



squareroots - Capture the Flag

26. August 2008



Ben Stock / ben@squareroots.de



Wer sind wir

- Studenten und Mitarbeiter des Lehrstuhl PI1
- Gegründet als Projekt des Lehrstuhl
 - Erstmals 2006 beim UCSB Wettbewerb
- Harter Kern aus ca. 10 Leuten
 - Bei großen Wettbewerben bis zu 25 Spieler
- Eigener CTF Pool im Keller von A5 Bauteil B





Bisherige Wettbewerbe

- Erster Wettbewerb: vorletzter Platz :-(
- Zweiter Wettbewerb (CIPHER 2007): 5. Platz
(Teilnahme aus Luzern)
- Dritter Wettbewerb (UCSB 2007): 2. Platz
- Vierter Wettbewerb (CIPHER 2008): 8. Platz :-/
- Fünfter Wettbewerb (Da Op3n): 6. September





- Was stellt Ihr euch darunter vor?
- Einigen ein Begriff aus Spielen?





- CTF = “Capture the Flag”
 - Kurz: Flaggen klauen und verteidigen
- In unserem Sinne: IT-Sicherheitswettbewerb
 - Viele teilnehmende Teams
 - Verschiedene Dienste mit absichtlich eingebauten Schwachstellen
 - Zentraler Gameserver, der Flaggen verteilt/überprüft





- **Verschiedene Arten von Punkten**
 - Defensiv: Dienst ist erreichbar, akzeptiert Flaggen und auf Anfrage kann er dem Gameserver die Flagge wieder nennen
 - Offensiv: für das Stehlen der Flaggen von anderen Teams
 - Zusätzliche Punkte für das Erstellen von sog. Advisories
 - Genaue Beschreibung der Schwachstelle/Möglichkeit, diese auszunutzen
 - wichtiger Teil der Ausbildung von IT-Sicherheitlern





- Idee: Programmierfehler/Schwachstellen im eigenen System finden
 - beim eigenen System beheben
 - Einbrüche verhindern
 - beim Gegner ausnutzen
 - Stehlen von Flaggen





- “Geheime” Zeichenkette variabler Länge
 - CIPHER: 32-stellig
 - Da Op3n: 64-stellig
 - z.B. 5FF5AC73E11B43963918F1E028B42BF0
- Nachweis, dass Dienst funktioniert
 - Auch, dass Dienst erfolgreich kompromitiert wurde





- **Verschiedene Speicherorte**
 - im Dateisystem
 - als Dateiname
 - als Dateiinhalt
 - als Rückgabe eines ausführbaren Programms
 - in Datenbanken
 - MySQL
 - SQLite
 -





- **Verschiedene Programmiersprachen**
 - PHP
 - Perl
 - Haskell
- **Verschiedene Dienste**
 - Gästebücher
 - Online-Shops
 - ...



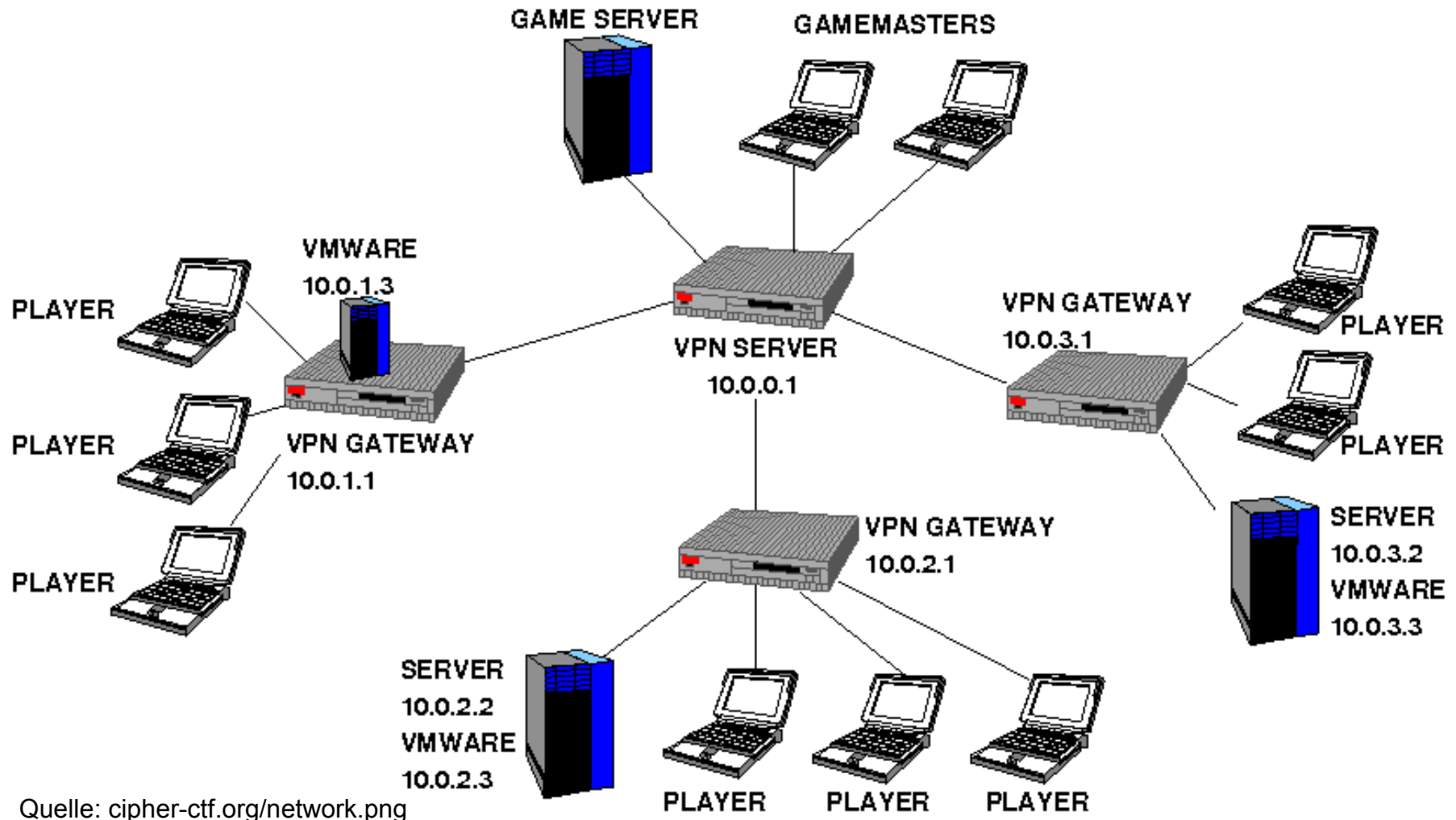


- Angriffsvektoren vielfältig
 - SQL-Injection
 - Remote File Inclusion
 - Ausführung beliebiger Befehle
 - Upload von ausführbaren Dateien
 - Cross Site Scripting
 -





CTF - Netzaufbau



Quelle: cipher-ctf.org/network.png





CTF – Vulnerable Image

- **Verwundbares System**
 - Meistens Linux-Derivate
 - Als virtuelle Maschine (VMWare, qemu)
 - keine Kompromittierung des “echten” Betriebssystems
 - somit für alle Teilnehmer exakt gleiche Ausgangsbedingung





- Virtual Private Network
 - Virtuelles, vom Internet getrenntes Netz
 - Dadurch wird “Schaden” an der Aussenwelt verhindert
- Ebenfalls an der Universität Mannheim
 - Hier aber nicht zum Verhindern von Schaden
 - Zugriffssteuerung





- Rough Auditing Tool for Security
 - scant auf bekannte Schwachstellen/verwundbare Funktionen
 - ... Demo!
 - <http://www.fortify.com/security-resources/rats.jsp>





Fragerunde

- Was erwartet Ihr vom CTF?
- Was wollt Ihr machen?





- SQL ist eine Abfragesprachen für Datenbanken
- z.B. Telefonbuch, Forum,
 - Beispiel Telefonbuch: Abfrage der Telefonnummer von “Michael”
 - `SELECT telefonnummer FROM kontakte WHERE name="Michael"`
- Oftmals ist Benutzereingabe die Kondition
 - `SELECT telefonnummer FROM kontakte WHERE name="<Benutzereingabe>"`





- Beispiel

- `SELECT telefonnummer FROM kontakte WHERE name="Michael" AND vorwahl = "0621"`
- Ergebnis: Telefonnummer von Michael, aber nur, wenn der als Vorwahl 0621 hat

- Idee bei der SQL Injection

- eine Kondition mit OR übergeben, die immer wahr ergibt
- z.B. `1=1` ist immer wahr





- Vorbereitete Abfrage

- SELECT telefonnummer FROM kontakte WHERE name="<Benutzereingabe>"

- Benutzereingabe: 'Michael' OR "1" = "1'

- SELECT telefonnummer FROM kontakte WHERE name="Michael" OR "1" = "1"
- Ergebnis: alle Telefonnummern!





SQL Injection

- http://de.wikipedia.org/wiki/SQL_Injection
- <http://www.heise.de/security/Giftspritze--/artikel/43175>
- <http://www.php-center.de/de-html-manual/security.database.sql-injection.html>
- http://www.owasp.org/index.php/SQL_injection
- ...





Arbitrary Command Execution

- http://www.owasp.org/index.php/Command_Injection
- ...





Remote File Inclusion

- http://de.wikipedia.org/wiki/Remote_File_Inclusion
- http://www.owasp.org/index.php/Top_10_2007-A3
- ...





- http://www.owasp.org/index.php/Cross_Site_Scripting
- http://de.wikipedia.org/wiki/Cross-Site_Scripting
- <http://www.heise.de/security/Cross-Site-Scripting-Datenklau-ueber-Bande--/artikel/38658>
- ...





Linux Kommandos

- **grep**
 - http://linuxseiten.kg-it.de/index.php?index=bash_Der_Befehl_grep
- **sed**
 - http://linuxseiten.kg-it.de/index.php?index=bash_Der_Befehl_sed
- **curl**
 - http://linux.about.com/od/commands//blcmdl1_curl.htm





Linux Kommandos II

- netcat
 - http://de.wikibooks.org/wiki/Linux-Kompendium:_netcat
 - http://www.netmage.info/latex_doc/netmage_netcat.pdf





regelmäßige Vorbereitungstreffen

- Nachbereitung der Wettbewerbe
- Workshops (SQL-Injection, reversing, rfi, scripting...)
- Informationen über die Mailingliste
 - <http://lists.squareroots.de/cgi-bin/mailman/listinfo/ctf-pub>
(ctf-pub@lists.squareroots.de)
 - <http://blog.squareroots.de/>





- 6. September 18 bis 2 Uhr
- Team der squareroots nimmt teil
- A5, B-124 (Keller des B-Teils, Zugang über A-Teil)
- ca. 20-25 Teams
- jeder Besucher und Mitspieler ist herzlich willkommen





Danke für die Aufmerksamkeit

