GETU ACADEMY

16 Cybersecurity Projects to Build

One skill = one project.
The 6 from the video, then 10 more.
Every project has what you need, the steps, the commands to type, how you know you are done, and a line for your resume.

HOW TO USE THIS

1. Start with project 01 this week.
2. Do one project per skill.
3. Take screenshots as you go.
4. Put every finished project on GitHub and on your resume.
5. Only test systems you own.

Next: the roadmap to your first cyber job

getuprep.com/paths/cybersecurity

01 LOG ANALYSIS FROM THE VIDEO
Brute-Force Detection Dashboard

YOU NEED

VirtualBox, an Ubuntu Server VM, a Kali Linux VM, Splunk (free license)

Steps to Build

01 Create an Ubuntu Server VM and a Kali VM. Put both on the same Host-only network so they can only reach each other.

02 On Ubuntu, install SSH and add a test user with a weak password such as password123.

```
sudo apt install openssh-server
sudo adduser labuser
```

03 Find the Ubuntu VM's IP address.

```
ip a
```

04 On Kali, unpack the wordlist and attack your own server with Hydra.

```
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
hydra -l labuser -P /usr/share/wordlists/rockyou.txt \
  ssh://UBUNTU_IP
```

05 Download Splunk Enterprise from splunk.com (free account) and install it on Ubuntu. Then go to Settings > Licensing > Change license group and pick Free license.

06 In Splunk go to Settings > Add Data > Monitor > Files & Directories. Choose /var/log/auth.log and set the source type to linux_secure. If Splunk cannot read the file, add its user to the adm group.

07 Search for the failed logins and pull out the attacker's IP.

```
index=* "Failed password"
| rex "from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| timechart count by src_ip
```

01

LOG ANALYSIS FROM THE VIDEO (continued)

Brute-Force Detection Dashboard

08 Click Save As > Dashboard Panel. Add a second panel that ranks the attackers.

```
index=* "Failed password"
| rex "from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| stats count by src_ip | sort -count
```

YOU ARE DONE WHEN

Your dashboard shows a clear spike from the Kali IP at the time of the attack.

ON YOUR RESUME

Built a Splunk dashboard that detects SSH brute-force attacks from Linux authentication logs.

02 THREAT DETECTION FROM THE VIDEO
Home SOC Lab with Wazuh

YOU NEED

An Ubuntu Server VM with at least 4 GB RAM, a Windows 10 or 11 VM

Steps to Build

01 On Ubuntu, run the all-in-one installer from the Quickstart page at documentation.wazuh.com. It prints the dashboard password when it finishes. Save it.

02 Open https://UBUNTU_IP in a browser and log in to the Wazuh dashboard as admin.

03 In the dashboard click Deploy new agent, choose Windows, and enter the server IP. Copy the command it gives you and run it in PowerShell as Administrator on the Windows VM.

04 Download Sysmon from Microsoft Sysinternals and a community config (search GitHub for SwiftOnSecurity sysmon-config). Install it on Windows.

```
Sysmon64.exe -accepteula -i sysmonconfig-export.xml
```

05 Tell the agent to collect Sysmon events: in the agent's ossec.conf add a localfile block for the Microsoft-Windows-Sysmon/Operational event channel, then restart the agent.

```
Restart-Service WazuhSvc
```

06 Install Atomic Red Team in PowerShell, then run a test attack.

```
IEX (IWR 'https://raw.githubusercontent.com/
redcanaryco/invoke-atomicredteam/master/
install-atomicredteam.ps1' -UseBasicParsing)
Install-AtomicRedTeam -getAtomics
Invoke-AtomicTest T1059.001
```

07 In Wazuh open Threat Hunting > Events and find the test. Run three more techniques. Note which raised alerts and which did not.

02 THREAT DETECTION FROM THE VIDEO (continued)

Home SOC Lab with Wazuh

08 Write a rule for one that was missed in /var/ossec/etc/rules/local_rules.xml on the server. Restart the manager and run the test again.

```
sudo systemctl restart wazuh-manager
```

YOU ARE DONE WHEN

A technique that was silent before now raises your own custom alert.

ON YOUR RESUME

Deployed a Wazuh SIEM with Sysmon, simulated MITRE ATT&CK techniques and wrote custom detection rules.

03 Malware Infection Investigation

INCIDENT RESPONSE FROM THE VIDEO

YOU NEED

Wireshark, one exercise from malware-traffic-analysis.net

Steps to Build

01 Go to malware-traffic-analysis.net and open Traffic Analysis Exercises. Pick one and download the PCAP zip. The zip password is explained on the site's About page.

02 Open the PCAP in Wireshark. Start with Statistics > Conversations to see which machines talked the most.

03 Identify the victim: its IP, MAC address, hostname and Windows user name. Try these display filters one at a time.

```
dhcp
nbns
kerberos.CNameString
```

04 Find the web traffic that started the infection.

```
http.request or tls.handshake.type == 1
```

05 Export any downloaded files with File > Export Objects > HTTP, then hash them. Do not open them.

```
sha256sum FILENAME
```

06 Look up the hashes, domains and IP addresses on virustotal.com to name the malware family.

07 Write a one-page incident report: summary, victim details, timeline, indicators of compromise, and what to contain first. Then compare it with the answers posted on the site.

03 INCIDENT RESPONSE FROM THE VIDEO (continued)

Malware Infection Investigation

YOU ARE DONE WHEN

Your report names the infected host and user, the malware family, and lists the indicators.

ON YOUR RESUME

Investigated a malware infection from packet capture and wrote the incident report with IOCs.

04 Pentest of a Vulnerable Machine

PEN TESTING FROM THE VIDEO

YOU NEED

VirtualBox, Kali Linux, Metasploitable 2 (free download)

Steps to Build

01 Import both VMs. Set both network adapters to Host-only so the vulnerable machine never touches the internet. Only ever test machines you own.

02 On Kali, find your network, then find the target.

```
ip a
sudo nmap -sn 192.168.56.0/24
```

03 Scan every port and identify each service and version.

```
sudo nmap -sV -p- TARGET_IP
```

04 Pick a service and search for its version plus the word exploit. Example: vsftpd 2.3.4 has a known backdoor.

05 Exploit it with Metasploit.

```
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS TARGET_IP
run
```

06 Prove your access and take a screenshot.

```
whoami
hostname
```

07 Repeat with a second service. Then write the report: scope, each finding, the evidence, a risk rating, and how to fix it.

YOU ARE DONE WHEN

You have root on the target and a report a client could act on.

ON YOUR RESUME

Performed a full penetration test in a lab: enumeration, exploitation with Metasploit, and a written report.

05 CLOUD SECURITY FROM THE VIDEO
Hardened AWS Account from Scratch

YOU NEED

A new AWS account on the free tier, the AWS CLI

Steps to Build

01 Sign in as root one time. Under Security credentials turn on MFA and confirm root has no access keys.

02 Create an admin IAM user with MFA for daily work. Stop using root.

03 Create a group called ReadOnlyAnalysts with the AWS managed policy ReadOnlyAccess. Add a test user and confirm it can look but cannot change anything.

04 Turn on CloudTrail: create a trail that sends management events to a new S3 bucket.

05 Check that S3 Block Public Access is on for the whole account.

```
aws s3control get-public-access-block \
  --account-id YOUR_ACCOUNT_ID
```

06 Create a test bucket and turn Block Public Access off for it on purpose. Then detect it from the command line.

```
aws s3api get-public-access-block --bucket BUCKET
```

07 Fix it.

```
aws s3api put-public-access-block --bucket BUCKET \
  --public-access-block-configuration \
  BlockPublicAcls=true,IgnorePublicAcls=true,\
  BlockPublicPolicy=true,RestrictPublicBuckets=true
```

08 Find your own changes in CloudTrail > Event history. Write down each control and the attack it stops. Set a budget alert and delete the test resources.

05 CLOUD SECURITY FROM THE VIDEO (continued)

Hardened AWS Account from Scratch

YOU ARE DONE WHEN

Root is locked down, every change is logged, and you caught and fixed your own public bucket.

ON YOUR RESUME

Hardened an AWS account: MFA, least-privilege IAM, CloudTrail logging and S3 public-access controls.

06 Threat-Intel Enrichment Bot

SECURITY AUTOMATION FROM THE VIDEO

YOU NEED

Python 3, free VirusTotal and AbuseIPDB accounts, a Discord server you own

Steps to Build

01 Create free accounts at virustotal.com and abuseipdb.com and copy your API keys. In Discord go to Server Settings > Integrations > Webhooks > New Webhook and copy the URL.

02 Install the library and put suspicious IPs in iocs.txt, one per line.

```
pip install requests
```

03 Ask VirusTotal about each IP.

```
requests.get(
  "https://www.virustotal.com/api/v3/ip_addresses/"+ip,
  headers={"x-apikey": VT_KEY})
```

04 Ask AbuseIPDB about each IP.

```
requests.get(
  "https://api.abuseipdb.com/api/v2/check",
  params={"ipAddress": ip},
  headers={"Key": ABUSE_KEY})
```

05 Read the scores from the JSON: last_analysis_stats.malicious from VirusTotal and abuseConfidenceScore from AbuseIPDB. Wait 16 seconds between VirusTotal calls to stay inside the free limit.

06 Post anything malicious to your Discord channel.

```
requests.post(WEBHOOK_URL, json={"content": msg})
```

07 Keep the keys in environment variables, not in the code. Then schedule it to run every 30 minutes.

```
crontab -e
*/30 * * * * python3 /home/you/bot.py
```

06 SECURITY AUTOMATION FROM THE VIDEO (continued)

Threat-Intel Enrichment Bot

YOU ARE DONE WHEN

A bad IP in iocs.txt produces an alert in Discord without you touching anything.

ON YOUR RESUME

Wrote a Python bot that enriches indicators with VirusTotal and AbuseIPDB and alerts to Discord.

07 EMAIL SECURITY
Phishing Email Analyzer

YOU NEED

A phishing email from your own spam folder, Python 3

Steps to Build

01 In your mail app choose Show original or Download message and save the email as mail.eml. Do not click anything inside it.

02 Open the file in a text editor. Read Return-Path, Reply-To and the Received lines from the bottom up to see where it really came from.

03 Find the Authentication-Results header and note the results for spf, dkim and dmarc.

04 Parse it with Python's built-in email module.

```
import email
msg = email.message_from_file(open("mail.eml"))
print(msg["From"], msg["Return-Path"])
```

05 Pull every link out of the body, and hash any attachments with SHA-256.

```
re.findall(r"https?://\S+", body)
```

06 Check the links and hashes on virustotal.com.

07 Make the script print a verdict with reasons: failed checks, mismatched sender, bad links.

YOU ARE DONE WHEN

You feed it an .eml file and it prints phish or safe, with the evidence.

ON YOUR RESUME

Built a Python tool that analyzes email headers, authentication results and links to flag phishing.

08 THREAT INTEL
SSH Honeypot

YOU NEED

A small cloud VM with nothing else on it, Docker

Steps to Build

01 Create the smallest VM your cloud provider offers. Move your real SSH login to a different port first so you do not lock yourself out.

02 Install Docker, then run Cowrie, an open-source SSH honeypot.

```
docker run -d -p 2222:2222 cowrie/cowrie
```

03 Send port 22 to the honeypot.

```
sudo iptables -t nat -A PREROUTING -p tcp \
  --dport 22 -j REDIRECT --to-port 2222
```

04 Open port 22 in the provider's firewall and leave it running for 3 to 7 days.

05 Read what the attackers did.

```
docker ps
docker logs CONTAINER_ID
```

06 Count the top usernames, passwords and source IPs they tried. List the commands they ran after logging in.

07 Chart the results, write up what you learned, and delete the VM.

YOU ARE DONE WHEN

You have real attacker data and a chart of who tried what.

ON YOUR RESUME

Deployed a Cowrie SSH honeypot and analyzed real attacker credentials and commands.

09 VULNERABILITY MANAGEMENT
Vulnerability Scan + Fix Report

YOU NEED

Nessus Essentials (free activation code from tenable.com) or OpenVAS, a lab VM you own

Steps to Build

01 Register for Nessus Essentials, install it, and wait for the plugins to finish downloading.

02 Click New Scan > Basic Network Scan. Enter your lab VM's IP address and nothing else. Launch it.

03 When it finishes, sort by severity and open the top five findings. Read the Description and the Solution for each.

04 Fix them. Apply updates, turn off the service, or change the setting the Solution names.

```
sudo apt update && sudo apt upgrade
```

05 Run the same scan again and export both reports.

06 Write a before-and-after table: finding, severity, fix applied, result.

YOU ARE DONE WHEN

The second scan shows your top findings gone, and you can explain each fix.

ON YOUR RESUME

Ran vulnerability scans with Nessus, remediated critical findings and documented the results.

10 IDENTITY
Active Directory Lab

YOU NEED

Windows Server evaluation ISO (free from Microsoft), a Windows 10 or 11 VM, VirtualBox

Steps to Build

01 Install Windows Server in a VM and give it a static IP. In PowerShell as Administrator, add the role.

```
Install-WindowsFeature AD-Domain-Services `
  -IncludeManagementTools
```

02 Create the domain. The server restarts as a domain controller.

```
Install-ADDSForest -DomainName lab.local
```

03 Create OUs, groups and a few users in Active Directory Users and Computers, or with PowerShell.

```
New-ADUser -Name "Sam Lee" -SamAccountName slee `
  -Enabled $true -AccountPassword `
  (Read-Host -AsSecureString)
```

04 On the client VM set DNS to the server's IP, then join it to lab.local from the system settings (Rename this PC, advanced).

05 In Group Policy Management edit the Default Domain Policy. Set a minimum password length and an account lockout threshold.

06 From the client, try one wrong password against several users. That is a password spray, on your own lab only.

07 On the domain controller open Event Viewer > Windows Logs > Security. Find the failed logons (Event ID 4625) and the lockouts (4740).

10 IDENTITY (continued) Active Directory Lab

YOU ARE DONE WHEN

You can show the attack in the logs and the policy that stopped it.

ON YOUR RESUME

Built an Active Directory domain, applied Group Policy, and detected a password spray in the security logs.

NETWORK SECURITY

11 Home Firewall + IDS

YOU NEED

pfSense CE (free), VirtualBox, two lab VMs

Steps to Build

01 Create a pfSense VM with two adapters: WAN set to NAT and LAN set to an internal network. Put a lab VM on the LAN side.

02 From the LAN VM open https://192.168.1.1 and finish the setup wizard.

03 Go to Firewall > Rules > LAN. Add a rule that blocks one destination, test it, and find the block in Status > System Logs > Firewall.

04 Go to System > Package Manager > Available Packages and install Suricata.

05 Go to Services > Suricata. Add the LAN interface, enable the ET Open rules, update them, and start the interface.

06 From a second VM, scan the LAN VM.

```
sudo nmap -sS -p- TARGET_IP
```

07 Open the Suricata Alerts tab and find the scan. Then suppress one noisy rule that is a false positive in your lab.

YOU ARE DONE WHEN

Your firewall blocks what you told it to and your IDS caught the scan.

ON YOUR RESUME

Deployed a pfSense firewall with Suricata IDS, wrote rules and tuned alerts.

12 PASSWORDS

Password Cracking Lab

YOU NEED

Kali Linux (Hashcat and the rockyou wordlist are included)

Steps to Build

01 Make your own test hashes so you never touch real accounts. Repeat this with a few weak and a few strong passwords.

```
openssl passwd -6 'password123' >> hashes.txt
```

02 Unpack the wordlist if you have not already.

```
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

03 Crack with the wordlist. Mode 1800 is sha512crypt.

```
hashcat -m 1800 hashes.txt \
  /usr/share/wordlists/rockyou.txt
```

04 Add rules to catch variations of common passwords.

```
hashcat -m 1800 hashes.txt \
  /usr/share/wordlists/rockyou.txt \
  -r /usr/share/hashcat/rules/best64.rule
```

05 Show what cracked.

```
hashcat -m 1800 hashes.txt --show
```

06 Record which passwords fell, how long each took, and which survived.

07 Write a one-page password policy based on what you saw: length, passphrases, MFA, lockout.

YOU ARE DONE WHEN

You can show which passwords broke in seconds and which held.

ON YOUR RESUME

Audited password strength with Hashcat and wrote a password policy from the results.

APP SECURITY

13 Web App Hacking

YOU NEED

Docker, OWASP Juice Shop, Burp Suite Community (all free)

Steps to Build

01 Run the deliberately vulnerable shop on your own machine.

```
docker run -d -p 3000:3000 bkimminich/juice-shop
```

02 Start Burp Suite. Go to Proxy > Open browser and visit http://localhost:3000. Browse the shop so the requests show up in HTTP history.

03 SQL injection: on the login page type this as the email, with any password.

```
' OR 1=1--
```

04 You are now logged in as the admin. Find that request in Burp and work out why it worked.

05 Cross-site scripting: paste this into the search box.

```
<iframe src="javascript:alert(`xss`)">
```

06 Open http://localhost:3000/#/score-board to see every challenge. Solve three more.

07 For each finding write: the OWASP Top 10 category, how you found it, the impact, and the fix. For SQL injection the fix is parameterized queries.

YOU ARE DONE WHEN

Five solved challenges, each with a write-up and a fix.

ON YOUR RESUME

Found and exploited SQL injection and XSS in OWASP Juice Shop using Burp Suite, with remediation notes.

14 MALWARE
Malware Analysis Lab

YOU NEED

The REMnux VM (free), VirtualBox

Steps to Build

01 Import the REMnux VM and take a snapshot. Before you handle any sample, set its network adapter to Host-only or disconnect it.

02 Download one sample from bazaar.abuse.ch and move it into the VM. The zip password is: infected. Never unzip or run it on your real computer.

03 Identify the file and record its hash.

```
file sample.bin
sha256sum sample.bin
```

04 Pull the readable text and look for URLs, IPs, file paths and commands.

```
strings -n 8 sample.bin | less
```

05 For Windows programs, list what the file is capable of.

```
capa sample.bin
```

06 Look the hash up on virustotal.com and on MalwareBazaar to confirm the family.

07 Write the indicators report: hashes, family, network indicators, what it appears to do. Then revert the VM to the snapshot.

YOU ARE DONE WHEN

A one-page report another analyst could use to hunt for this sample.

ON YOUR RESUME

Performed static malware analysis in an isolated REMnux lab and produced an IOC report.

15 GRC
Risk Assessment

YOU NEED

A spreadsheet, the NIST Cybersecurity Framework 2.0 (free from nist.gov)

Steps to Build

01 Invent a 20-person company: what it sells, where its data lives, which tools it uses.

02 List its assets: laptops, email, customer database, website, payroll, backups.

03 For each asset write what could go wrong: phishing, ransomware, a lost laptop, a leaked database.

04 Score each risk for likelihood and for impact, from 1 to 5. Multiply the two and sort highest first.

05 For the top ten write a control and tag it with a CSF function: Govern, Identify, Protect, Detect, Respond or Recover.

06 Mark each risk as reduce, accept, transfer or avoid, with an owner and a date.

07 Turn the top five into a one-page summary a manager could read in two minutes.

YOU ARE DONE WHEN

A risk register and a one-page summary for a non-technical reader.

ON YOUR RESUME

Completed a risk assessment mapped to the NIST Cybersecurity Framework for a small business.

16 DETECTION ENGINEERING

Detection Rules with Sigma

YOU NEED

Python 3, sigma-cli, your Splunk or Wazuh lab from projects 01 and 02

Steps to Build

01 Install the tools.

```
pip install sigma-cli
sigma plugin install splunk
```

02 Pick three techniques from attack.mitre.org that you can run in your lab, for example T1059.001 (PowerShell).

03 Read two or three rules in the SigmaHQ/sigma repository on GitHub to learn the format.

04 Write your own rule as a .yml file with a title, a logsource, a detection section (selection and condition), a level, and an ATT&CK tag.

05 Convert it into a Splunk search.

```
sigma convert -t splunk -p splunk_windows \
  my_rule.yml
```

06 Run the technique in your lab, then run the search. Confirm it fires, and check it stays quiet on normal activity.

```
Invoke-AtomicTest T1059.001
```

07 Document each rule: what it detects, the test you ran, the result, and known false positives.

YOU ARE DONE WHEN

Three rules that each fire on your own test and are written up.

ON YOUR RESUME

Wrote and tested Sigma detection rules mapped to MITRE ATT&CK and converted them for Splunk.

Built one?

Reply to my DM and tell me which project you finished. I will point you to the next step.

NEXT

Certs help. Skills get you hired.

You just got the skills side. Here is the cert side:

THE ROADMAP TO YOUR FIRST CYBERSECURITY JOB

Network+ > Security+ > CySA+

Start free: 15 Network+ practice questions, no sign-up.

getuprep.com/paths/cybersecurity

More free tech resources daily:

@getuacademy on Instagram