Intelligence Gathering

Max, Johannes

Team 1
20.04.2015

Outline

1. Motivation
2. Typen der Informationsbeschaffung
3. Technische Systeme
4. Personen / Firmen
5. Gegenmaßnahmen

Motivation

- Überblick über ein Ziel
- Identifikation von Angriffspunkten
- Ausarbeitung eines Plans für das weitere Vorgehen

Informationssammlung: Typen

- Aktivität
  1. Passiv: kein direkter Kontakt mit dem Ziel
  2. Semi-passiv: gewöhnlicher Kontakt mit dem Ziel, keine Unterscheidung zu alltäglichem Traffic
  3. Aktiv: gezielte Anfragen an das Ziel

- Disziplinen

Informationssammlung: Typen

- Aktivität
- Disziplinen
  1. HUMINT: Personen
  2. OSINT: offene Quellen (Dokumente, Records, Webseiten, …)
  3. COMINT: Kommunikation
  4. ...

(Begriffe aus Geheimdiensten)

Technische Systeme

Hosts finden

Hosts und IP-Bereiche einer Organisation ermitteln

- DNS-Abfrage bekannter Domainnamen (semi-passiv)
- Überprüfen, ob Organisation eigene autonome Systeme hat (passiv)
- Whois-Abfrage der IP-Adressen -> IP-Range (Hoster oder eigene IP-Range) (passiv)
- Subject Alternative Names in SSL-Zertifikaten (semi-passiv)
- Shodan (Suche nach Geräten im Internet)

Hosts finden (aktiv)

- Scannen aller Reverse DNS Einträge in IP-Bereich
- Ausprobieren geläufiger Subdomains, Brute force
- Pingscan des kompletten IP-Bereich
- Zone Transfer

Informationen über Host

- Normaler HTTP-Request (semi-passiv)
  - Header können einiges verraten
    - *Server, X-Powered-By*
  - Webserver - Name und Version
  - Linux-Distribution/Version, PHP-Version, OpenSSL-Version, ...
- *nmap -O* (aktiv)
  - OS-Detection von nmap (funktioniert manchmal)

Informationen über Dienste

- Portscan
- *nmap -A*
  - Führt eine Vielzahl von Erkennungen aus
  - OS Detection, Version detection, Zertifikate, Traceroute, …
  - Pager benutzen
  - *nmap -sC* (schneller, keine OS Detection)

Demo

nmap

Web-Anwendungen finden

- robots.txt
- sitemap.xml
- Directory Indexes
- Ausprobieren von Standard-URLs (/wp-admin, /webmail, …)
- Entwicklertools: typische Seitenstruktur, nachgeladene Scripts

Web-Anwendungen finden

Built-With:

- als Plugin für Chrome und Firefox
- zeigt verwendete Technologien an: Server, Versionen, PHP/Python/Ruby etc., Hostingprovider, Document Standards, CMS, Frameworks, Encoding, Protokolle, …
- Statistiken über globale Verwendung der Technologien

Demo

Built-With

Personen / Firmen

PGP-Keys

- Zuordnung Name <-> Mail-Adressen
- Öffentlich zugänglich über Keyserver
- automatisiert auswertbar
- sehr guter Einstiegspunkt

Organsization Chart

- weitere E-Mail-Adressen durch Google
- Angaben auf Webseiten
- Aufbau eines Graphen über Firmenstruktur: Mitarbeiter, Angriffspunkte, …
- Social Engineering: Anruf bei der Firma, Bekannte fragen, ...

Social Media

- ausgehend von bekannten Namen
- Struktur / interne Vernetzung
- möglicherweise sensible Daten (Druckmittel, Hebelpunkte, …)
- relativ anonyme Kontaktaufnahme zu Mitarbeitern möglich

Physikalische Angriffspunkte

- Zutritt zur Firma / Haus unter Vorwand
- Installation von Keyloggern, Kameras, Trojanern, …
- Spionage von Passwörtern und/oder Firmeninterna
- Verhaltensmuster

Social Engineering

- Bei nichtsahnenden Mitarbeitern unter Vorwand Informationen erlangen
- Anruf, als Admin ausgeben
- Bitte um Aufruf einer präparierten Webseite

Automatisiertes Vorgehen

- Informationsbeschaffung über Personen teilweise automatisiert möglich
- Beispiel eines solchen Tools: Maltego
- Darstellung von Wissen als Graph, Erweiterung und Suche durch bestimmte Transformationen

Demo

Maltego

Gegenmaßnahmen

gegen Netzwerkidentifikation

- ✓ DNS Zone Transfers deaktivieren
- ✓ ICMP filtern?
- ✓ kein RST-Paket, DROP bei geschlossenen Ports
- ✓ Firewall (internes Netz nicht ans Internet hängen)

gegen Netzwerkidentifikation

- ✓ Whois-Privacy
- ✓ eigene SSL-Zertifikate für einzelne Webseiten
- ✓ Banner abschalten soweit möglich
- ✓ Infrastrukturdienste (SSH, …) auf alternative Ports legen

gegen Webseitenidentifikation

- ✓ Serversignatur deaktivieren
- ✓ Apache:

  ServerSignature Off

  ServerTokens Prod
- ✓ nginx:

  server_tags Off;
- ✓ PHP (php.ini):

  expose_php = Off

gegen menschliches Versagen

- ✓ misstrauisch sein!
- ✓ Mitarbeiter schulen, sensible Daten nicht direkt herauszugeben
- ✓ technische Kontrolle (Logfiles, Zugriffsrechte, …)
- ✓ E-Mail-Adressen verschleiern (kein Klartext auf der Webseite)

gegen physikalische Angriffe

- ✓ Offline-Security
- ✓ BIOS-Einstellungen setzen, sodass neuer Hardware nicht vertraut wird
- ✓ Passwörter verdeckt eingeben
- ✓ besser Public-Key-Krypto verwenden
- ✓ aber: sehr schwer zu verhindern...

Literatur und Quellen

http://nmap.org/book/

http://www.pentest-standard.org/index.php/Intelligence_Gathering

http://tools.kali.org/tools-listing

Danke für die Aufmerksamkeit!