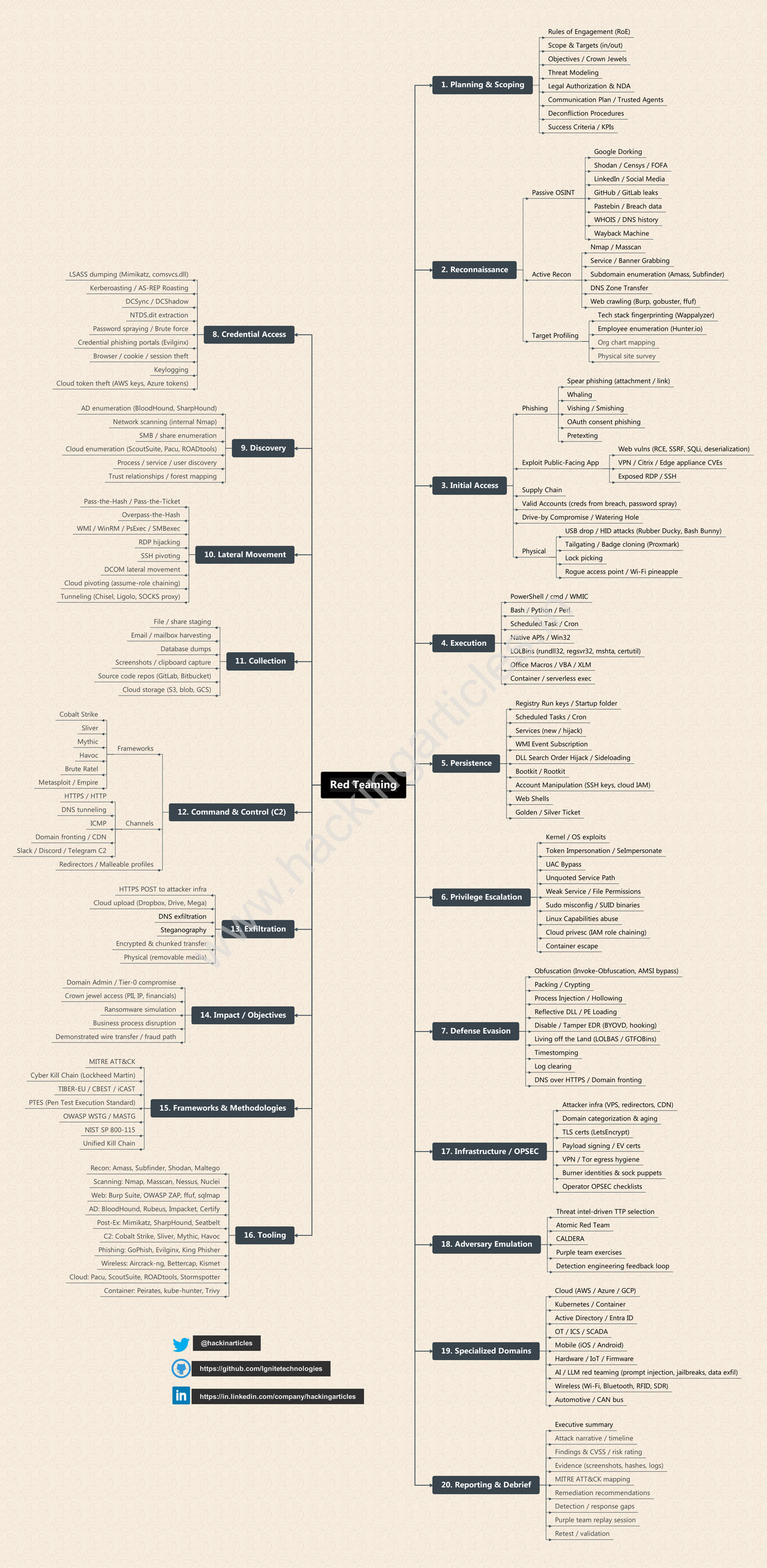

Red Teaming
1. Planning & Scoping
Rules of Engagement (RoE)
Scope & Targets (in/out)
Objectives / Crown Jewels
Threat Modeling
Legal Authorization & NDA
Communication Plan / Trusted Agents
Deconfliction Procedures
Success Criteria / KPIs
2. Reconnaissance
Passive OSINT
Google Dorking
Shodan / Censys / FOFA
LinkedIn / Social Media
GitHub / GitLab leaks
Pastebin / Breach data
WHOIS / DNS history
Wayback Machine
Active Recon
Nmap / Masscan
Service / Banner Grabbing
Subdomain enumeration (Amass, Subfinder)
DNS Zone Transfer
Web crawling (Burp, gobuster, ffuf)
Target Profiling
Tech stack fingerprinting (Wappalyzer)
Employee enumeration (Hunter.io)
Org chart mapping
Physical site survey
3. Initial Access
Phishing
Spear phishing (attachment / link)
Whaling
Vishing / Smishing
OAuth consent phishing
Pretexting
Exploit Public-Facing App
Web vulns (RCE, SSRF, SQLi, deserialization)
VPN / Citrix / Edge appliance CVEs
Exposed RDP / SSH
Supply Chain
Valid Accounts (creds from breach, password spray)
Drive-by Compromise / Watering Hole
Physical
USB drop / HID attacks (Rubber Ducky, Bash Bunny)
Tailgating / Badge cloning (Proxmark)
Lock picking
Rogue access point / Wi-Fi pineapple
4. Execution
PowerShell / cmd / WMIC
Bash / Python / Perl
Scheduled Task / Cron
Native APIs / Win32
LOLBins (rundll32, regsvr32, mshta, certutil)
Office Macros / VBA / XLM
Container / serverless exec
5. Persistence
Registry Run keys / Startup folder
Scheduled Tasks / Cron
Services (new / hijack)
WMI Event Subscription
DLL Search Order Hijack / Sideloading
Bootkit / Rootkit
Account Manipulation (SSH keys, cloud IAM)
Web Shells
Golden / Silver Ticket
6. Privilege Escalation
Kernel / OS exploits
Token Impersonation / SeImpersonate
UAC Bypass
Unquoted Service Path
Weak Service / File Permissions
Sudo misconfig / SUID binaries
Linux Capabilities abuse
Cloud privesc (IAM role chaining)
Container escape
7. Defense Evasion
Obfuscation (Invoke-Obfuscation, AMSI bypass)
Packing / Crypting
Process Injection / Hollowing
Reflective DLL / PE Loading
Disable / Tamper EDR (BYOVD, hooking)
Living off the Land (LOLBAS / GTFOBins)
Timestomping
Log clearing
DNS over HTTPS / Domain fronting
8. Credential Access
LSASS dumping (Mimikatz, comsvcs.dll)
Kerberoasting / AS-REP Roasting
DCSync / DCShadow
NTDS.dit extraction
Password spraying / Brute force
Credential phishing portals (Evilginx)
Browser / cookie / session theft
Keylogging
Cloud token theft (AWS keys, Azure tokens)
9. Discovery
AD enumeration (BloodHound, SharpHound)
Network scanning (internal Nmap)
SMB / share enumeration
Cloud enumeration (ScoutSuite, Pacu, ROADtools)
Process / service / user discovery
Trust relationships / forest mapping
10. Lateral Movement
Pass-the-Hash / Pass-the-Ticket
Overpass-the-Hash
WMI / WinRM / PsExec / SMBexec
RDP hijacking
SSH pivoting
DCOM lateral movement
Cloud pivoting (assume-role chaining)
Tunneling (Chisel, Ligolo, SOCKS proxy)
11. Collection
File / share staging
Email / mailbox harvesting
Database dumps
Screenshots / clipboard capture
Source code repos (GitLab, Bitbucket)
Cloud storage (S3, blob, GCS)
12. Command & Control (C2)
Frameworks
Cobalt Strike
Sliver
Mythic
Havoc
Brute Ratel
Metasploit / Empire
Channels
HTTPS / HTTP
DNS tunneling
ICMP
Domain fronting / CDN
Slack / Discord / Telegram C2
Redirectors / Malleable profiles
13. Exfiltration
HTTPS POST to attacker infra
Cloud upload (Dropbox, Drive, Mega)
DNS exfiltration
Steganography
Encrypted & chunked transfer
Physical (removable media)
14. Impact / Objectives
Domain Admin / Tier-0 compromise
Crown jewel access (PII, IP, financials)
Ransomware simulation
Business process disruption
Demonstrated wire transfer / fraud path
15. Frameworks & Methodologies
MITRE ATT&CK
Cyber Kill Chain (Lockheed Martin)
TIBER-EU / CBEST / iCAST
PTES (Pen Test Execution Standard)
OWASP WSTG / MASTG
NIST SP 800-115
Unified Kill Chain
16. Tooling
Recon: Amass, Subfinder, Shodan, Maltego
Scanning: Nmap, Masscan, Nessus, Nuclei
Web: Burp Suite, OWASP ZAP, ffuf, sqlmap
AD: BloodHound, Rubeus, Impacket, Certify
Post-Ex: Mimikatz, SharpHound, Seatbelt
C2: Cobalt Strike, Sliver, Mythic, Havoc
Phishing: GoPhish, Evilginx, King Phisher
Wireless: Aircrack-ng, Bettercap, Kismet
Cloud: Pacu, ScoutSuite, ROADtools, Stormspotter
Container: Peirates, kube-hunter, Trivy
17. Infrastructure / OPSEC
Attacker infra (VPS, redirectors, CDN)
Domain categorization & aging
TLS certs (LetsEncrypt)
Payload signing / EV certs
VPN / Tor egress hygiene
Burner identities & sock puppets
Operator OPSEC checklists
18. Adversary Emulation
Threat intel-driven TTP selection
Atomic Red Team
CALDERA
Purple team exercises
Detection engineering feedback loop
19. Specialized Domains
Cloud (AWS / Azure / GCP)
Kubernetes / Container
Active Directory / Entra ID
OT / ICS / SCADA
Mobile (iOS / Android)
Hardware / IoT / Firmware
AI / LLM red teaming (prompt injection, jailbreaks, data exfil)
Wireless (Wi-Fi, Bluetooth, RFID, SDR)
Automotive / CAN bus
20. Reporting & Debrief
Executive summary
Attack narrative / timeline
Findings & CVSS / risk rating
Evidence (screenshots, hashes, logs)
MITRE ATT&CK mapping
Remediation recommendations
Detection / response gaps
Purple team replay session
Retest / validation
@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles
www.hackingarticles.in