Hacker-Contest | SS 2015
FG Security Engineering

Dr. Erik Tews, erik@datenzone.de
PGP: 7C7B 2C41 4EF9 F9B9 FC82 ABE8 D55E ECE1 107B 0807

Mit Hiwi: hackercontest@cased.de

Ablauf heute

- Anmeldeaufgabe
- Vorstellungsrunde
- Vorstellung des Praktikums
- Terminplan & Einteilung der Teams
- Aufgaben für diese Woche

Anmeldeaufgabe

Wie sah eine gute Lösung aus?

Vorstellungsrunde

Was hat sie zu diesem Praktikum geführt?

Vorstellung des Praktikums

- 6 Teams à 2 Mitglieder
- ggf. noch weitere „Zuhörer“
- Jedes Team darf einen der Computer im Poolraum verwenden
- Eigene Laptops dürfen auch benutzt werden
- Alle Computer hier sind zu einem geschlossenen Netzwerk verbunden
- Zugriff nach außen nur per HTTP und SSH
    - wir wollen das Uni-Netzwerk und das Internet schützen
- Zugriff von außen ist möglich (SSH)

Ablauf des Praktikums

- Bearbeitung der Aufgabenblätter
- Wöchentliches Treffen zur Besprechung der Aufgaben und Erkenntnisse
- Alle 2 Wochen stellt ein Team ein Thema vor
- Ein anderes Team stellt aktuelle Entwicklungen in der IT-Sicherheit vor
- Sonst freie Zeiteinteilung (Zugang zum Praktikumsraum während der Gebäudeöffnungszeiten)
- Nach möglichkeit noch zwischendurch Spezialthemen

Themen

- Informationssammlung
- Netzwerksicherheit
- Softwaresicherheit
- Webapp-Security
- Kryptographie
- Forensik

Jedes Team stelle ein Thema in einem Vortrag vor.

Voraussetzung für den Erwerb des Scheins (je Team)

- Vorbereiten und Halten des Vortrags Thema (10%)
- Vorbereiten und Halten des Vortrags „Aktuelle Themen“ (10%)
- Mindestens 40% der Punkte von jedem Aufgabenblatt (60%)
- Abgabe eines Praktikumsberichts (einen Monat nach Praktikumsende, ggf. auch mehr Zeit) (20%)
- Regelmäßige Anwesenheit (max. 2 mal entschuldigtes Fehlen) und aktive Mitarbeit

Aufgabenblätter

- Werden vor Beginn des Praktikumstermins abgegeben, an dem ein neues Thema beginnt
- Jeweils komplette Lösung als Anhang in einer Email
- Entweder als PDF oder als Text
- Wenn Dateien angehängt werden müssen als ZIP oder tar.gz
- Subject der Mail: Blattnummer und Teamnummer
- Dateiname: teamX_blattY.*
- Digital signiert mit einem bekannten GPG Schlüssel
- Am Anfang jeder Aufgabe den/die Bearbeiter angeben
- Alle verwendete Literatur/Webseiten und Tools angeben
- Und ganz wichtig: der Lösungsweg
- Bepunktung:
    - 70% Korrektheit
    - 30% Stil und Details
- Weitere Angaben folgen ggf.

Rechtliches

- §202a, StGB: Ausspähen von Daten
    - Geldstrafe oder bis zu 3 Jahre Freiheitsstrafe
- §303a, StGB: Datenveränderung
    - Geldstrafe oder bis zu 2 Jahre Freiheitsstrafe
    - auch der Versuch ist strafbar
- §303b, StGB: Computersabotage
    - Geldstrafe oder bis zu 5 Jahre Freiheitsstrafe
    - auch der Versuch ist strafbar
- §202c, StGB: „Hacker-Paragraph“

    - Geldstrafe oder Freiheitsentzug bis zu einem Jahr
    - „wer eine Straftat vorbereitet durch das Herstellen, Verschaffen, Verkaufen, überlassen, Verbreiten oder Zugänglichmachen von Passwörtern oder sonstigen Sicherheitscodes für den Datenzugang, sowie von Computerprogrammen, deren Zweck die Begehung einer entsprechenden Tat ist“
    - genaue Bedeutung musste durch Gerichtsurteile geklärt werden
- § 823, BGB: Schadensersatzpflicht
    - Verpflichtung zum Ersatz eines Schadens
- § 826 BGB Sittenwidrige vorsätzliche Schädigung
    - Verpflichtung zum Ersatz eines Schadens

Regeln

- Keine Angriffe auf den Praktikumsserver oder Router
- Und keine Angriffe außerhalb des Praktikumsnetzes

Kommunikation

- für Ankündigungen, Fragen, etc.: Mailingliste hc@lists.cased.de
- für Infos, Downloads, Linksammlungen, etc.: Wiki
- https://130.83.239.76/dokuwiki/ (Zertifikat selbstsigniert, wird noch erneuert)

Terminplanung und Teameinteilung

Nachästes Treffen am 21.04.2015

- Team-PC & VM installieren: ein Linux, ein Windows, inkl. Serverdienste, jeweils auf Stand von vor mind. zwei Jahren
- Automatische Updates und ähnliches sind nicht erlaubt bzw. zu deaktivieren
- IP-Adressen aus 10.0.x.0/8, Team-PC: x.1, VM: beliebig, x = Teamnummer
- GPG-Schlüssel erstellen (pro Person; falls noch nicht vorhanden)
- Zugangsdaten für Server werden in einer Woche ausgehändigt

Netzwerk

- Server: 10.0.0.100/8
- Router: 10.0.0.1/8