zyBook Introduction to Security: Labs and Skills Matrix

Chapter Title	Walkthrough Lab Title	Case Study: Practical Insights Title	Scenario Lab Title	Key Skills / Focus	Real-World Connection	Student Outcomes
Introduction to Security	Malware	Sony Pictures Entertainment malware attack (2014)	N/A	- Crafting payloads with Metasploit Framework (Kali Linux) • Creating reverse shells with *msfvenom* • Configuring listeners with *multi/handler* • Executing post-exploitation commands (*pwd*, *cd*, *dir*, *download*, *cat*) - Delivering phishing attachments via Thunderbird	Demonstrates how attackers used spear-phishing and malware payloads for lateral movement, highlighting the need for user awareness, endpoint monitoring, and timely incident investigation.	Enables learners to simulate real-world attacker behaviors by crafting and delivering malware via spear-phishing, and gain hands-on experience with post-exploitation tools, directly supporting red teaming. Validation example**:** Confirm a *Meterpreter* session is established and a file from the target system can be downloaded.
Identity and Access Management	Account management	SolarWinds supply chain attack (2020)	Account Management • Learners harden an Active Directory domain by creating users and OUs, applying GPOs, and enforcing password and lockout policies to strengthen identity governance	- Creating Organizational Units with ADUC - Adding domain users with ADUC - Configuring GPOs with GPMC (disable Control Panel, block removable storage) - Enforcing password length and lockout policies via GPMC	Highlights how weak Active Directory governance enabled persistent threats in the SolarWinds breach, reinforcing the importance of robust identity management frameworks for organizational security.	Provides practical experience in hardening enterprise domains through account creation and group policy design, helping learners implement access controls and audit user privileges which are essential tasks for preventing persistent threats and enhancing organizational identity governance. Validation example: Confirm users cannot access *Control Panel* after GPO enforcement.
Cryptography	Public Key Infrastructure (PKI)	Comodo Certificate Authority attack (2011)	N/A	- Installing Root CA role with AD CS - Configuring standalone CA with SHA-512 signing - Creating a website in IIS - Generating a CSR in IIS - Transferring CSR via *scp* - Retrieving issued certificates from CA - Binding HTTPS certificate to port 443 in IIS	Links mis-issued certificates in the Comodo incident to poor CA management, underlining the importance of trustworthy digital authentication and lifecycle oversight for all secure infrastructures.	Develops core skills in deploying PKI, from configuring certificate authorities to managing SSL lifecycle, enabling secure web service implementation and improving understanding of best practices for digital trust and authentication in enterprise environments. Validation example: Confirm browsing to site's HTTPS address displays valid SSL padlock with correct certificate details.
Network Attacks and Secure Network Protocols	Network enumeration	WannaCry ransomware attack (2017)	Security audit through network scanning • Learners perform host discovery, packet capture, and OS fingerprinting to identify vulnerable systems in a network environment, replicating adversary scanning behavior.	- Discovering hosts with *arp-scan* (active) - Identifying hosts with *netdiscover -p* (passive) - Capturing ARP and ICMP traffic with Wireshark - Running ICMP echo and port scans with *hping3* - Fingerprinting OS and services with *nmap* (*-sV, -O*)	Illustrates how WannaCry exploited SMB scans for rapid propagation, stressing the need for proactive network monitoring and vulnerability assessment across interconnected organizations.	Trains learners to act as network defenders by conducting active and passive host discovery, interpreting packet captures, and fingerprinting systems to uncover risks and attack surfaces, which are foundational skills for vulnerability assessment and penetration testing roles. Validation example: Verify *nmap -O* identifies Windows Server operating system.
Secure Network Design	Firewalls	Capital One breach (2019)	Securing the network • Learners design and test firewall rules to block insecure services and confirm only authorized traffic is allowed, reinforcing secure network operations.	- Creating inbound/outbound firewall rules with Windows Defender Firewall (ICMP, L2TP, HTTP, SSH, SMB) - Validating rules with ping tests - Scanning with *nmap* and *Zenmap* GUI - Testing blocked access via web browser - Confirming SMB sharing denial	Connects the Capital One breach to misconfigured firewalls, demonstrating the critical role of thorough access control policies and regular rule validation in defending against diverse attack vectors.	Equips learners to design, test, and document granular firewall rules, diagnose misconfigurations, and validate access restrictions, building operational capabilities for real-time network security management and compliance assurance. Validation example: Confirm *nmap* shows port 80 closed after HTTP blocking rule applied.

zyBook Introduction to Security: Labs and Skills Matrix

Physical Security and Cybersecurity Resilience	Redundant Array of Independent Disks (RAID)	Change Healthcare ransomware attack (2024)	N/A	- Configuring RAID 0 (striping, 2 disks) - Configuring RAID 1 (mirroring, 2 disks) - Configuring RAID 5 (striping + parity, 3 disks) - Converting basic to dynamic disks - Labeling and formatting volumes	Relates RAID redundancy and its limits to real-world ransomware resilience failures, informing strategies for data protection, business continuity, and rapid recovery planning.	Strengthens understanding of redundant storage architectures through hands-on disk provision and failure simulation, teaching learners to protect data availability and mitigate the impact of ransomware, which are critical for systems administration and disaster recovery planning. Validation example: Confirm RAID 1 array remains accessible after one disk taken offline.
Security Assessment	Log management in Windows and Linux	Equifax breach (2017)	Enhancing log management practices • Learners configure and analyze Windows and Linux logs, and use command-line tools to detect suspicious activity for early breach detection.	- Analyzing Application, Security, and System logs with *Event Viewer* - Saving logs as *.evtx* files - Configuring log size and retention policies - Inspecting /var/log files in Linux (syslog, auth.log, messages) - Viewing logs with *less* - Searching logs with *grep* - Monitoring logs with *tail -f* - Configuring log rotation with *logrotate* - Forcing rotation with *logrotate -v -f*	Shows how delayed breach detection at Equifax resulted from inadequate logging, highlighting the role of integrated log management for compliance and early threat identification.	Provides mastery of log collection, parsing, and rotation on both Windows and Linux systems, developing the tools and workflows used in compliance validation and proactive monitoring for breaches as practiced by defense teams in security operations centers. Validation example: Verify running *logrotate -f* creates new compressed log file.
Privacy and Risk Management	Business continuity planning (BCP)	Hurricane Sandy's impact on data centers (2012)	N/A	- Installing DHCP role - Configuring DHCP scopes (range, exclusions, subnet mask, gateway, lease) - Setting up DHCP failover with primary and hot standby	Connects DHCP failover to disaster recovery during events like Hurricane Sandy, emphasizing resilient infrastructure design and effective emergency preparedness in enterprise environments.	Builds disaster recovery expertise by configuring and testing high-availability DHCP services, preparing learners to design and validate resilient network infrastructure for operational continuity during major outages or security incidents. Validation example: Confirm standby DHCP server issues new leases from correct scope after primary shut down.