Money for Nothing... and Bits4free

8.8.2011

Gilbert Wondracek, gilbert@iseclab.org

Hacker & Co

- Begriff hat je nach Kontext andere Bedeutung, Ursprung: 50er Jahre, MIT
  - Ausnutzen von Funktionalität die vom Erfinder nicht gedacht war (wertungsfrei)
  - Software & Hardware
- In den Medien heute zumeist negativ besetzt
  - Datendiebstahl, Computersabotage,...
- Was motiviert verschiedene „Hacker“?

Motivation

- Hacktivism
  - HACKing + acTIVISM
  - Politisch motiviert, typisch ist eine ideologische Nachricht und großer Geltungsdrang
  - Defacement als Klassiker (Vandalismus auf einer Website)
- Cybercrime
  - Ausnutzen von Schwachstellen um Verbrechen zu begehen, finanzielle Motivation
  - Botnets, Malware (Würmer & Co.)

Motivation

- Cyber-warfare, Wirtschaftsspionage
  - Kritische Infrastruktursysteme sind computergesteuert und mit Netzwerken verbunden
  - Prominentes Beispiel: Stuxnet
- Ethical Hacking
  - (Vielleicht) die Guten
  - Schwachstellen werden den Opfern aufgezeigt ohne Schaden zu verursachen

Motivation

- Penetration Testing
  - Ziemlich sicher die Guten :-)
  - Ethical Hacking im Unternehmenskontext, Überprüfen von Sicherheitsstandards
  - Rechtliche Basis, PTA, ROE, ...

Aktuelle Beispiele

- Anonymous
  - Musikindustrie, VISA
  - GIS, FPÖ, Grüne (?), SPÖ, ...
- LulzSec
  - Sony, CIA (dann aufgelöst :-)
- AntiSec
  - Kreuzzug gegen Securityindustrie
- Wikileaks
  - Whistleblowing

Kommunikation

- Effektive Kommunikation erlaubt umfangreichere Angriffe, Synergien,...
- Früher: Einzelne Hacker oder kleine Gruppen
- Heute: Kein Realkontakt, Kommunikation und Koordination über Websites, „Kollektive“ ohne offensichtliche Hierarchie
  - Twitter, Facebook, 4chan, pastebin, einschlägige (gekaperte) Foren …
  - Trend zu Non-Hacker Websites und Services (Untertauchen in der Masse)

Beispiele

- http://twitter.com/#!/anonaustria
- http://twitter.com/#!/lulzsec
- http://www.zone-h.org/archive/notifier=BriscO-Dz
- http://forum.freelanceswitch.com/topic.php?id=11748
- Dropzone für Keylogger, z.B. pastebin

Hacking Phasen

- Klassische Vorgangsweise
  1. Reconnaissance „Aufklärung“
  2. Scanning
  3. Gain Access
  4. Maintain Access
  5. Cover Tracks

Technische Hintergründe

- Im Prinzip geht es um das Ausnutzen von Schwachstellen in Software oder Hardware
- Security wird oft vernachlässigt, „nicht sichtbar“
  - Kostet Geld, bringt nichts tangibles → Bis etwas passiert
- Die gleichen Arten von Schwachstellen werden von Generationen von Entwicklern und Ingenieuren wiederholt
  - Googlen: OWASP Top 10

Technische Hintergründe

- Zwei Beispiele für häufige Lücken im Web
  - Cross Site Scripting (XSS)
  - SQL Injection
- Prinzip:
  - In der Website oder dem Programm werden Eingaben des Users verarbeitet
  - z.B. Suche nach einem Begriff, Einloggen für bestimmten Usernamen
  - Über die Usereingaben kann der Angreifer das Programm in seiner Ausführung beeinflussen

Cross Site Scripting

- Cross Site Scripting
- Typische Schwachstelle in HTML Code

```
http://example.com?suchbegriff=blabla

…

Suchergebnisse:<br>

Leider konnte zu dem Begriff<b>[TOKEN]</b> kein
Ergebnis gefunden werden

…
```

- Was passiert, wenn man HTML Code als Suchbegriff eingibt?

Cross Site Scripting

- Ungefilterte Usereingaben sind eine Sicherheitslücke
- Kann für Defacements oder Phishing verwendet werden
- Sehr viele Websites betroffen

- Demo

SQL Injection

- SQL ist die Sprache mit der man innerhalb von Programmen auf Datenbanken zugreifen kann

```
SELECT id, bild FROM users WHERE
name="[TOKEN]";
```

- Wieder: Userinput ungefiltert verwendet
- Angriff:

```
SELECT id, bild FROM users WHERE

name="asd" OR "1"="1";
```

- Dürfte z.B. auch bei den Hacks auf FPÖ und SPÖ verwendet worden sein

SQL Injection

- Erlaubt dem Angreifer Datendiebstahl, Hochladen von Dateien (c99 Shell), Kontrolle über System,...
- An sich kann man sich dagegen recht gut verteidigen → Filtern
- Wird aber oft schlampig oder gar nicht umgesetzt
- Kann mit Softwaretools automatisch und ohne Detailwissen gegen hunderte Websites eingesetzt werden
- Demo

Technische Hintergründe

- Wirkt mühsam und schwierig... oder?
- Cheat Sheets → Online Sammlungen mit gängigen Angriffen
  - Abschreiben reicht leider oft schon aus
- Automatisierte Tools
  - SQLMap, Metasploit, …
  - Frei verfügbar
  - Expertenwissen in den Tools
  - User muss oft nur noch Ziel (URL) angeben

Ziele finden

- Wie findet man etwas im Netz?
- Genau!
  - Google & Co.
- Demo

Fazit

- Man muss *kein* Computergenie sein um eine Website zu hacken
- Viele Systeme sind geradezu fahrlässig programmiert
- Neue Kommunikationsmethoden erlauben schnelle Organisation und Informationsaustausch für Hacker
- Politische Motivation => sichtbar
- Finanzielle Motivation => versteckt

Vielen Dank!
Fragen?

Danke an SBA Research gGmbh
http://www.sba-research.org/