esse

Security for Systems Engineering - VO 08: Capture the Flag

Christian Schanes und Markus Gruber

Agenda

CTF

Voraussetzungen

Bewertung

Regeln

CTF Ersatz

Gruppenbildung

Termine

Scripting

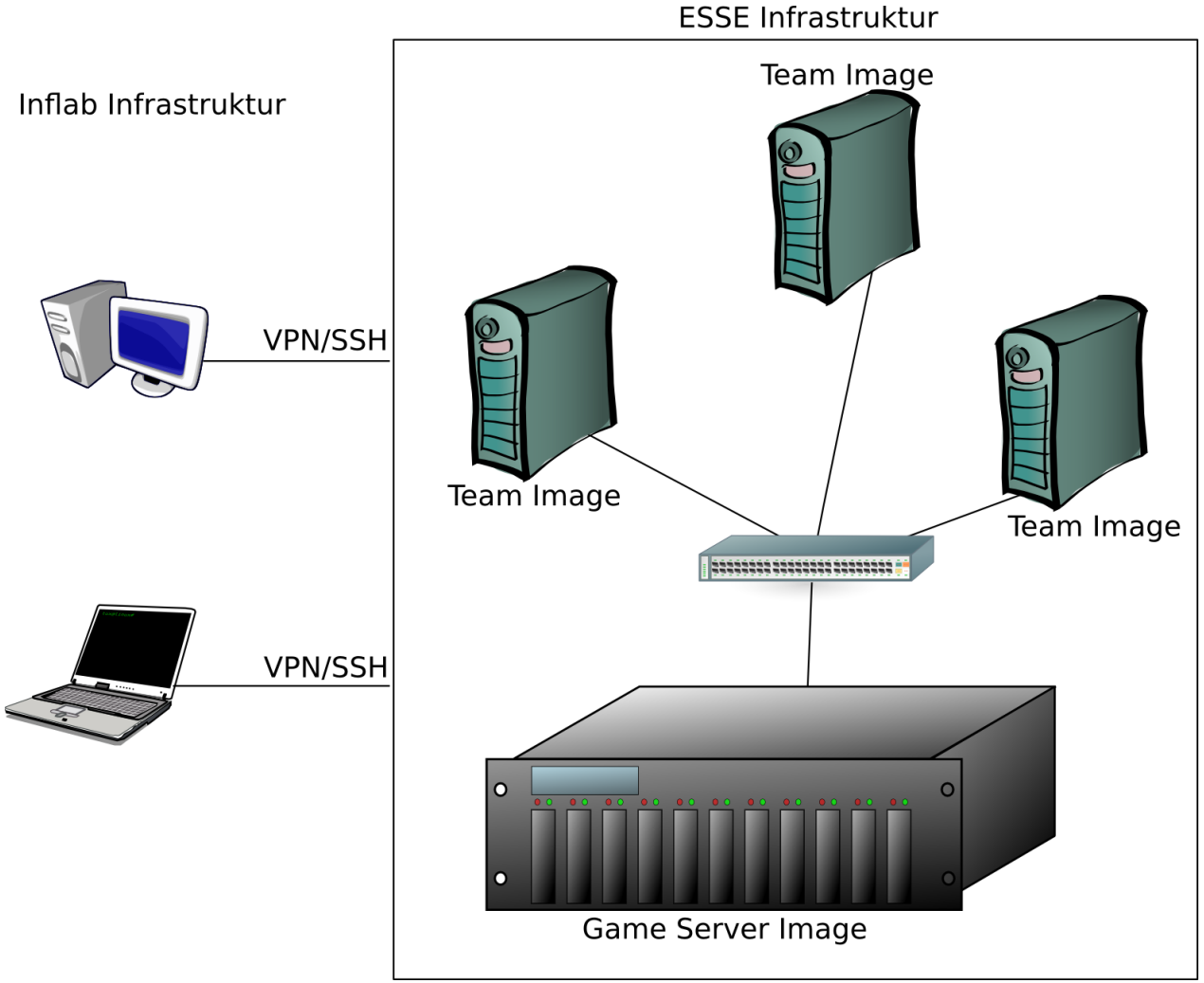
CTF - Capture The Flag

- CTF → Capture the Flag
  - Traditionelles Kinderspiel
  - Teams versuchen jeweils die gegnerische Fahne zu entwenden und in das eigene Lager zu bringen
- Für die LVA ist der Bewerb Teil des Übungsbetriebs

CTF - Capture The Flag

- Teams treten gegeneinander an
- Spielfeld ist eine abgeschlossene Umgebung
- Flags sind Strings in Services
- Flags werden von Gameserver verteilt
- Ziele für die Lehrveranstaltung
  - Erkennen und Beheben von Schwachstellen in Systemen
  - Praktische Umsetzung von Angriffstechniken
  - und natürlich viel Spaß ;-)

Aufbau der Übungsumgebung - Übersicht



Aufbau der Übungsumgebung - Bestandteile

- Definierte Hosts
- Server-Images
- IP Adressen der Images werden bekannt gegeben
- Zentraler Knoten (Logging!)
- Gameserver
- Clients: Inflab Rechner (eigene Boot CDs sind möglich), Notebooks

Images

- Alle Gruppen bekommen (fast) identes Image
  - Unterschied bei root Passwort und IP Adresse
- Dienste sind selbstentwickelte Applikationen mit Schwachstellen
  - Schwachstellen sollen behoben werden
  - Angriffe auf die Schwachstellen der anderen Images
  - Fehlkonfigurationen (Standardpasswörter, Berechtigungen, ...) können auch vorhanden sein
- Flags sind Daten der Dienste und werden periodisch vom Gameserver verteilt (ca. 1-5 min)
  - z.B. 0023A0DB76FF9DBA48979E24C39B408C

Zeitverlauf

- Aktivieren der Zugänge
- Analyse, Absicherung der Images ohne Bewertung
- Gameserver startet zeitverzögert mit der Bewertung
- CTF Contest läuft
- Nach Ende Siegerehrung und Protokoll

Voraussetzungen

- Organisatorische
  - StudentIn von Security for Systems Engineering oder IT Security in Large IT Infrastructures
  - Anmeldung für CTF per tuwel
- Kenntnisse
  - Kenntnisse aus Labs
  - Generelle Security Kenntnisse (Schwachstellen,...)
  - Linux-Kenntnisse

Vorbereitung Programmiersprachen

- Einarbeitung in unterschiedliche Programmiersprachen
- Wie können Schwachstellen behoben werden?
  - Validieren der Eingaben
  - Logische Fehler
- Programmiersprachen
  - C / C++, Perl, Java, PHP, Ruby, Shell Scripts, ...
  - Vielleicht auch Exoten wie von `http://en.wikipedia.org/wiki/Esoteric_programming_language`

Scripting

- Bei Scripts Denial of Service verhindern
- z.B. Sleep beim Abfragen
- Automatische Abgabe von Flags beim Gameserver optimieren (nur die letzten Flags abgeben und nicht sämtliche gefundenen Flags probieren). Durch Rundennummer im Flag können die aktuellen Flags erkannt werden.

Bewertung

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

Bewertung - lab2 (i)

- Wurde das Service analysiert und beschrieben?
- Wurden die vorhandenen Fehler gefunden und beschrieben? Vermutungen vorhanden?
- Welche Ansätze zur Behebung der Fehler möglich? Vermutung zur Behebung vorhanden?
- Welche Ansätze für Angriff gegen diesen Fehler?
- Welche Angriffe wurden durchgeführt bzw. versucht?
- Kreative Ideen für Angriffe und Verteidigung?
  - Anführen auch wenn diese nicht durchgeführt wurden
  - Beispiel: automatisierte Angriffe

Bewertung - lab2 (ii)

- Anzahl der bearbeiteten/beschriebenen Services (Punkte pro Service)
- Automatisierung des Angriffs
- Automatisierung von Flag Submit
- Analysen und Konfigurationstätigkeiten zur Härtung des Systems
- Punkteabzug bei formalen Fehlern (Vorlage 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.

Bewertung - Bewerb

- Verteidigung (Services müssen funktionieren, keine Angriffe)
- Angriff (Flags von anderen Teams sammeln)
- Verteidigung besser als Angriff
- Bonuspunkte (manuell: gute, kreative Lösungen anhand von Advisories)
- Bonuspunkte für ein Team wenn für alle Services zumindest einmal ein gültiges Flag gewertet wurde (Erhöhung der Punkte um 15% am Ende des Bewerbs)

Punkte für Angriffe

- Flags sind für einen beschränkten Zeitraum gültig. Rundenabhängig.
- Keine Punkte für eigene Flags
- Nach Übermittlung eines gültigen Flags an den Gameserver Punkte, abhängig von
  - Läuft das Service der eigenen Gruppe korrekt?
  - Anzahl abgegebener Flags des Teams von Service/Team $\rightarrow$ laufendes manuelles Ausnutzen des gleichen Services nicht zielführend

Punkte für Verteidigung

- Periodische Überprüfung der Services
- Service erreichbar, Punkte für erreichbare Services
- Service funktional, weitere Punkte für funktionale Services
- Kennzeichnung bei der Übersicht am Gameserver als “up”, “down” oder “broken”

- Wird ein gültiges Flag für ein Service eines Teams übermittelt, werden die Verteidigungspunkte für diese Runde annuliert.
- Übersicht der Punkteverteilung am Gameserver

Regeln

- **Angriffe außerhalb der Übungsumgebung sind verboten!**
- Es muss mit Konsequenzen vom Institut sowie der TU gerechnet werden.

- Den Anweisungen der Tutoren und VU-Mitarbeitern muss Folge geleistet werden.
- Regelverstöße können Punkteabzug bringen, gleich oder nach Analyse der Logs.
- Kein „gruppenübergreifender“ Kontakt
- Kein Kontakt mit externen Personen

Regeln – Verbote bei Angriffen

- ARP Spoofing
- DoS Attacken
- Server vom Netzwerk nehmen
- Flags löschen oder ändern
- Angriffe auf Gameserver
- Angriffe außerhalb der UE-Umgebung
- Angriffe auf Inflab Rechner oder Notebooks

Regeln – Verbote bei der Verteidigung

- Zugriffsbeschränkungen (Firewalls) auf Grund von IP Adressen
- Zugriffe auf Applikationsebene filtern (z.B. nur Gameserver erlauben)
- Aktivierung von Methoden, die Buffer Overflows verhindern
- Deaktivierung von Funktionen, die bei den Services auf der Website beschrieben sind

Regeln – Erlaubt ist

- Übermitteln der gefundenen Flags via Webinterface des Gameservers – erst dann zählt ein erfolgreicher Angriff

- Neukompilieren von Services
- Anpassen von Services/Scripts, solange die spezifizierte Funktion erhalten bleibt
- Anlegen von Backups von Konfigurationsfiles, ...
- Kreativität

Zusätzliche Hinweise

- Neue, zusätzliche Images stehen begrenzt zur Verfügung
- Tutoren/Mitarbeiter stehen bei Fragen zur Verfügung
  - z.B. Wenn Fehler am Gameserver vermutet
- Eventuelle Regelverstöße bitte unmittelbar an Tutoren/Mitarbeiter der VU melden
- Falls Sie denken, dass eine Gruppe unfair handelt, bitte teilen Sie uns das ebenfalls gleich mit.

- Regeln demnächst online
- Fragen dazu via e-mail/Übungsforum

CTF Ersatz

- Wenn parallel IT Security in Large IT Infrastructures besucht wird, ist CTF Ersatz verpflichtend
  - Punkte des CTF können nur für eine LVA verwendet werden
- Bitte eine mail an `lva.security@inso.tuwien.ac.at`.

Gruppenbildung Security for Systems Engineering

- Gruppen von 4 StudentInnen
- Fixe Anmeldung der Gruppen ab 01.06.2013 bis 07.06.2013
- Durchführung über tuwel (siehe Website)
- Name der Gruppe frei wählbar → Kreativität :) (Ueber ein TUWEL-Wiki)
- Gewinner vom SS 2012
  - “Apfelwasser”
  - “”; DROP TABLE Teams; –”

Termine

- 2 Termine mit fixen Plätzen
  - MI 12.06.2013 - Bewerb: 10:30-15:30, Einlass: ab 10:00, Preisverleihung ca. 16.00, Protokoll bis 17:00
  - DO 13.06.2013 - Bewerb: 10:30-15:30, Einlass: ab 10:00, Preisverleihung ca. 16.00, Protokoll bis 17:00
- Ort: Informatiklabor (`http://www.inflab.tuwien.ac.at/`)
- Anmeldung zu Terminen wird bei der Gruppenanmeldung über tuwel durchgeführt

Hinweise für die Vorgehensweise

- Backups von Dateien vor Änderungen
- Finden von Services
  - Benutzer am System (/etc/passwd, /home/*)
  - Prozesse untersuchen
  - Offene Ports und zugehörige Applikationen (netstat, lsof)
- Beispielhafte Schwachstellen
  - Fehlkonfigurationen / Standardpasswörter
  - Implementierungsfehler z.B. *-Injection, Overflows, ...
- Log-Dateien überwachen. Diese können wichtige Hinweise liefern.

Hinweise für die Vorgehensweise

- Überprüfen der Schwachstellen am eigenen Image. Dabei können auch die vorgenommenen Fehlerbehebungen untersucht werden.
- Angriffe wenn möglich automatisieren → Punkte für lab2 wenn dies im Protokoll beschrieben wurde
- Protokoll nicht nur am Ende erstellen sondern laufende Ergänzung des Protokolls
- Überprüfen Sie regelmäßig das Punkteranking am Gameserver → Kennzeichnung von fehlerhaften Services, Nachrichten der Übungsleitung, ...

Scripting

- Scriptsprachen: bash, perl, python
- HTTP Requests: wget, curl
- Netzwerk: telnet, netcat (nc)
- Zum Filtern/Suchen: grep, sed, awk
- Prozesse: netstat
- Dateien: ls, find, cat, tac, tail
  - Änderungen von Dateien verfolgen: `tail -f datei`
  - Zuordnung von offenen Dateien/Ports zu Prozessen: `lsof`

Script Beispiel vom CTF08 - (i)

```
#! /bin/bash
rm flag;
#getting flags
for i in `seq 100 1 108` `seq 110 1 111`;
do
  curl http://127.0.0.1:5${i}/~chatservice/userlist |
    sed 's/^.*::.*::.*::\(.*\)/\1/g' |
    grep -v steve >> flag ;
done
```

Script Beispiel vom CTF08 - (ii)

```
#! /bin/bash
rm flag
rm data
for i in `seq 100 1 108` `seq 110 1 111`; do
  echo $i;
  nc 127.0.0.1 6${i} -w 1 < input |
    grep patent-idea > data
done;
```

Script Beispiel vom CTF08 - (iii)

```
#submitting flags
for i in `cat flag`;
  do curl 'http://sela.inso.tuwien.ac.at:3207/submit.php?
team=109&flag='$i -u ctf:password;
done
```

Fragen

- Wenn Sie Fragen haben, stellen Sie sie jetzt!
- ...oder
  - stellen Sie Ihre Frage im tuwel Übungsforum
  - schreiben Sie uns ein e-mail:
    `lva.security@inso.tuwien.ac.at`

Weitere CTF Bewerbe

- ESSE nimmt bei weiteren internationalen CTF Bewerben teil
- Wenn Interesse besteht, können Sie sich gerne unter `http://www.defragmented-brains.at/` zu unserem Mailverteiler anmelden. Bei einer bevorstehenden Teilnahme senden wir die Information an alle InteressentInnenen aus.
- Die unterschiedlichsten Kenntnisse sind erforderlich, daher kann jeder/jede etwas beitragen.

Vielen Dank!

http://security.inso.tuwien.ac.at/