WMAP – Metasploit 3.2 Module für Pentester von Webapplikationen

Hans-Martin Münch
it.sec GmbH & Co KG
mmuench@it-sec.de

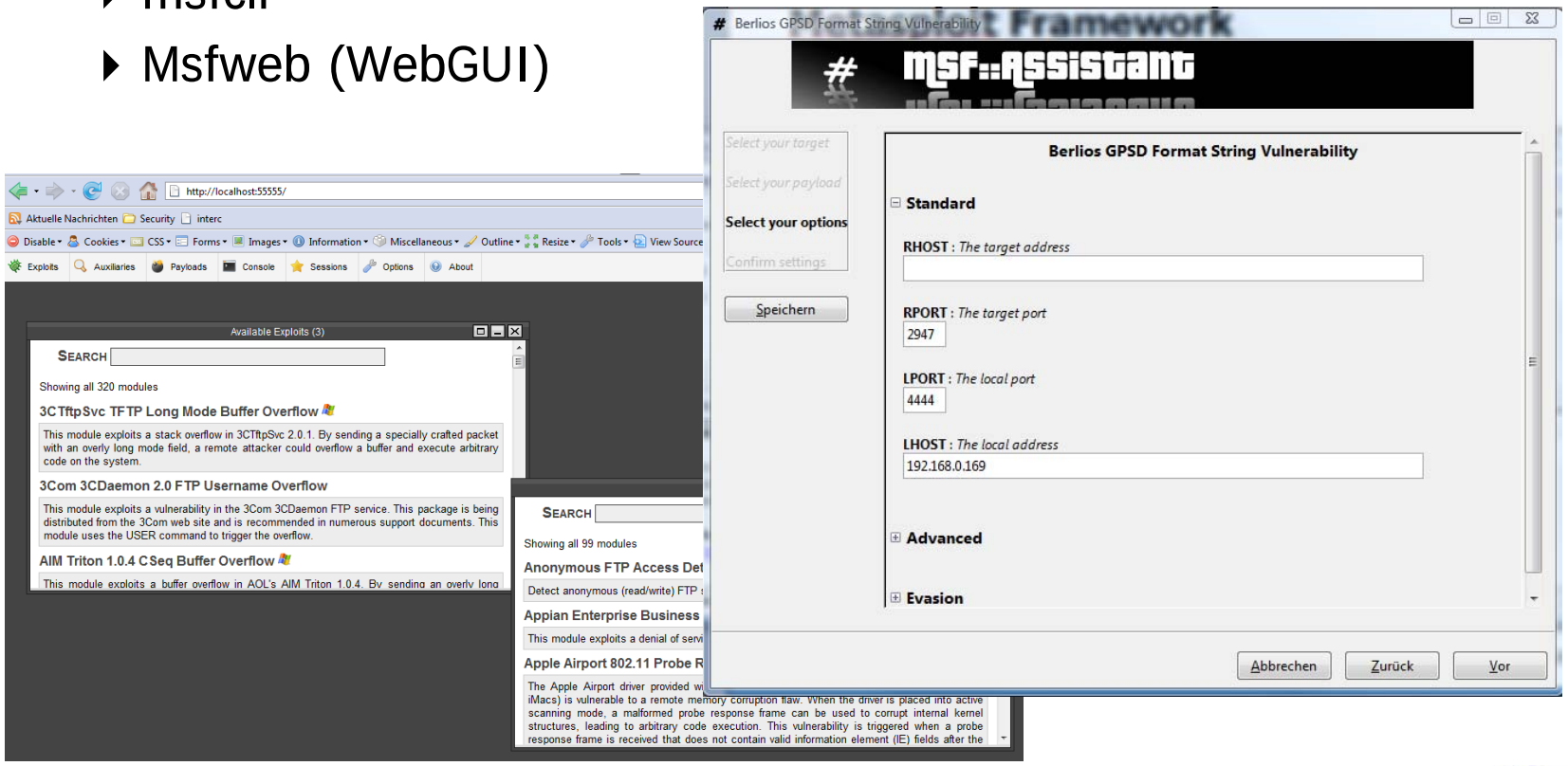
OWASP
Frankfurt, 25.11.08

Metasploit Framework

- Framework zur Entwicklung und Anwendung von Exploits
- Momentan 302 Exploits, 156 Payloads
  - ms08_067, Apache mod_jk...
  - Exploits sind parametrisierbar
  - Kombination von Exploits mit unterschiedlichen Payloads
- „Auxilary“ Module
  - Keine Exploits, jedoch Tools, die bei einem Penetrationstest nützlich sind
  - Implementierung von DoS Angriffen
  - Scanner (anonymous Login FTP Server)
  - Ebenfalls parametrierbar

Metasploit Framework

- Verschiedene Interfaces
  - msfconsole (DOS ähnliche Konsole)
  - msfcli
  - Msfweb (WebGUI)



Metasploit Framework

- Einfach erweiterbar
  - Scriptsprache Ruby
  - Modularer, klar strukturierter Aufbau
  - Eigene Protokoll Bibliotheken (WebClient, FTPClient, SMB)
  - Plugin Schnittstelle
    - Anbindung an Datenbank
    - Erweiterung mit eigenen Befehlen
- Großteil Infrastrukturebene
  - Einzelne Webapplikationen (Cacti, AwStats)
  - Browser Exploits

Metasploit Version 3.2

- Release Date: 19. November 2008
  - Viele Neuerungen (Karmetasploit, IPv6 usw.)
- Interessant für Webapplikationen
  - PHP Payloads
  - WMAP

Was ist WMAP ? (1/3)

- Websecurity Scanner, vergleichbar mit
  - „Paros“
  - „Grendel-Scan“
  - „W3AF“
- Gleiche Einschränkungen
- Noch ein Scanner?
  - Personen die sich sowieso mit Metasploit beschäftigen
  - Script - Autoren

Was ist WMAP ? (2/3)

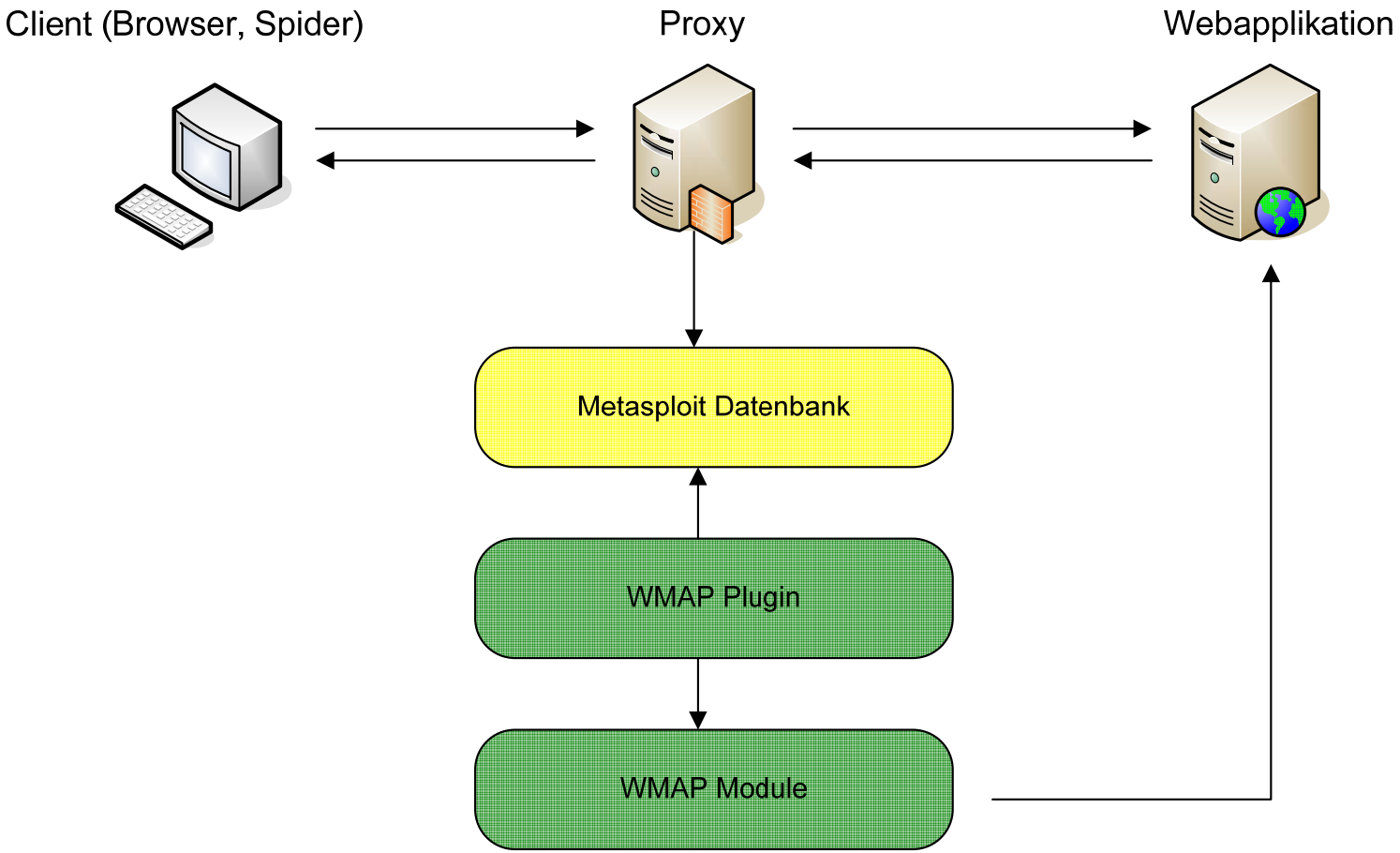
- Sammlung von Auxiliary Modulen
  - Direkter Aufruf per Konsole bzw. Kommandozeile möglich

```
msf > use scanner/http/wmap_backup_file

msf auxiliary(wmap_backup_file) > set RHOSTS 192.168.8.40
RHOSTS => 192.168.8.40
msf auxiliary(wmap_backup_file) > set PATH /index.php
PATH => /index.php
msf auxiliary(wmap_backup_file) > run

[*] NOT Found http://192.168.8.40:80/index.php.backup
[*] NOT Found http://192.168.8.40:80/index.php.bak
[*] NOT Found http://192.168.8.40:80/index.php.copy
[*] NOT Found http://192.168.8.40:80/index.php~
[*] NOT Found http://192.168.8.40:80/.index.php.swp
[*] Auxiliary module execution completed
```

Was ist WMAP ? (3/3)

- Datenbank Backend
- Proxy zur Befüllung der Metasploit DB
- Datenbank Plugin
  - Aufruf der WMAP Module mit Werten aus dem Datenbank-Backend

WMAP - Ablauf


Client (Browser, Spider)
Proxy
Webapplikation
Metasploit Datenbank
WMAP Plugin
WMAP Module

WMAP Datenbank Plugin

- Muss extra geladen werden („load db_wmap“)
- Stellt Befehle zur Kommunikation mit der Datenbank zur Verfügung
  - Auswahl des Ziels (“wmap_target”)
  - Auslesen der Webseiten Struktur (“wmap_website”)
  - Start der Module (“wmap_run”)
  - Ausgabe eines Reports (“wmap_report”)

WMAP Module (1/2)

- Bereits existierende Module
  - wmap_dir_scanner
  - wmap_sql_map
  - wmap_blind_sql_query
  - wmap_vhosts_scanner
  - wmap_backup_files
  - wmap_verb_auth_bypass
  - ...

WMAP Module (2/2)

- Mixin “Auxilary::WMAPModule”
- Wird verwendet von
  - Auxilary::WMAPScanServer
  - Auxilary::WMAPScanDir
  - Auxilary::WMAPScanFile
  - Auxilary::WMAPScanUniqueQuery
  - Auxilary::WMAPGeneric
  - ...
- Definieren Methode “wmap_type”
- Definiert wo das Modul bei der Ausführung von “wmap_run” überall gestartet wird

Reporting

- Speicherung in SQL Datenbank
- Ausgabe mittels „wmap_report“
- Prinzip: Name, Typ, Wert
- Baumstruktur über “parent_id”

	id	target_id	parent_id	entity	etype	value	notes	source	created
1	1	-619791618	0	WMAP	REPORT	127.0.0.1,80,0	Metasploit WMAP	WMAP Scanner	2008-11-23 20:
2	2	-619266038	0	WMAP	REPORT	127.0.0.1,80,0	Metasploit WMAP	WMAP Scanner	2008-11-23 20:
3	3	-615361098	0	WMAP	REPORT	127.0.0.1,80,0	Metasploit WMAP	WMAP Scanner	2008-11-23 20:
4	4	-619407548	3	WEB_SERVER	TYPE	Apache/2.2.8 (Uni		HTTP Version Det	2008-11-23 20:
5	5	-616663128	3	VULNERABILITY	DIR_LISTING	/	Directory / disclos	HTTP Directory Li:	2008-11-23 20:
6	6	-616125318	3	DIRECTORY	NAME	/cgi-bin/	Directory /cgi-bin/	HTTP Directory Sc	2008-11-23 20:
7	7	-616145758	6	DIRECTORY	RESP_CODE	403		HTTP Directory Sc	2008-11-23 20:

“Beta” Charakter

- Version 0.3
- Kein eigener Crawler
- Kein eigener Proxy, aktuell nur Codepatch für Googles RATProxy
- Datenbanksupport: SQLite3
- Steuerung nur aus MsfConsole

Probleme

- Keine Unterstützung von Threads
  - Vergleich: WMAPDirScanner: 3 Min, Dirbuster: 10 Sek.
- Keine Ausführung einzelner Befehle mit Daten aus dem DB-Backend
- Keine Scanpolicy bzw. momentan nur auf Umwegen realisierbar
- DB speichert Servername als IP
  - Problem falls mehrere DNS Namen auf eine IP zeigen.
  - Abhilfe: Setzen einer globalen VHOST Variable

Fragen & Antworten