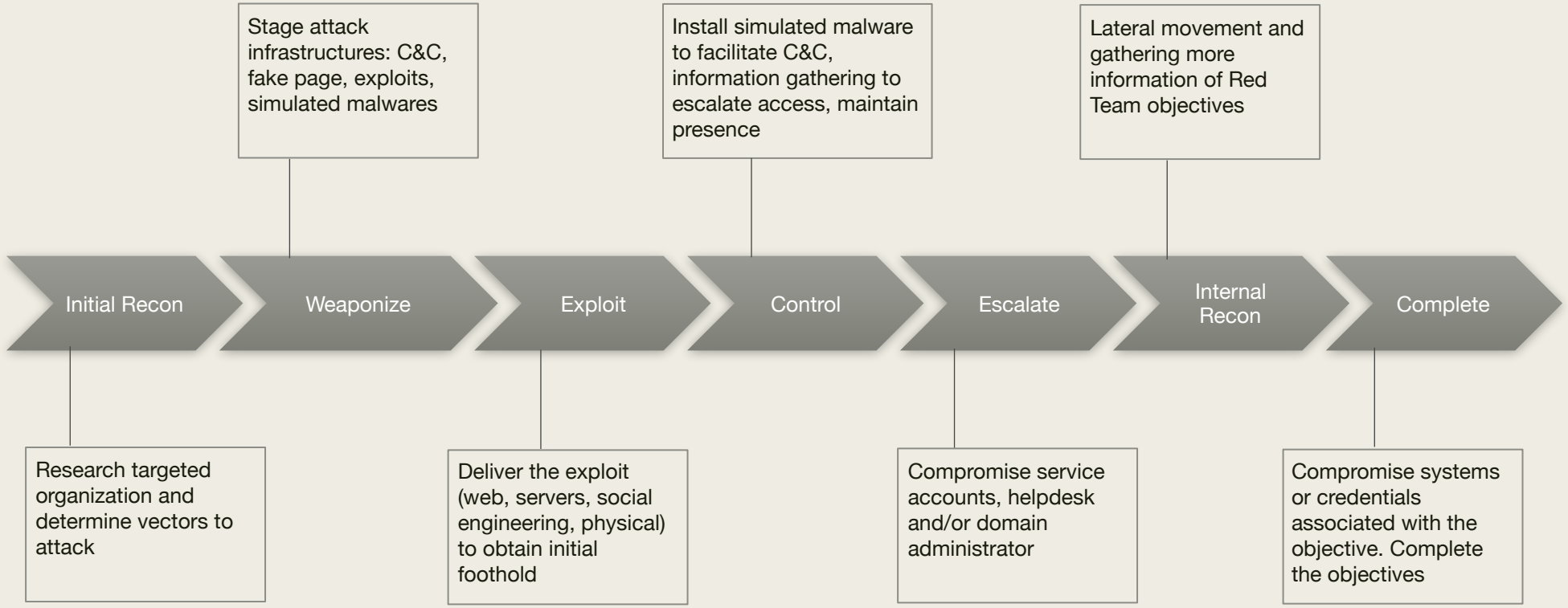
RED TEAMING: EMULATING ADVANCED ADVERSARIES IN CYBERSPACE

CDEF meetup 4th - Atik Pilihanto

Red Team Phases = Attack Kill Chains



Initial Recon

- Lets start with researching the targeted organization and determining vectors to attack.
- Employee names, employee emails, employee phone numbers, employee roles, screenshot of employee's computers (e.g., social media, search engine, hunter.io)
- Recent company events (e.g., official company website)
- Disclosed credentials in breaches (e.g., your own private repo!, pwnedlist?) – crack and/or utilize these credentials
- Intentionally/unintentionally published corporate application source codes (e.g., github)
- Network blocks, domains, subdomains, IP addresses, exposed ports, web applications (e.g., shodanhq, censysio, census_2012, whois, robtex and so forth)
- Some activities can be scripted – Recon-ng, theharvester, EyeWitness, SpiderFoot, Maltego, etc
- How's about advanced adversaries?

Weaponize

- Now you have the target detail, continue to stage attack infrastructures: C&C, fake page, exploits, simulated malwares!
- C&C Infra to receive command & control traffic after compromise
  - *Commonly used: HTTP, DNS, HTTPS (preferable, do not used default cert)*
  - *Simple redirector (e.g., iptables NAT), reverse proxy, domain fronting (AWS, Azure, etc)*
  - *Domain vs IP – categorized expired domain (e.g., expired domains in education) – CatMyFish, expireddommains.net, sitereview.bluecoat.com*
  - *Determine your malleable-c2 profile*
  - *Twitter, Gmail (e.g., twittor, gcat, gdog), etc*
- Fake web page to host social engineering stuffs
  - *Domains – convincing domain name vs punycode vs categorized expired domain*
  - *To host a website to harvest credentials*
  - *To host payloads – HTA, ClickOnce, macro-enabled document/sheet, DDE document/sheet, malicious JAR, malicious applet etc – sometime victims even voluntarily opening password-protected document.*
  - *Obfuscate payload? (e.g., HTA obfuscation – demiguise nccgroup, morphHTA)*
- Exploits and simulated malwares
  - *The exploit used to deliver attacks e.g., weaponized macro-enabled document, web page equipped with HTA, etc*
  - *Simulated malware – as the 2nd stage malware*
    - Commonly used during a red team engagement – veiled metasploit payload, Empire, cobaltstrike
- How's about advanced adversaries?

Exploit

- We have everything ready, now deliver the exploit (public applications, public servers, social engineering, physical) to obtain initial foothold
- Public servers vulnerabilities – e.g. default password in administrative services, RCE to compromise the server
- Web application vulnerabilities – e.g. SQL injection with DBA privilege, OS command injection
- OK – those two vulnerabilities above seem to not make sense in mature cyber environment, but sometime being a shortcut
- Social Engineering: most commonly used by adversaries is email – email vs phone?
  - *Harvesting credentials – email must reach victim mailbox – bypass mail gateway, sandboxing, isolation – Web to harvest credential must bypass proxy (web filtering), sandboxing, isolation – victim must be convinced enough.*
    - Credential harvested: Email, VPN, Citrix, or?
    - How's about 2FA? (e.g., soft token with seed file, such as .sdtid file)
    - How's about endpoint checker to join VPN? (see here for example: http://kolbi.cz/blog/?p=114)
  - *Remote Code Execution – email must reach victim mailbox (attach or URL?) – bypass mail gateway, sandboxing, isolation – victim must be convinced enough to follow – the RCE payload should be able to bypass endpoint protection – even after bypassing EPP/EDR the C&C traffic must be able to bypass network/web filtering*
  - *0day exploits during engagement? Depends on how you defined 0day – but most likely doesn't make any sense. Well, even a 0day must be able to bypass all those mentioned perimeters otherwise you just gave away your 0day to another security vendor*
- In case remote attacks failure? Some made a hype of break-in physically. Ok, attempts to break in physically VS Simulated compromise (insider involvement)
- How's about advanced adversaries?

Control

- Now you have the network access either through VPN or the RCE. Now, aim to install the simulated malware (if you haven't) to facilitate C&C, maintain presence, and information gathering to escalate access.
- Your initial compromise is a Windows or Non-Windows? Is the system in the domain or no? – most of the cases, social engineering victims were Windows & joined to the domain.
- OK, we'll focus with an initial compromise on a Windows workstation joined to the Windows domain – which is most of the case in a corporate network, other scenarios? Let's have another session.
- Simulated malware: to runs only on memory or drop a file to hard drive?
- How to be persistence? Autorun registries, schedule task, windows services, etc?
- Exploring the first compromised machine – processes, endpoint protections, local users, local group, group memberships, etc?
  - *If any high privileged domain users ever logged in? Event Log ID 4624, C:\Users*
- Start exploring the windows domain: domain users, domain groups, hosts joined to the domain, trust relation between domain/forest, membership of sensitive groups, etc?
- Some tools to help: Windows CLI (such as net, tasklist, etc), PowerSploit, BloodHound, PS Get-EventLog, CobaltStrike aggressor script
- Tools to help evading detection: Invoke-DOSfucation, Invoke-Obfucation, Invoke-CradleCrafter
- Post compromise, be careful with "big name" MSSP
- How's about advanced adversaries?

Escalate

- Now we have information about the network, Lets escalate - Compromise service accounts, helpdesk and/or domain administrator
- Local Escalation VS Domain Escalation?
- Local Escalation
  - *In some cases local escalation is not necessary – minimize risk being detected.*
  - *Escalation required to dump credentials e.g., mimikatz*
- Domain Escalation
  - *MS14-025 Group Policy Preference Password – vulnerability against KB2962486*
  - *MS14-068 Kerberos Vulnerability – vulnerability against KB3011780*
  - *Kerberoasting – requires an event with ID 4769*
  - *SQL server with weak password*
  - *File/folder sharing*
  - *Vulnerable JBOSS, Windows Exploit such as ms17-010, ms10-061, ms08-067*
  - *Local Administrator Pivot (WMI/psexec/WinRM,DCOM) (if Red Team has possession to privileged user) – Obfuscated Mimikatz*
- Once domain admin compromised, collect all domain admins' username & password, obtain plaintext or crack the NTLM hash
- Some tools to help: PowerSploit (e.g., PowerView Get-GPPPassword, Invoke-FileFinder; PowerUp Allchecks), PowerUpSQL, Invoke-AutoKerberoast, Mimikatz, Proxychains, Jboss scanner, metasploit
- How's about advanced adversaries?

Internal Recon

- Now you have the key to the kingdom! Lets look for the target objectives, key person managed those systems, lateral movement and gathering more information.
- The objective can be within the domain but on a strictly filtered network segment. The objective system is also possibly outside the domain/different domain on a strictly filtered network segment.
  - *Intranet portal such as Sharepoint, Jira, Wiki? (if any) – this can be a gold mine to look for the target*
  - *Who's responsible for the target systems?*
  - *What process is likely associated?*
  - *Determine whether or not there's "jump host" servers?*
  - *What is the systems (e.g., Unix, Linux, Mainframe, Web App, etc)*
  - *File/folder sharing associated with systems of interest*
- Lateral movement to systems of interest using privileged accounts that has been compromised during escalation (WMI/WinRM/DCOM/psexec) – e.g., workstation of employee who is responsible to target systems, compromise "jump host" servers, etc
- Some tools to help: Proxychains, PowerSploit PowerView (e.g., Invoke-UserHunter, Invoke-ProcessHunter, Invoke-FileFinder), Invoke-SessionGopher, Key Logger, BrowserGather.ps1
- How's about advanced adversaries?

Complete

- Once the target has been determined and credentials have been obtained, complete missions of the Red Team e.g.,:
  - *Access the system or web application*
  - *Doing certain transactions, modify configuration, add admin users, or financial transactions*
  - *Exfiltrate data or information*
- Some obstacles:
  - *DLP?*
  - *2FA?*
  - *etc*