

PRACTICAL TOOLS AND COURSE PATHWAYS

Top 10 Foundational Cybersecurity Tools

Practical learning guide and CyberJA course catalogue

Prepared by Richea Perry | Cybersecurity and GRC practitioner and educator

Cybersecurity tools help you collect evidence. Their value comes from understanding what the evidence means for business risk, security controls and decisions. This guide introduces ten foundational tools, gives you safe practice tasks and connects your next learning step to CyberJA courses.

How to use this guide

Choose a skill area that matches your current role or the role you want to enter.

Practise with your own lab or authorised training data, and retain a small work sample.

Explain the finding, business consequence and recommended action in plain language.

Use the course context to choose focused learning rather than trying to study everything at once.

For beginners and working professionals

Beginners can start with networking, Linux and discovery before progressing to vulnerability management and logs. Existing professionals can use the practice outputs to strengthen assessment, assurance and stakeholder communication skills.

[Take the free Cyber Career Roadmap Assessment](#)

The course scenarios and suggested outputs are illustrative applications, not promises of specific assignments. Course availability and content can change; review the linked course page before enrolling. Some links use CyberJA instructor referral codes. No fixed prices or discounts are promised.

PRACTICAL TOOLS AND COURSE PATHWAYS

Network foundations and assessment

1 Wireshark

Focus Network Security

Capture and inspect packets; understand TCP/IP, DNS, HTTP/HTTPS, ports and protocols; apply display filters; follow TCP streams; identify unusual or suspicious network activity.

Practice Inspect a DNS lookup and connection in your own lab capture. Explain the source, destination and protocol.

Keep as evidence A network summary that separates observed facts from assumptions.

[Official documentation](#)

2 Kali Linux

Focus Linux / Security Testing

Use core Linux commands, navigate the file system, understand permissions and networking utilities, install security tools, and learn how multiple assessment tools fit together.

Practice Navigate a lab file system, inspect permissions and identify the current user and network configuration.

Keep as evidence A short Linux command log with explanations.

[Official documentation](#)

PRACTICAL TOOLS AND COURSE PATHWAYS

Network foundations and assessment

3 Nmap

Focus Network Discovery

Discover live hosts, identify open TCP/UDP ports, enumerate services, perform basic OS/service detection, and understand network attack surfaces.

Practice Inventory hosts and services on an authorised lab network. Compare the result with your expected inventory.

Keep as evidence An asset list with unexpected services flagged for review.

[Official documentation](#)

4 OpenVAS / Greenbone

Focus Vulnerability Management

Run vulnerability scans, interpret CVEs and severity ratings, identify affected systems, understand remediation recommendations, and review vulnerability reports.

Practice Scan a deliberately vulnerable lab host. Select three findings and propose verification and remediation steps.

Keep as evidence A prioritised vulnerability report with owners and review dates.

[Official documentation](#)

PRACTICAL TOOLS AND COURSE PATHWAYS

Web testing validation and monitoring

5 Burp Suite

Focus Web Application Security

Inspect and modify HTTP requests/responses, understand headers, cookies, sessions and authentication, and learn the fundamentals of testing web applications.

Practice Use a training application to observe a login request, cookie and response. Explain how a session is maintained.

Keep as evidence An annotated HTTP example and a description of the security concern.

[Official documentation](#)

6 Metasploit Framework

Focus Penetration Testing

Understand vulnerabilities, exploits, payloads, modules and controlled exploitation in authorized lab environments; connect scanning findings with practical validation.

Practice In an isolated training environment, examine a module and its prerequisites. Explain what a validation result would and would not prove.

Keep as evidence A validation plan with scope, evidence and restoration steps.

[Official documentation](#)

7 Splunk / SIEM Platform

Focus Security Monitoring

Search and analyze logs, correlate events, build dashboards, create alerts, investigate suspicious activity, and understand the purpose of centralized security monitoring.

Practice Search sample authentication logs for repeated failed logins. Correlate timestamps and users before drawing a conclusion.

Keep as evidence A short investigation timeline and an alert rationale.

[Official documentation](#)

PRACTICAL TOOLS AND COURSE PATHWAYS

Windows evidence and investigation

8 Microsoft Sysinternals

Focus Windows Security

Use tools such as Process Explorer, Process Monitor, Autoruns, TCPView and Sysmon to understand processes, persistence, network connections and Windows security events.

Practice Observe a benign process, its network connections and startup entry in a Windows lab.

Keep as evidence An endpoint evidence summary using timestamps and process details.

[Official documentation](#)

9 Autopsy

Focus Digital Forensics

Examine disk images and storage media, recover deleted files, inspect browser and file-system artifacts, analyze metadata, and understand evidence preservation and forensic investigation.

Practice Examine a training disk image. Record relevant files, timestamps and the limits of your findings.

Keep as evidence An evidence log and an incident timeline using fictional data.

[Official documentation](#)

10 PowerShell

Focus Administration / IR Automation

Inspect processes, services, users, permissions, networking and Windows event logs; automate repetitive administration and incident-response tasks.

Practice Collect process, service and event-log information from your own Windows lab. Start with read-only commands.

Keep as evidence A documented script and a plain-language explanation of its output.

[Official documentation](#)

PRACTICAL TOOLS AND COURSE PATHWAYS

Turn tool practice into business value

Use a fictional training company with an employee portal, finance data and Windows endpoints. Give each technical activity a clear question and a decision it supports.

Discover what exists

Use Nmap to compare systems and services with the asset inventory. An unexpected service is a finding to investigate, not proof of compromise.

Assess weaknesses

Use Greenbone to identify potential vulnerabilities. Validate applicability and relate the result to asset criticality, exposure and remediation effort.

Observe and detect

Use Wireshark and sample SIEM logs to examine traffic and events. Correlate timestamps and identities; distinguish unusual activity from a confirmed incident.

Investigate an endpoint

Use Sysinternals, PowerShell and Autopsy in a lab to document processes, events and artifacts. Record collection details and the limits of your evidence.

Communicate a decision

Explain the affected asset, evidence, weakness, potential business consequence, recommended control, accountable owner and follow-up date.

Suggested learning progression

Start with Linux and networking using Kali Linux, Wireshark and Nmap. Add vulnerability assessment with Greenbone. Explore HTTP and authorised validation with Burp Suite and Metasploit. Then develop log analysis, Windows investigation and forensic skills using a SIEM, Sysinternals, PowerShell and Autopsy.

Kali Linux is a platform containing many tools, not one tool. Splunk is one example of a SIEM platform; the principles apply across products. Never scan, intercept traffic or validate exploits outside your authorised scope. Use fictional or sanitised data in your portfolio.

PRACTICAL TOOLS AND COURSE PATHWAYS

CyberJA course catalogue

Choose a course by the responsibility you want to develop. The situations below explain how the topic can support practical work.

1 GRC Analyst to Manager: Exploring Real Job Descriptions

Workplace context You want to move from completing GRC tasks to owning reviews, coordinating stakeholders or managing a programme.

Learning relevance Compare target job descriptions and identify the responsibilities you still need to demonstrate.

Suggested application Write a development plan that links three responsibilities to practical evidence.

[Explore this course on Udemy](#)

2 Practical Compliance Management for GRC Professionals

Workplace context An organisation has policies but cannot consistently show which obligations apply or whether controls operate.

Learning relevance Connect requirements, evidence and ownership in a practical compliance process.

Suggested application Map one obligation to a control, an evidence record and a review owner.

[Explore this course on Udemy](#)

3 “Best Practices” for Cybersecurity & GRC Professionals

Workplace context Your team needs a consistent approach to security activities across systems, policies and suppliers.

Learning relevance Use established practices to structure work and connect controls with business needs.

Suggested application Choose three improvements and explain the risk each addresses.

[Explore this course on Udemy](#)

PRACTICAL TOOLS AND COURSE PATHWAYS

CyberJA course catalogue

Choose a course by the responsibility you want to develop. The situations below explain how the topic can support practical work.

4 Practical Assessments for Cybersecurity & GRC Professionals

Workplace context Management asks whether security controls are effective and which gaps deserve attention first.

Learning relevance Turn observations and control evidence into an assessment that supports decisions.

Suggested application Write a finding with evidence, business impact and a recommended action.

[Explore this course on Udemy](#)

5 Effective IAM Governance: A Practical Approach

Workplace context Employees change roles, privileged permissions grow and departed users retain access.

Learning relevance Connect account lifecycle tasks with approvals, ownership and least privilege.

Suggested application Draft a joiner, mover and leaver workflow with completion evidence.

[Explore this course on Udemy](#)

6 Practical Zero Trust Implementation

Workplace context Users access cloud and internal services from different devices and locations.

Learning relevance Explore readiness and an implementation approach that treats access as a decision requiring verification.

Suggested application Outline access decisions for one sensitive application and identify prerequisites.

[Explore this course on Udemy](#)

PRACTICAL TOOLS AND COURSE PATHWAYS

CyberJA course catalogue

Choose a course by the responsibility you want to develop. The situations below explain how the topic can support practical work.

7 Developing an Effective Cybersecurity Program

Workplace context Security tools exist, but activities are fragmented and leadership cannot see a coherent programme.

Learning relevance Connect assets, risks, people, processes and technology when developing a cybersecurity programme.

Suggested application Outline programme priorities, owners and evidence of progress.

[Explore this course on Udemy](#)

8 Cloud Adoption Risk Assessment

Workplace context A business plans to move a sensitive application or dataset to the cloud.

Learning relevance Assess adoption risks and relate security protections to business and information needs.

Suggested application Create a risk summary covering data, identities, dependencies and responsibilities.

[Explore this course on Udemy](#)

9 Management of AI Risk

Workplace context A team wants to adopt an AI service without a clear view of data exposure or governance responsibilities.

Learning relevance Identify proposed uses, assess consequences and plan oversight for AI adoption.

Suggested application Document one use case, its key risks, controls and accountable owner.

[Explore this course on Udemy](#)

PRACTICAL TOOLS AND COURSE PATHWAYS

CyberJA course catalogue

Choose a course by the responsibility you want to develop. The situations below explain how the topic can support practical work.

10 IT Auditing Fundamentals for the GRC Analyst

Workplace context An auditor needs to determine whether access, change or operational controls are supported by reliable evidence.

Learning relevance Build a practical approach to reviewing controls and communicating findings.

Suggested application Define a test objective, evidence request and finding for one IT control.

[Explore this course on Udemy](#)

11 GRC Fundamentals

Workplace context You are new to GRC and need to understand how governance, risk and compliance relate to business operations.

Learning relevance Develop the vocabulary and context needed before attempting more specialised tasks.

Suggested application Explain how one business objective connects to a risk, control and owner.

[Explore this course on Udemy](#)

12 Implementing an Information Security Baseline

Workplace context A team manages systems with inconsistent minimum protections.

Learning relevance Explore how a baseline defines required controls and how implementation can be planned and checked.

Suggested application Specify minimum protections for one system and document exceptions.

[Explore this course on Udemy](#)

PRACTICAL TOOLS AND COURSE PATHWAYS

CyberJA course catalogue

Choose a course by the responsibility you want to develop. The situations below explain how the topic can support practical work.

13 Assessing Information Security Risk

Workplace context Management needs a structured view of threats, vulnerabilities and business consequences.

Learning relevance Develop a risk assessment approach using NIST SP 800-30, from preparation through communication and maintenance.

Suggested application Create one risk scenario and explain likelihood, impact and the decision required.

[Explore this course on Udemy](#)

14 Selection and Implementation of Security Controls

Workplace context An assessment identifies risk, but the team must decide which controls are appropriate.

Learning relevance Consider governance and business context when selecting and implementing security controls.

Suggested application Compare two control options and document the implementation owner and verification approach.

[Explore this course on Udemy](#)

15 Deepfake Defense

Workplace context A convincing voice or video message asks staff to take a sensitive action.

Learning relevance Explore deepfake risks and develop a defence strategy for verification and response.

Suggested application Draft a verification procedure for unusual payment or account-change requests.

[Explore this course on Udemy](#)

PRACTICAL TOOLS AND COURSE PATHWAYS

CyberJA course catalogue

Choose a course by the responsibility you want to develop. The situations below explain how the topic can support practical work.

16 Misconfigurations Management

Workplace context A service is exposed or an access setting is overly permissive despite deployed security tools.

Learning relevance Connect common misconfigurations with prevention and collaboration between offensive and defensive teams.

Suggested application Record an expected configuration, observed deviation and remediation evidence.

[Explore this course on Udemy](#)

17 Pivoting Into Cybersecurity & GRC

Workplace context You are considering a career change and want realistic expectations about roles and preparation.

Learning relevance Explore career experiences, common misconceptions and the business purpose of cybersecurity.

Suggested application Compare two roles and outline how your existing skills could support each.

[Explore this course on Udemy](#)

18 Introducing to Threat Hunting

Workplace context Alerts do not answer whether suspicious behaviour is already present in the environment.

Learning relevance Explore the threat-hunting mindset, approaches and basic hunts. The course is also promoted as Cybersecurity Threat Hunting Professional.

Suggested application Write a hunt hypothesis, required data sources and criteria for reviewing results.

[Explore this course on Udemy](#)

PRACTICAL TOOLS AND COURSE PATHWAYS

CyberJA course catalogue

Choose a course by the responsibility you want to develop. The situations below explain how the topic can support practical work.

19 Cybersecurity & GRC Professionals Tool-kit

Workplace context You need practical resources to connect career development, assessments and business impact.

Learning relevance Explore a collection of cybersecurity and GRC tasks, resources and career guidance.

Suggested application Choose one assessment resource and explain how you would use its output.

[Explore this course on Udemy](#)

20 Mobile Defense Technology Security

Workplace context Mobile devices and communications support sensitive defence operations.

Learning relevance Explore mobile technology risks, regulatory considerations and protective practices in a defence context.

Suggested application Outline a mobile-device risk scenario and appropriate protection considerations.

[Explore this course on Udemy](#)

21 Cybersecurity Strategy Development and Implementation

Workplace context Leadership needs a cybersecurity direction that aligns spending and activities with business goals.

Learning relevance Explore an approach to developing a cybersecurity strategy and presenting it to senior management.

Suggested application Prepare a strategy outline with objectives, priorities, owners and progress measures.

[Explore this course on Tutorialspoint](#)

[View Richea Perry instructor profile for catalogue updates](#)

Catalogue reviewed October 2026. Developing an Effective Cybersecurity Program uses the earlier The Ultimate Cybersecurity Professional course URL. Public course titles may differ from earlier promotional names.