Penetrationstests mit Metasploit

Michael Kohl

Linuxwochenende 2011

24 September 2011

Outline

Über mich

- Früher: Linux/Unix Admin / Systems Engineer
- Jetzt: Rails-Entwickler, DevOps
- Ab Oktober: Penetration Tester
- Gentoo Entwickler, Metalab, RubyLearning, etc.

Warum Penetration Testing?

- Schwachstellen identifizieren
- Aufdecken von Fehlern aus falscher Bedienung
- Erhöhung der Sicherheit auf technischer und organisatorischer Ebene
- externe Validierung der Sicherheit

Pre-Engagement

- Zieldefinition (z.B. compliance)
- Abklären der Rahmenbedingungen (z.B. overt/covert)
- Limitierungen (z.B. nur Kernarbeitszeit, Wochenenden)
- Umfang (Netzwerk, Apps, WLAN, physische Tests, Social Engineering)
- Kommunikationswege definieren

Intelligence Gathering

- Versuch möglichst viel über Ziel herauszufinden
- Social Media
- Footprinting
- Portscans
- Firewalls etc?
- physische Locations

Threat Modeling

- benutzt Informationen aus dem vorherigen Schritt
- Versuch vielversprechendsten Angriffsvektor zu finden
- in die Rolle des Angreifers versetzen
  - Analyse von Assets
  - Analyse der Geschäftsprozesse
  - Unternehmenstruktur
  - Attacken auf ähnliche Unternehmen

Vulnerability Analysis

- Port- und Service-Scans
- Banner Grabbing
- SQL Injection Scanner
- Traffic Monitoring

Exploitation

- "spektakulärste" Phase
- nach Indentifikation der vielversprechenden Vektoren
- Exploits für bekannte Versionen
- Buffer Overflows, SQL Injections, Passwort Bruteforce etc.

Post Exploitation

- nach dem Kompromittieren eines oder mehrerer Systeme
- Identifikation wichtiger Infrastruktur
- Identifikation wichtigster Daten
- Schwachstellen mit grösstem Business Impact
- Aufräumen

Reporting

- wichtigster Teil
- was?
- wie?
- wie reparieren?
- generelle Security, nicht nur technische Schwachstellen

Metasploit Framework

- Penetration Testing Framework in Ruby
- Scanner/Fuzzer
- Payloads
- Exploits
- Post-Exploitation Tools (Meterpreter)
- Libraries zur Entwicklung eigener Tools

Demo

- Metasploitable VM
- prinzipieller Ablauf, kein vollständiger Pen Test

Ressourcen

- http://de.wikipedia.org/wiki/Penetrationstest_(Informatik)
- http://www.pentest-standard.org/index.php/Main_Page
- http://www.metasploit.com/
- http://www.offensive-security.com/metasploit-unleashed/
- http://nostarch.com/metasploit
- http://www.offensive-security.com/metasploit-unleashed/Metasploitable