy Change Notification

Generate an email template to notify all employees of an updated cybersecurity policy. Include a summary of the change, effective date, and action required.

Cloud Security & DevSecOps

AWS IAM Misconfiguration Hunt

Generate a checklist for identifying common AWS IAM misconfigurations, including overly permissive roles, wildcard policies, and role chaining issues.

S3 Bucket Security Audit

Write a prompt to audit S3 buckets for public exposure, weak permissions, and improper encryption. Include remediation steps.

Cloud Security & DevSecOps

Azure Conditional Access Simulation

Simulate a conditional access policy in Azure AD that enforces MFA for high-risk logins and blocks legacy authentication.

CI/CD Pipeline Threat Model

Create a threat model for a Jenkins-based CI/CD pipeline, identifying risks at the code, build, and deployment stages using STRIDE.

Cloud Security & DevSecOps

GitHub Secrets Scanning

Design a prompt workflow that detects accidentally committed secrets in GitHub repos. Include recommended scanning tools and mitigation steps.

Infrastructure as Code (IaC) Linter Prompt

Create a prompt to review a Terraform configuration file for security misconfigurations such as open security groups or plaintext credentials.

Cloud Security & DevSecOps

Least Privilege Role Design in AWS

Generate IAM policies for a developer who only needs read access to CloudWatch, Lambda logs, and S3 buckets. Follow the principle of least privilege.

Detect Misconfigured Azure Storage Blobs

Write an Azure CLI prompt sequence to list public blob containers and detect those that allow anonymous read access.

Cloud Security & DevSecOps

Kubernetes Pod Security Policy Generator

Generate a Kubernetes Pod Security Policy that prevents containers from running as root and enforces read-only filesystem mounts.

AWS GuardDuty Alert Investigation

Create a step-by-step guide to triage a GuardDuty alert about potential EC2 credential exfiltration. Include log sources and actions to take.

Cloud Security & DevSecOps

GCP IAM Role Mapping

Generate a prompt to help identify inherited IAM permissions in GCP projects and determine whether roles violate least privilege.

CI/CD Secrets Management Prompt

Write a secure approach to manage secrets across CI/CD pipelines using Vault, GitHub Actions secrets, or AWS Secrets Manager.

Cloud Security & DevSecOps

CloudFormation Template Risk Review

Review a CloudFormation YAML template for security risks such as permissive networking or unencrypted volumes.

Docker Image Hardening Checklist

Create a checklist to harden Docker images before deploying them to production. Include base image choice, user permissions, and signing.

Cloud Security & DevSecOps

K8s Misconfiguration Detection Prompt

Build a prompt that reviews Kubernetes YAML deployment files to detect risky configurations like hostPath volumes, privileged mode, and lack of resource limits.

Detect Public Cloud Keys in Repos

Create a scanning prompt that detects AWS access keys or Azure secrets committed to code repositories. Include Regex patterns and next steps.

Cloud Security & DevSecOps

DevSecOps Alert Fatigue Mitigation

Design a system to reduce noise in DevSecOps alerting pipelines using risk-based prioritization, tool tuning, and suppression rules.

Multi-Cloud Security Posture Assessment

Write a prompt for assessing multi-cloud environments (AWS, Azure, GCP) for compliance with CIS Benchmarks and centralized logging.

Cloud Security & DevSecOps

Serverless Function Threat Modeling

Create a threat model for AWS Lambda functions exposed via API Gateway. Include common injection vectors, over-privileged roles, and log visibility gaps.

DevSecOps Training Plan Builder

Generate a 4-week DevSecOps training curriculum for developers transitioning to cloud-native security roles. Include labs, tools, and certification resources.

Thank You for Empowering Your Cyber Journey

You've just unlocked 200 AI-powered prompts designed to accelerate your cybersecurity workflows, training, and technical creativity. Whether you're defending networks, breaking into boxes, or building awareness, this guide is built for your success.

About the Creator / PORT::ZERO Cyber Solutions

Led by Rick Kelly, a U.S. military veteran, former law enforcement professional, and cybersecurity strategist, PORT::ZERO Cyber Solutions empowers individuals and organizations with world-class cybersecurity awareness and incident response resources. We believe in protecting against cyber threats through preparation, education, and innovation.

Contact / Social Links

Website: https://www.portzerocyber.com

Email: rgkelly@portzerocyber.com

Phone: (877) 317-4422

PORT::ZERO Cyber Solutions

Disclaimer:

This resource is intended for educational and ethical use only. PORT::ZERO Cyber Solutions is not responsible for how these prompts are used. Offensive tactics must be tested in legal, controlled environments.