



Carsten Eilers | ceilers-it.de

Angriffs-Frameworks:

Kenne Deinen Feind!



Vorstellung

- » Berater für IT-Sicherheit
- » Autor
 - » About Security
 - » Standpunkt Sicherheit
 - » und anderes...
- » Schwachstellen-Datenbank
 - » „Security Aktuell“ auf entwickler.de



Agenda

- » Einführung
- » Mailinglisten
- » PHP-Shells
- » Google Dorks
- » milw0rm.com
- » Metasploit Framework
- » BeEF - Browser Exploitation Framework
- » MPack



Einführung

- » Warum mache ich das?
 - » Wer Angreifer abwehren will, muss wissen, wie er angegriffen wird
 - » Full Disclosure ist NICHTS Böses: Nur wenn ich weiß, das ich bedroht bin, kann ich mich schützen:
 - » Patches installieren
 - » Workaround nutzen
 - » Programm vom Netz nehmen



Agenda

- » Einführung
- » **Mailinglisten**
- » PHP-Shells
- » Google Dorks
- » milw0rm.com
- » Metasploit Framework
- » BeEF - Browser Exploitation Framework
- » MPack



Mailinglisten (1)

» Bugtraq

- » gegründet 5.11.1993
- » Ziel: Diskussion über Schwachstellen und deren Behebung
- » bis 5.6.1996 unmoderiert, seitdem moderiert
- » nach mehreren Umzügen bei SecurityFocus, SecurityFocus seit 2002 bei Symantec
- » Durch Moderation nur sachbezogene Mails, trotzdem auch Falschmeldungen



Mailinglisten (2)

» Full-Disclosure

- » gegründet 9.7.2002
(Reaktion auf Verkauf von SecurityFocus)
- » Ziel: Diskussion über Schwachstellen und deren Behebung - ohne Moderation
- » Unmoderiert => Flamewars usw.,
dafür schneller als Bugtraq



Mailinglisten (3)

- » VIM - Vulnerability Information Managers
 - » Diskussion über bereits anderswo veröffentlichte Schwachstellen
 - » Nützlich, um Falschmeldungen aus den anderen Listen zu erkennen



Mailinglisten (4)

- » SecurityFocus Schwachstellen-Datenbank
 - » „Sammelbecken“ von u.a. auf Bugtraq veröffentlichten Schwachstellen
- » Bereich „Security aktuell“ auf entwickler.de
 - » Suchfunktion kommt im Sommer



Mailinglisten (5)

» CVE-IDs

- » Common Vulnerabilities and Exposures
- » seit 1999
- » Eindeutige Bezeichner für Schwachstellen
- » Aufbau: CVE-Jahr-Ifd.Nr.



Agenda

- » Einführung
- » Mailinglisten
- » **PHP-Shells**
- » Google Dorks
- » milw0rm.com
- » Metasploit Framework
- » BeEF - Browser Exploitation Framework
- » MPack



PHP-Shells (1)

»Einfachste Variante:

```
<?php  
    system($_GET['cmd']);  
?>
```



PHP-Shells (2)

» Geht aber auch komfortabler:

» r57shell („Deluxe-Version“)

» c99shell

» und einige mehr

» Auch für andere Sprachen, z.B. ASP



Agenda

- » Einführung
- » Mailinglisten
- » PHP-Shells
- » **Google Dorks**
- » milw0rm.com
- » Metasploit Framework
- » BeEF - Browser Exploitation Framework
- » MPack



Google Dorks

» Ursprünglich:

We call them 'googledorks': Inept or foolish people as revealed by Google.

(Johnny 'ihackstuff' Long, Google Hacking Database (GHDB))

» Inzwischen auch Bezeichnung für die Suchstrings, die zu möglichen Opfern führen



Google Dork Beispiele

- » „Powered by ABC v.1.2.3“
- » `inurl:"index.php?action=download&file="`
- » `intitle:"Irgend ein Titel"`
- » `filetype:cgi inurl:load.cgi`



Agenda

- » Einführung
- » Mailinglisten
- » PHP-Shells
- » Google Dorks
- » **milw0rm.com**
- » Metasploit Framework
- » BeEF - Browser Exploitation Framework
- » MPack



milw0rm.com

- » Laufend aktualisierte Sammlung von
 - » Exploits
 - » Shellcode
 - » Paper
 - » Videos



Agenda

- » Einführung
- » Mailinglisten
- » PHP-Shells
- » Google Dorks
- » milw0rm.com
- » **Metasploit Framework**
- » BeEF - Browser Exploitation Framework
- » MPack



Metasploit Framework (1)

- » Entwicklungsplattform für Sicherheitstools und Exploits
- » Verwendbar für z.B.
 - » Penetration-Tests
 - » Test von Patches



Metasploit Framework (2)

- » „Exploitation“ ist damit sehr einfach
 - » Ziel auswählen
 - » Exploit auswählen
 - » Payload auswählen
 - » ggf. konfigurieren
 - » ... und abfeuern



Metasploit Framework (3)

- » 3 Benutzerinterfaces:
 - » msfconsole für textbasierte Terminals
 - » msfd öffnet Netzwerkinterface dazu
 - » msfweb als Weboberfläche
 - » mfscli für Kommandozeilen



Metasploit Framework (4)

» Erweiterungen

» Meterpreter (Meta-Interpreter)

- » Payload, die eine eigene Shell bereit stellt

» VNC Inject

- » Payload, die eine VNC-Verbindung aufbaut

» PassiveX

- » Payloads, die über einen temporären Webserver ein ActiveX-Control in den IE einschleusen
- » Danach sieht alles wie Web-Traffic aus



Metasploit Framework (5)

» Datenbank-Modul für automatisierte Pen-Tests



Agenda

- » Einführung
- » Mailinglisten
- » PHP-Shells
- » Google Dorks
- » milw0rm.com
- » Metasploit Framework
- » **BeEF - Browser Exploitation Framework**
- » MPack



BeEF - Browser Exploitation Framework

- » Fernsteuerung von über XSS übernommenen Webbrowsern
- » Läuft auf Server
- » Clients verbinden sich mit Server
- » Server startet Aktionen auf Client, z.B.
 - » Clipboard auslesen
 - » JavaScript-Portscan
 - » Ausnutzen von Browser-Schwachstellen



Agenda

- » Einführung
- » Mailinglisten
- » PHP-Shells
- » Google Dorks
- » milw0rm.com
- » Metasploit Framework
- » BeEF - Browser Exploitation Framework
- » **MPack**



MPack (1)

- » Massive Angriffe im Sommer 2007
- » Sammlung von PHP-Scripts
- » Enthält Exploits verschiedener Schwachstellen
- » Das einzige heute vorgestellte Programm, das wirklich ein verbotenes Hackertool ist



MPack (2)

- » In Websites eingeschleuste IFrames leiten Benutzer über eine zweiten Server auf den MPack-Server
- » Analysiert die HTTP-Header
- » Schleust passenden Exploit ein
- » Opfer ist Teil eines Bot-Nets



Fragen?



Vielen Dank...

... für Ihre Aufmerksamkeit!

Material und Links auf
www.ceilers-it.de/konferenzen/

