**WordPress Portal with Splunk SOAR & Deep Testing: 12-Day Plan**

**Project Overview**

* **Goal**: Build a WordPress student portal on AWS (EC2, Elastic Beanstalk) and Azure (VM, App Service), add Splunk SOAR automation, and perform in-depth security testing.
* **Timeline**: 12 days, ~5 hours/day (~60 hours total).
* **Resources**: AWS Free Tier, Azure for Students ($100 credit), Splunk SOAR Community Edition, free tools (WPScan, Nmap, OpenVAS).
* **Skills**: Basic Linux, Git, WordPress; no prior SOAR/pentesting experience needed.
* **Deliverables**:
  + WordPress portal (courses, Azure AD login, API).
  + Security: IAM, SSL, VPC/NSG, Splunk logs, SOAR automation.
  + Testing: Nmap, WPScan, OpenVAS, IAM/NSG audits.
  + Report (~8 pages), screenshots, GitHub repo.

**Assumptions**

* Use **Splunk SOAR Community Edition** (AWS Marketplace, free, 100 actions/day) for basic automation (e.g., login failure alerts).
* Deep testing: Nmap scans, WPScan (WordPress), OpenVAS (infrastructure), manual IAM/NSG checks.
* No custom coding; leverage pre-built playbooks and Marketplace WordPress.
* Solo/small team (1–2 students).

**Time Estimate for New Tasks**

1. **Splunk SOAR** (~5 hours):
   * Setup: Deploy SOAR on EC2 (t2.micro, 2 hours).
   * Integration: Link with Splunk, CloudTrail, Azure Monitor (1.5 hours).
   * Playbooks: Activate pre-built (e.g., “Account Lockout,” 1 hour).
   * Test: Simulate failed logins, verify alerts (0.5 hours).
2. **In-Depth Testing** (~9 hours):
   * Nmap Scans: Scan EC2/VM/App Service (1.5 hours).
   * WPScan: Check WordPress plugins/themes (2 hours).
   * IAM/NSG Review: Audit permissions (1.5 hours).
   * OpenVAS: Scan for CVEs (2 hours).
   * Fixes/Report: Update plugins, document findings (2 hours).
3. **Total Added**: ~14 hours (replaces ~5 hours basic pentesting, ~5 hours automation).

**Adjusted 12-Day Plan (~57 hours)**

* **Optimization**: Use WordPress Marketplace (~2 hours saved), merge logging/SOAR (Day 7), reduce documentation (Day 12: 5 → 4 hours).
* **Daily Hours**: ~4.75 hours/day average, ~3 hours buffer.

**Day 1: Planning & Setup (~4.5 hours)**

* Tasks: Define scope, setup AWS/Azure accounts, install Terraform/CLI/Git/Nmap/WPScan, create GitHub repo.
* Deliverables: Requirements doc, tools ready, repo.
* Notes: Reuse old plan to save time.

**Day 2: IAM & Storage (~4.5 hours)**

* Tasks: AWS IAM (EC2/S3), Azure RBAC (VM/App Service), encrypted S3/Blob Storage, Terraform scripts.
* Deliverables: Secure IAM/RBAC, storage, scripts.
* Notes: Streamline testing.

**Day 3: AWS EC2 WordPress Backend (~5 hours)**

* Tasks: Terraform EC2 (t2.micro, VPC), deploy WordPress (Marketplace), configure security group (HTTP:80, SSH:your IP).
* Deliverables: EC2 WordPress backend.
* Notes: Marketplace saves ~1 hour.

**Day 4: Azure VM MySQL (~5 hours)**

* Tasks: Terraform VM (B1s, VNet, NSG:3306), deploy MySQL, connect EC2 WordPress.
* Deliverables: MySQL VM, EC2 connected.

**Day 5: AWS Elastic Beanstalk Frontend (~4.5 hours)**

* Tasks: Deploy WordPress (Marketplace), configure MySQL, sync wp-content with S3.
* Deliverables: WordPress frontend, S3 sync.
* Notes: Marketplace saves ~0.5 hours.

**Day 6: Azure App Service API (~4.5 hours)**

* Tasks: Deploy WordPress (Marketplace, F1 tier), enable REST API, connect MySQL.
* Deliverables: WordPress API, frontend integrated.
* Notes: Marketplace saves ~0.5 hours.

**Day 7: Logging & Splunk SOAR (~5 hours)**

* Tasks: Setup CloudTrail (S3), Azure Log Analytics, Splunk Community, SOAR (EC2), integrate SOAR with Splunk/AWS/Azure, configure playbook (e.g., login alerts).
* Deliverables: Logs, Splunk, SOAR playbooks.
* Notes: Merge logging/SOAR to save ~2 hours.

**Day 8: Security & Azure AD (~5 hours)**

* Tasks: HTTPS (AWS ACM, App Service), Azure AD SSO (MiniOrange), VPC/NSG, GuardDuty/Defender alerts.
* Deliverables: HTTPS, SSO, secure network.

**Day 9: Deep Testing Part 1 (~5 hours)**

* Tasks: Nmap scans (EC2/VM/App Service), WPScan (WordPress), IAM audit.
* Deliverables: Nmap/WPScan results, IAM findings.
* Notes: Split testing for focus.

**Day 10: Deep Testing Part 2 (~5 hours)**

* Tasks: NSG audit, OpenVAS scan (EC2/VM), apply fixes (e.g., plugins, ports).
* Deliverables: NSG findings, OpenVAS results, fixes.
* Notes: Complete testing.

**Day 11: Integration & Validation (~5 hours)**

* Tasks: Test WordPress (login, courses, API), verify SOAR alerts, check S3 sync, Splunk logs.
* Deliverables: Working portal, verified automation.

**Day 12: Documentation & Cleanup (~4 hours)**

* Tasks: Write report (~8 pages), capture screenshots (WordPress, Splunk, SOAR, Nmap), terminate resources.
* Deliverables: Report, screenshots, clean accounts.
* Notes: Compressed to fit SOAR/testing.