COMPLETE EXTERNAL PENTES

🧭 PHASE 1 – Attack Surface Validation (CRITICAL GAP)

1.1 Asset Drift & Shadow IT Detection

✔	Task	Tool
□	Compare scope vs DNS reality	`amass enum -passive -d example.com`
□	Identify forgotten hosts	`shodan search ssl:"example.com"`
□	Certificate transparency	`crt.sh` , `certspotter`
□	Old IP reuse	`whois IP → historical owners`
□	CDN bypass detection	`curl --resolve host:IP`

> This finds systems your org forgot existed (common breach vector).

🌐 PHASE 2 – DNS & Infrastructure Attacks (Often Missed)

2.1 DNS Exploitation

✔	Check
□	Subdomain takeover (CNAME dangling)
□	Zone transfer (`AXFR`)
□	DNSSEC misconfiguration
□	SPF/DKIM/DMARC enforcement
□	Wildcard DNS abuse

Tools

```
dig axfr @ns target.com
subjack -w subs.txt
dnsrecon -d target.com
```

☁️ PHASE 3 – Cloud & Edge Security (MAJOR GAP)

3.1 Cloud Edge Enumeration

✔	Task
□	AWS S3 public write/read
□	Azure Blob anonymous access
□	GCP bucket exposure
□	Cloud load balancer headers
□	IAM role assumption via metadata

Tools

```
cloud_enum.py
aws s3 ls s3://bucket --no-sign-request
curl http://169.254.169.254/
```

🔐 PHASE 4 – Authentication & Identity (CRITICAL)

4.1 Identity Attack Paths

✔	Check
□	MFA enforcement gaps
□	Password reset poisoning
□	JWT signing flaws
□	OAuth misbinding
□	Session fixation

✓	Check
□	Token reuse across apps

Burp Checks

- Change `aud`, `iss`, `exp`
- Remove signature
- Swap users
- Reuse refresh tokens

🔁 PHASE 5 – API-Specific Attacks (COMMONLY MISSED)

✓	API Vulnerability
□	BOLA / IDOR
□	Mass assignment
□	Function-level auth bypass
□	GraphQL introspection
□	Rate limit bypass
□	Object nesting abuse

Tools

```
postman
burp
graphql-voyager
nuclei -tags api
```

🧬 PHASE 6 – TLS, CRYPTO & TRUST

✓	Check
□	Weak cipher negotiation

✓	Check
□	TLS downgrade
□	Expired / rogue certs
□	Client cert bypass
□	HSTS missing

```
testssl.sh
sslscan
sslyze
```

🔗 PHASE 7 – Attack Chaining (EXPERT DIFFERENTIATOR)

> Most critical findings come from chaining low-risk issues.

Chain Example
Open S3 → config leak → JWT secret → admin takeover
Subdomain takeover → cookie scope abuse
SSRF → metadata → cloud IAM → full compromise
IDOR → password reset → account takeover

✓ Explicitly document at least one realistic attack chain

🕵️ PHASE 8 – Evasion & Realism

✓	Check
□	Rate limit evasion
□	WAF bypass techniques
□	Header mutation
□	IP rotation / user-agent control

✔	Check
□	Time-delay attacks

🧪 PHASE 9 – Zero-Day & Logic Risk Acknowledgment

You **cannot find zero-days reliably**, but you must:

✔	Task
□	Identify unmaintained software
□	Flag EOL components
□	Assess patch latency
□	Highlight “single-auth control” systems