Module 5: Ethical hacking

Roy Prins
Principal Systems Architect, Salesforce

Agenda

- Wat is Ethical Hacking
- Statistieken
- Terminologie
- Impact
- Aanpak en werkwijzes
- Ethiek

Ethical Hacking

- Een ethical hacker is iemand die lekken, kwetsbaarheden en beveiligingsproblemen opspoort in infrastructuur, systemen, en applicaties
- Opsporen gebeurt meestal middels penetratie testen
- Gebeurt veelal in opdracht van bedrijven zelf
- Het doel is altijd hetzelfde: verbeteren van IT-security
- Eventuele gevonden kwetsbaarheden worden alleen bekend gemaakt aan opdrachtgever

Statistieken en wetenswaardigheden

- Elke 39 seconden vindt een hack aanval plaats
- Elke dag worden 300.000(!) nieuwe malware gemaakt
- In januari 2022 was Nederland het grootste doel voor phishing aanvallen, gevolgd door Rusland, Moldavie en de VS.
- Elke dag vinden meer dan 4000 ransomware aanvallen plaats
- Cybersecurity budget van de US overheid is 14,98 miljard USD
- Mensen en machines gebruiken meer dan 300.000 wachtwoorden
- 45% van alle data lekken betreft cloud systemen
- Phishing is de meest gerapporteerde vorm van cybercrime, gevolgd door non-payment/non-delivery (bv Marktplaats oplichting)
- De top-5 meest gebruikte bedrijfsnamen bij phishing zijn LinkedIn, Microsoft, DHL, Amazon, Apple

Terminologie

- Black hat hacker: ervaren hacker met criminele bedoelingen, bv stelen van data, geld, crypto's, aanrichten van schade of verspreiden van malware of ransomware.
- White hat hacker: ethical hacker die opereert binnen de grenzen van de wet, vaak in samenwerking met grote bedrijven, om beveiligingslekken te vinden om deze te dichten.
- Grey hat hacker: zelfstandig opererende hacker die kwetsbaarheden opspoort en deze voor een beloning kenbaar maakt bij het betreffende bedrijf
- Script kiddie: veelal jong en onervaren persoon die gebruik maakt van kant-en-klare tools om schade aan te richten uit baldadigheid. Overziet meestal niet de gevolgen.

Welke skills/kennis heb je nodig?

- Programmeren, scripting
  - C/C++, BASH, Python, Go, Rust
- Netwerken en telecommunicatie
  - Protocollen, beveiliging, TCP, UDP, packages
- Bestandsformaten
  - XML, JSON,PDF, Word, Edifacts
- Infrastructuur
  - CloudNative, AWS, GCP, Azure, Infrastructure-as-code
- Databases
  - SQL, RDBMS, Oracle, MySQL, Postgres
- Besturingssystemen
  - Windows, Linux, MacOS

Hoe gaat een hack in z'n werk?

- Een hack is vaak een langdurig process van meerdere weken of zelfs maanden
- Meestal bestaat een hack uit 5 fases
  1. Observatie
  2. Analyse/strategie bepalen
  3. Voorbereiding
  4. Uitvoering
  5. Opruimen, evaluatie

Welke tools/producten gebruikt een hacker?

- Linux
- Decompilers
- Debuggers
- Sniffers
- Spoofers
- Programmeertalen

Thank you