

Security for Systems Engineering – VO 01: Capture the Flag

Martin Moutran, Florian Fankhauser, Christian Brem



Grundlagen zum CTF-Contest

Organisatorisches

Aufbau der Übungsumgebung

Bewertung

Auszug Regeln

Tipps zur Vorgehensweise

Anhang

- CTF → Capture the Flag
 - Traditionell: Offline-Spiel
 - Teams versuchen jeweils die gegnerische Fahne zu entwenden und in das eigene Lager zu bringen

- In der LVA
 - Online-Spiel
 - Bewerb Teil der Übung

- Teams treten gegeneinander an
- Spielfeld ist eine abgeschlossene Umgebung
- Flags sind Strings in Services
- Flags werden vom Gameserver verteilt
- Ziele für die Lehrveranstaltung
 - Praktische Erfahrungen in IT-Sicherheit
 - Erkennung und Behebung von Schwachstellen in Systemen
 - Ausarbeitung von Angriffstechniken (Sicherheitstests)
 - ... und natürlich viel Spaß ;-)

Voraussetzungen zur Teilnahme

- Studierende von Security for Systems Engineering / IT Security in Large IT Infrastructures
- Vor Ort, Teilnahme nur mit eigenem Gerät
- Anmeldung für CTF-Contest in TUWEL
- Kenntnisse
 - Inhalte Introduction to Security VU
 - Inhalte Security for Systems Engineering VU
 - Linux (siehe z.B. Linux Workshop Slides aus Introduction to Security)
 - Kenntnis unterschiedlicher Programmiersprachen

Teambildung Security for Systems Engineering

- Teams voraussichtlich zu je ca. 4 Studierenden
- Team-Namen
 - Fixe Anmeldung (TUWEL), nach Deadline für Team-Anm.
 - Kein Team-Name registriert → wir vergeben *gerne* einen ;)
 - Im Einzelfall behalten wir uns vor Team-Namen abzulehnen :)
- Beispiele für kreative Namen bisheriger CTF-Contests
 - „sudo make me a sandwich“
 - „Schaf-256“
- Beispiele für *mittlerweile* uncreative Namen
 - „'); DROP TABLE students; –“
 - „; DROP table groups –“

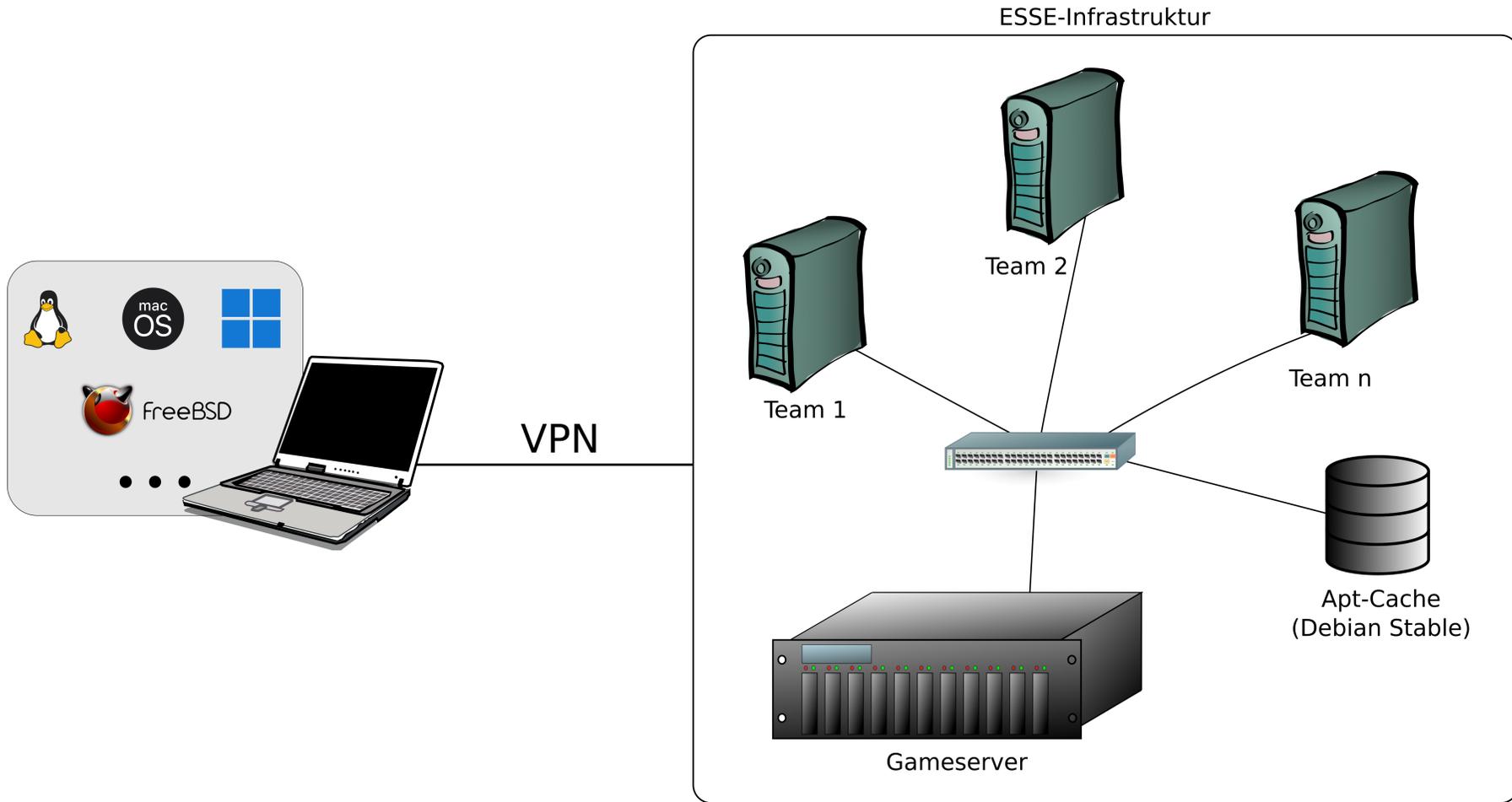
Paralleler Besuch zweier ESSE-LVAs

- Bei parallelem Besuch von IT Security in Large IT Infrastructures CTF-Contest-Ersatz verpflichtend
- Punkte des CTF können nur für IT Security in Large IT Infrastructures verwendet werden
- Bitte E-Mail an esse-secsyseng@inso.tuwien.ac.at

- 1 Termin mit fixen Plätzen
 - Sa. **17.06.2023**
 - Einlass ab 09:00 Uhr
 - Analyse-/Setup-Phase des Team-Servers: 09:30-10:30 Uhr
 - Bewerb: 10:30-16:30 Uhr
 - Preisverleihung ca. 17:00 Uhr
 - Protokoll bis 18:00 Uhr
- Treffpunkt für Einlass
 - Hörsaal 8 – TU Hauptgebäude → **nur unterer Eingang (EG)**
 - *Oberer Eingang* → *ESSE HQ*
- Anmeldung über TUWEL, Freischaltung während Lab1

- Aktivierung der Zugänge (VPN, Team-Server)
- Analyse, Absicherung der Server ohne Bewertung
- Parallele Ausarbeitung des Protokolls für LVA-Bewertung
- Gameserver startet zeitverzögert mit der Bewertung
- CTF-Contest läuft
- Nach Spielende: SiegerInnenehrung und Protokollabgabe
- Pause(n): keine Vorgabe, Selbstorganisation

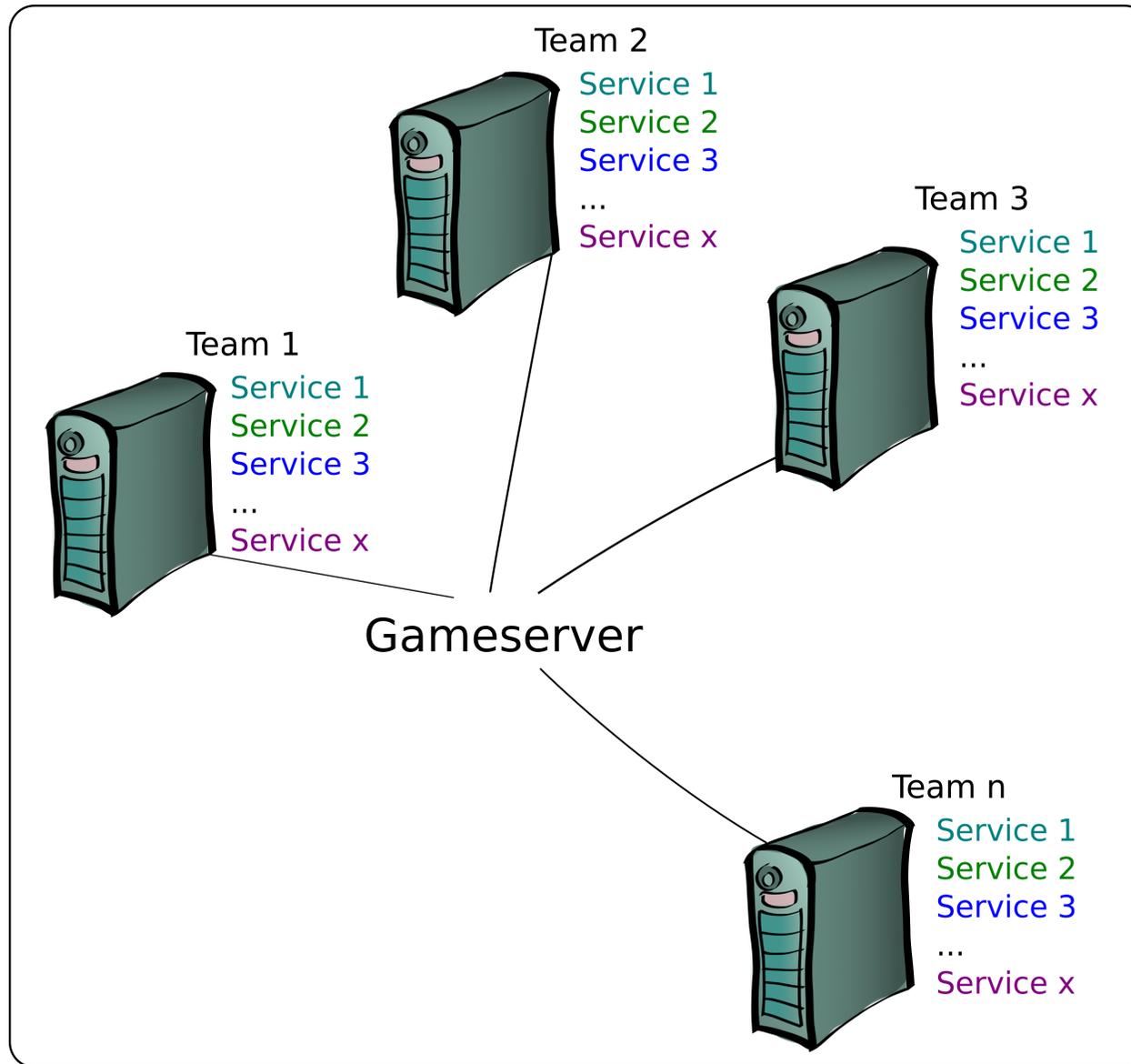
Aufbau der Übungsumgebung – Übersicht



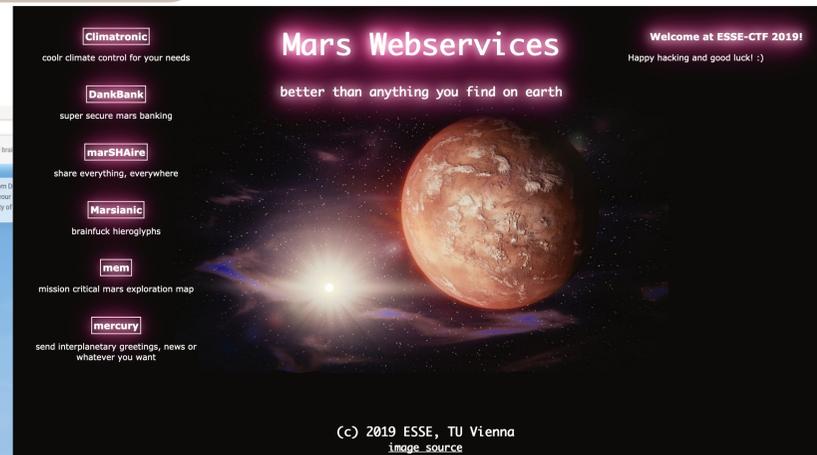
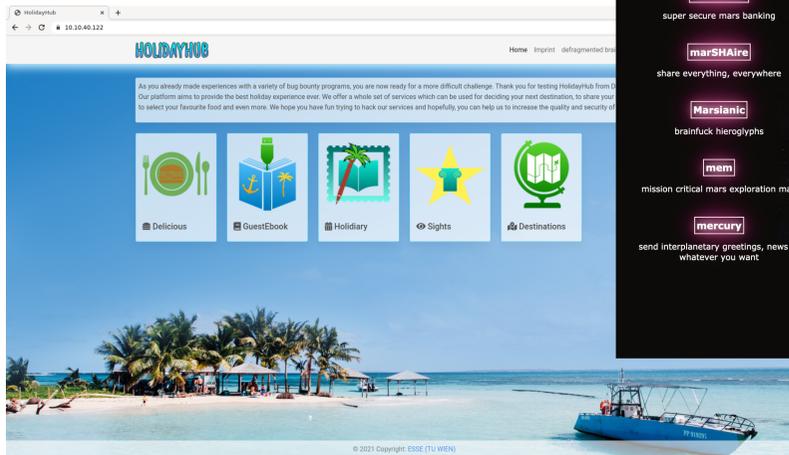
Aufbau der Übungsumgebung – Bestandteile

- Pro Team ein Server
- IP-Adressen der Server werden bekannt gegeben
- Gameserver
- Zentraler Knoten (VPN, Logging!)
- VPN
 - OpenVPN
 - Config + Anleitung wenige Tage vor Termin in TUWEL
 - Login: Lab0-Credentials
- Clients: Notebooks
 - ggf. Live-System auf USB-Sticks o.ä.
 - Vorab-Test der WLAN-Verbindung (z.B. eduroam, tunet) empfohlen

Aufbau der Übungsumgebung – Services



Beispiele für vergangene ESSE CTF-Contests



- Alle Teams bekommen (fast) identen Server
 - Unterschied bei IP-Adresse
- Login: Lab0-Credentials, sudo verfügbar
- Dienste sind selbstentwickelte Applikationen mit Schwachstellen
 - Schwachstellen sollen gefunden und behoben werden
 - Angriffe auf die Schwachstellen der anderen Team-Server
 - Beispiele für Arten von Sicherheitsfehlern
 - Implementierung (*-Injection, Logikfehler, ...)
 - Konfiguration (Standard-Passwörter, Berechtigungen, ...)
 - *Hinweis:* C bzw. C++ heißt nicht automatisch Buffer-Overflow!

Funktionsweise und Format von Flags

- Flags sind Daten der Dienste
- Periodische Verteilung durch Gameserver
- Flags besitzen eingeschränkten Gültigkeitszeitraum (ca. 15 Minuten)
- Flags sind immer als Ganzes hinterlegt und nicht deformiert
- Format
 - [Timecode inkl. Zeitzone][Zufalls-String]
 - Beispiel: **02062011180450UTC3ZL8T6XW1QKSJUU**
 - Timecode entspricht Verfallsdatum
 - Achtung Test-Flags: **02062011180814UTCTEST970VUKCGZIF**

- Unterscheidung zwischen Bewerb und Punkte für Lab
 - Übung → lab2, Bewertung auf Basis des Protokolls
 - Bewerb → Spaß und Preise
- Security for Systems Engineering oder IT Security in Large IT Infrastructures im selben Bewerb
 - Berücksichtigung bei Punktevergabe und Teamgröße

Bewertung – lab2: Abgabeprotokoll (i)

- Analyse und Beschreibung der einzelnen Services
- Dokumentation der vorhandenen Schwachstellen bzw. Vermutungen
- Dokumentation der Lösungen / Lösungsansätze
- Beschreibung des Angriffswegs bzw. der Vermutungen
- Weitere (kreative) Ideen für Angriffe und Verteidigung
 - Auch anführen, wenn diese nicht durchgeführt wurden
 - Beispiel: automatisierte Angriffe
- ggf. Dokumentation zur Härtung des Systems

Bewertung – lab2: Abgabeprotokoll (ii)

- Anzahl der bearbeiteten/beschriebenen Services (Punkte pro Service)
- Automatisierung des Angriffs
- Automatisierung der Abgabe von Flags
- Punkteabzug bei formalen Fehlern (Vorlage vom Gameserver nicht verwendet, erforderliche Angaben nicht vorhanden, Namenskonventionen, Teammitglieder nicht angeführt, usw.)

WICHTIG: Es zählen auch Tätigkeiten, welche nicht zum gewünschten Erfolg führten. Z.B. fehlgeschlagene Angriffsversuche, gefundene Fehler ohne Behebung, usw.

- Verteidigung (Services müssen funktionieren, keine Angriffe)
- Angriff (Flags von anderen Teams sammeln)
- Laufende und funktionierende Services Voraussetzung für Angriffe
- Bonuspunkte
 - Abgabe von Advisories
 - Gute, kreative Lösungen (Beschreibung in Advisories)
 - Erhöhung der Gesamtpunkte um 15% bei erfolgreicher Abgabe min. eines Flags / Service
(Visualisierung durch eine goldene Krone neben dem Team-Namen)
- Teams mit meisten geknackten Services: silberne Krone

ESSE CTF Contest 2021S Scoretable

| TEAM | TOTAL | OFFENSIVE | DEFENSIVE | BONUS | LOST |
|----------------------------------|-------|-----------|-----------|-------|------|
| 01. 10 (S) Long Island size_t | 1165 | 1056 | 132 | +50 | -73 |
| 02. 26 (L) GeröstetUndGesalzen | 1082 | 880 | 107 | +105 | -10 |
| 03. 14 (S) NameNotFound | 1030 | 870 | 136 | +80 | -55 |
| 04. 28 (L) Cobol19 Testers | 959 | 804 | 104 | +95 | -44 |
| 05. 24 (L) s0nn3nd3ck_m3g4_h4... | 778 | 658 | 79 | +85 | -44 |
| 06. 03 (S) Byters | 675 | 549 | 137 | +80 | -90 |
| 07. 20 (S) Herbert | 655 | 517 | 132 | +50 | -44 |
| 08. 11 (S) LaptopWalker | 648 | 582 | 115 | 0 | -49 |
| 09. 27 (L) Order of Any Key | 496 | 404 | 104 | +50 | -61 |
| 10. 05 (S) Hacking 4 Catfood | 489 | 482 | 134 | 0 | -127 |
| 11. 09 (S) NOK | 343 | 325 | 116 | 0 | -98 |
| 12. 21 (S) Bug Busters | 274 | 155 | 133 | 0 | -14 |
| 13. 15 (S) c4m0uFL4G3d | 257 | 186 | 126 | 0 | -55 |
| 14. 17 (S) Jason Wants Tokens | 245 | 208 | 132 | 0 | -95 |
| 15. 08 (S) TLSWarning | 146 | 116 | 132 | 0 | -102 |
| 16. 16 (S) Deauthenticated | 85 | 70 | 118 | 0 | -104 |

Punkte für Angriffe

- Nachweis eines erfolgreichen Angriffs: Abgabe eines gültigen Flags beim Gameserver
- Wiederholung: Flags sind für einen eingeschränkten Zeitraum gültig
- Verfügbarkeit des eigenen Services Voraussetzung zur erfolgreichen Flagabgabe
- Punkte bei einer erfolgreichen Abgabe eines gültigen Flags
 - Pro Service und Team volle Punkteanzahl für 4 Flags
 - Ab 5. Flag dieser Service/Team-Kombination nur mehr 20% der Punkte → laufendes manuelles Ausnutzen des gleichen Services nicht zielführend
 - Keine Punkte für eigene Flags oder Test-Flags

Punkte für Verteidigung / Schadenspunkte

- Periodische Überprüfung der Services
- Punkte für „*erreichbare*“ Services
- *Weitere* Punkte für *funktionale* Services
- Status-Kennzeichnung am Gameserver
 - Vor Spielbeginn: **hidden**
 - Ab Spielbeginn: **up**, **down** oder **broken**
- Schadenspunkte bei erfolgreichem Angriff des eigenen Services in aktueller Runde
- Übersicht der Punkteverteilung am Gameserver

ESSE CTF Contest 2021S Service Status

Services - ESSE CTF Contest x +

10.10.40.200/services

Incognito (7)

Services Refresh interval: 60s

| TEAM | DELICIOUS | DESTINATIONS | GUESTBOOK | HOLIDIARY | SIGHTS |
|--------------------------------|-----------|--------------|-----------|-----------|--------|
| 01 (S) RootKitKat | UP | UP | UP | UP | UP |
| 03 (S) Byters | UP | UP | UP | UP | UP |
| 04 (S) Kabelsalat | UP | UP | UP | UP | UP |
| 05 (S) Hacking 4 Catfood | UP | UP | UP | UP | UP |
| 06 (S) Network Erre | UP | UP | UP | UP | UP |
| 07 (S) broken teapots | BROKEN | UP | UP | UP | UP |
| 08 (S) TLSWarning | UP | UP | UP | UP | UP |
| 09 (S) NOK | UP | UP | UP | UP | UP |
| 10 (S) Long Island size_1 | UP | UP | UP | UP | UP |
| 11 (S) LaptopWalker | UP | UP | UP | UP | UP |
| 13 (S) PwnieHof | UP | UP | UP | UP | UP |
| 14 (S) NameNotFound | UP | UP | UP | UP | UP |
| 15 (S) oAmouFL493d | UP | UP | UP | UP | UP |
| 16 (S) Deauthenticated | UP | UP | BROKEN | UP | UP |
| 17 (S) Jason Wants Tokens | UP | UP | UP | UP | UP |
| 18 (S) xxxCrazyF3E5TyEh4K... | UP | UP | UP | UP | UP |
| 19 (S) Participations4 | BROKEN | BROKEN | BROKEN | BROKEN | BROKEN |
| 20 (S) Herbert | UP | UP | BROKEN | UP | UP |
| 21 (S) Bug Busters | UP | UP | UP | UP | UP |
| 22 (S) CTFnoobs | UP | UP | UP | UP | UP |
| 23 (L) Hugs for Blues | UP | UP | UP | UP | UP |
| 24 (L) s0m33nd3ck_m3g4_3dck... | UP | UP | UP | UP | UP |
| 25 (L) Format C: | UP | UP | UP | UP | UP |
| 26 (L) GeristetUndGesargen | UP | UP | UP | UP | UP |
| 27 (L) Order of Any Key | UP | UP | UP | UP | UP |
| 28 (L) Cobalt9 Testers | UP | UP | UP | UP | UP |

- Veröffentlichung der Detail-Regeln folgt in TUWEL
- **Angriffe außerhalb der Übungsumgebung und auf die Infrastruktur für den Spielbetrieb sind verboten!**
- Konsequenzen vom Institut sowie der TU möglich
- Befolgung der Anweisungen des ESSE-Teams
- Regelverstöße können Punkteabzug bringen, gleich oder nach Analyse der Logs
- Kein „teamübergreifender“ Kontakt
- Kein Kontakt mit externen Personen

Verbote bei Angriffen

- ARP-Spoofing
- DoS-Angriffe
- Flags löschen oder ändern
- Angriffe auf Notebooks
- **Angriffe außerhalb der Übungsumgebung und auf die Infrastruktur für den Spielbetrieb sind verboten!**

- Verbote
 - Zugriffsbeschränkungen
 - Netzwerk-Ebene (z.B. Filterung auf Grund von IP-Adressen)
 - Applikations-Ebene (z.B. nur Gameserver erlauben)
 - Deaktivierung von spezifizierten Funktionen bei Services
- Gebote
 - Korrigieren Sie Schwachstellen; keine Work-Arounds!
 - Neukompilierung/Neustart von Services
 - Anpassung von Services/Scripts, solange die spezifizierte Funktion erhalten bleibt

Hinweise für die Vorgehensweise (i)

- Finden von Services
 - Benutzer am System (/etc/passwd, /home/*)
 - Untersuchung von laufenden Prozessen
 - Services in Docker Containern
 - Offene Ports und zugehörige Applikationen (netstat, lsof)
- Backups von relevanten Dateien vor Änderungen
 - *git* wird auf Team-Server vorab eingerichtet, nur Source-Files
 - Keine externen Kopien des kompletten Servers durchführen (Traffic!)

Hinweise für die Vorgehensweise (ii)

- Suche nach Sicherheitslücken und Korrektur dieser
- Log-Dateien überwachen; können wichtige Hinweise liefern, z.B.:
 - `tail -f datei`
 - `journalctl -f`
- ggf. Verwendung des eigenen Servers für Analysen
- Angriff der anderen Teams mittels gefundener Sicherheitslücken

- Protokoll nicht nur am Ende erstellen, sondern laufende Ergänzung
- Regelmäßige Überprüfung des Status Ihrer Services am Gameserver
→ Kennzeichnung von fehlerhaften Services
- Kontrolle von Nachrichten der Übungsleitung am Gameserver/im Rocket.Chat
- Server kann notfalls durch ESSE-Team zurückgesetzt werden
→ Verlust des bisherigen Setups
- Unterstützung durch das ESSE-Team bei Fragen
- Unmittelbare Meldung eventueller Regelverstöße / Verdacht auf unfaires Handeln an das ESSE-Team

Vorbereitung – Programmiersprachen

- Auffrischung von Programmierkenntnissen
- Behebung von Schwachstellen
 - Inputvalidierung
 - Korrektur von logischen Fehlern
- Beispiele für Programmiersprachen
 - C, C++, Java, PHP, Python, Ruby, Shell Scripts, ...
 - Vielleicht auch Exoten
 - https://en.wikipedia.org/wiki/Esoteric_programming_language
 - https://esolangs.org/wiki/Language_list

- Angriffe
- Abgabe von Flags
- Eigene Programme (JAVA, C++ etc.) möglich, wenn installiert
- Scripts
 - Bsp. für Scriptsprachen: Shell-Scripts (z.B. bash), perl, python
 - HTTP/HTTPS-Requests: wget, curl
 - Netzwerk: telnet, netcat (nc)
 - Filterung/Manipulation von Ergebnissen/Strings: grep, sed, awk
 - Netzwerk-Prozesse, offene Dateien/Ports: netstat, lsof
 - Dateien: ls, find, cat, tac, tail

- Optimierung der automatischen Abgabe von Flags beim Gameserver
 - Abgabe nur der letzten Flags, nicht sämtliche gefundenen Flags
 - Timestamp zu Beginn der Flags (siehe Slide „Funktionsweise und Format von Flags“)
- Bei Scripts (unabsichtliches) Denial of Service verhindern, z.B. Sleep beim Abfragen
- TUWEL Ankündigungen kurz vor dem CTF-Contest
 - Interface-Beschreibung für Flag-Abgabe
 - Online Test-Service

- Optional, bei ausreichendem Interesse
- Informationen im Laufe des Semesters
- Anmeldung und Termin via TUWEL

- Optional
- In Planung
- Voraussichtlich am 02.06.2023, 18:00-21:00 Uhr
- Weitere Informationen folgen in TUWEL
- Test der Infrastruktur, des Gameservers
- Möglichkeit vorab System kennenzulernen
- Kein Protokoll und keine Punkte für die Übungsbewertung
- Andere Services als beim regulären ESSE-CTF-Contest

- Wenn Sie Fragen haben, stellen Sie sie jetzt!
- ... oder
 - Stellen Sie Ihre Frage im TUWEL-Übungsforum
 - Schreiben Sie uns ein e-mail: esse-secsyseng@inso.tuwien.ac.at

Weitere CTF-Bewerbe

- Teilnahme der ESSE bei internationalen CTF-Bewerben
- Bei bevorstehender Teilnahme Aussendung via Mailingliste
- Bei Interesse Informationen und Anmeldung zur Mailingliste auf
 - <https://twitter.com/defbra/>
 - <https://www.defragmented-brains.at/>
- Meistens unterschiedlichste Kenntnisse erforderlich vor Teilnahme
- Und natürlich...
... unsere neue Lehrveranstaltung :)



QR-Code – Big ;)



Vielen Dank!

<https://security.inso.tuwien.ac.at/>



- *Hinweis:* Code dient der Illustration!

```
#!/bin/bash
rm flag
#getting flags
for i in `seq 100 1 108` `seq 110 1 111`; do
    sleep 1
    curl http://1.1.1.${i}/~chatservice/userlist | \
        sed 's/^.*::.*::.*::\(.*\)/\1/g' | \
        grep -v steve >> flag
done
```

Script-Beispiel – Abholung von Flags eines proprietären Services

- *Hinweis:* Code dient der Illustration!

```
#!/bin/bash
rm data
for i in `seq 100 1 108` `seq 110 1 111`; do
    sleep 1
    echo $i
    nc 1.1.1.${i} 3553 -w 1 < input | \
        grep patent-idea >> data
done
```