FH MÜNSTER
University of Applied Sciences

Masterprojekte 2024

Prof. Dr. Sebastian Schinzel

E-Mail: schinzel@fh-muenster.de

Themen

Themen:

1. Hacking: Automatisierung von Intrusion Detection und Incident Response für CTF-Wettbewerbe
2. Forschung: Aufbau eines Test-Labors mit LDAP-Servern und LDAP-Clients
3. Forschung: Revokation (Zurückrufen) von X.509-Zertifkaten

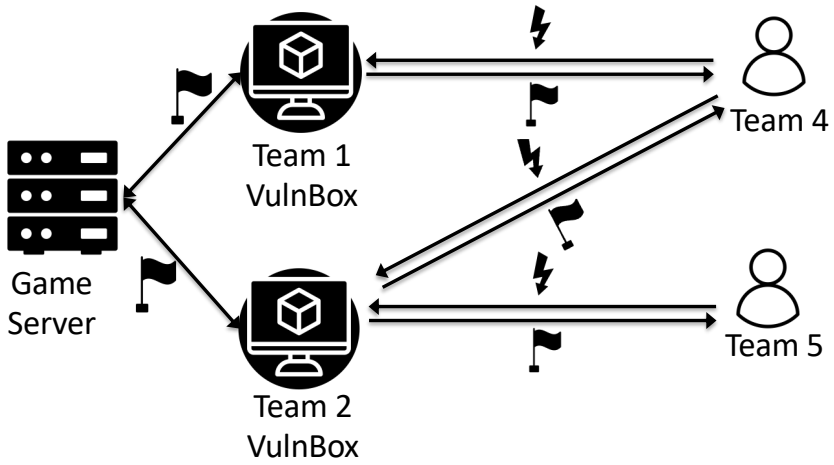
© Dr.-Ing. Fabian Ising, Prof. Sebastian Schinzel

1. Hacking:
   Automatisierung von Intrusion Detection und Incident Response für CTF-Wettbewerbe

Intrusion Detection und Response für CTF-Wettbewerbe

Bei Attack/Defense-CTFs bekommt jedes Team einen Server mit unsicheren Diensten, der vor Angriffen der anderen Teams abgesichert werden muss.

- Sowohl der (gute) Game-Server als auch die anderen (bösen) Teams sprechen mit diesen Diensten
- Die Analyse des Netzwerkverkehrs, besonders eingehende Anfragen, ist sehr wichtig!
  - Welche Anfrage ist legitim (Game-Server)?
  - Welche Anfrage ist ein Angriff anderer Gruppen?
  - Was ist eine angemessene Reaktion (Anfrage blockieren, weiterleiten, verändern, …)?
  - Was lernen wir aus der Anfrage über Sicherheitslücken im Dienst?



© Dr.-Ing. Fabian Ising, Prof. Sebastian Schinzel

FH MÜNSTER
University of Applied Sciences

Intrusion Detection und Response für CTF-Wettbewerbe

FlagHunter Services Exploits Traffic Teams Flags Statistics About Notifications 1 Admin Logout

Results

Raw PCAP-Files

Search (case sensitive!)

Time	Service	Application Protocol	Source	Size (Byte)	Flag Entry	Flag Exit
14:14:02 +0000 (18.11.2023)	turing-machines (2080 TCP)	Not Analyzed	**10.48.9.1**:17113	278584	No	Yes (3)
14:14:02 +0000 (18.11.2023)	turing-machines (2080 TCP)	HTTP	**10.48.9.1**:1640	26726	No	Yes (1)
14:14:12 +0000 (18.11.2023)	DjangoBells (8000 TCP)	Not Analyzed	**10.48.9.1**:33524	2828	No	Yes (1)
14:14:12 +0000 (18.11.2023)	DjangoBells (8000 TCP)	Not Analyzed	**10.48.9.1**:46931	2293	No	Yes (1)
14:14:13 +0000 (18.11.2023)	redisbbq (16379 TCP)	Not Analyzed	**10.48.9.1**:20400	1393	No	Yes (2)
14:14:13 +0000 (18.11.2023)	redisbbq (16379 TCP)	Not Analyzed	**10.48.9.1**:2367	818	No	Yes (1)
14:14:23 +0000 (18.11.2023)	DjangoBells (8000 TCP)	Not Analyzed	**10.48.9.1**:30659	2237	No	Yes (1)
14:14:24 +0000 (18.11.2023)	DjangoBells (8000 TCP)	Not Analyzed	**10.48.9.1**:52503	2237	No	Yes (1)

© Dr.-Ing. Fabian Ising, Prof. Sebastian Schinzel

FH MÜNSTER
University of Applied Sciences

Intrusion Detection und Response für CTF-Wettbewerbe

- Ziel: Entwicklung von Werkzeugen zur Abwehr von Cyber-Angriffen in CTF-Wettbewerben.
- Mögliche Features:
  - Transparenter TLS proxy
  - Mustererkennung Netzwerkverkehr
  - Modifikation oder Blockierung von Angriffen
  - Sandboxing
  - Aufbereiten von Netzwerkverkehr (für manuelle Analyse)
  - Automatische Schwachstellensuche
  - Automatisierte Angriffe gegen andere Teams

Mail: schinzel@fh-muenster.de, f.ising@fh-muenster.de

© Dr.-Ing. Fabian Ising, Prof. Sebastian Schinzel

2. Forschung: Aufbau eines Test-Labors mit LDAP-Servern und LDAP-Clients

FH MÜNSTER
University of Applied Sciences

Aufbau eines Test-Labors mit LDAP-Servern und LDAP-Clients

- Das Lightweight Directory Access Protocol (LDAP) wird internetweit z. B. für die Verwaltung von Benutzerstammdaten, aber auch für Zugangsdaten verwendet.
- In einem aktuellen Forschungsprojekt scannen wir im Internet nach öffentlichen LDAP-Servern, die sensible Daten preisgeben, wie z. B. Klartextpassworte
- In diesem Projekt soll aber die Sicherheit des LDAP-Protokolls inklusive gängiger LDAP-Server-Programme wie OpenLDAP, Microsoft Active Directory, … untersucht werden.

© Dr.-Ing. Fabian Ising, Prof. Sebastian Schinzel

FH MÜNSTER
University of Applied Sciences

Aufbau eines Test-Labors mit LDAP-Servern und LDAP-Clients

LDAP-Server:

- In einer virtuellen Umgebung sollen alle gängigen LDAP-Implementierungen installiert werden
- Im nächsten Schritt sollen automatisierte Tests gegen alle LDAP-Server gefahren werden.
- Gefundene Sicherheitslücken melden wir dann an die Hersteller.

© Dr.-Ing. Fabian Ising, Prof. Sebastian Schinzel

FH MÜNSTER
University of Applied Sciences

Aufbau eines Test-Labors mit LDAP-Servern und LDAP-Clients

LDAP-Clients:

- Auch LDAP-Clients (z. B. Outlook, Thunderbird, Mac OS X, …) sollen auf Sicherheitslücken untersucht werden.
- Dafür müssen diese Clients auch in virtuellen Umgebungen installiert werden und (teil-)automatisiert getestet werden.
- Für diese Tests müssen evt. eigene vereinfachte LDAP-Implementierungen entwickelt werden, die versuchen Fehler in LDAP-Clients zu provozieren.
- Auch hier: gefundene Sicherheitslücken melden wir dann an die Hersteller.
- Ziel: Erstellung und Veröffentlichung eines wissenschaftlichen Papiers!

© Dr.-Ing. Fabian Ising, Prof. Sebastian Schinzel

3. Forschung: Revokation (Zurückrufen) von X.509-Zertifkaten

© Prof. Sebastian Schinzel

Revokation (Zurückrufen) von X.509-Zertifkaten

- X.509-Zertifkate werden z. B. bei TLS oder auch S/MIME verwendet.
- Die Revokation beschreibt das Zurückziehen der Gültigkeit eines Zertifkats (z. B. weil Angreifer Zugriff auf Privatschlüssel hatten).
- Zertifkatssperrlisten werden von Certificate Authorities(CAs) veröffentlicht.
- Das Online Certificate Status Protocol (OCSP) ist eine Alternative zu diesen Sperrlisten.

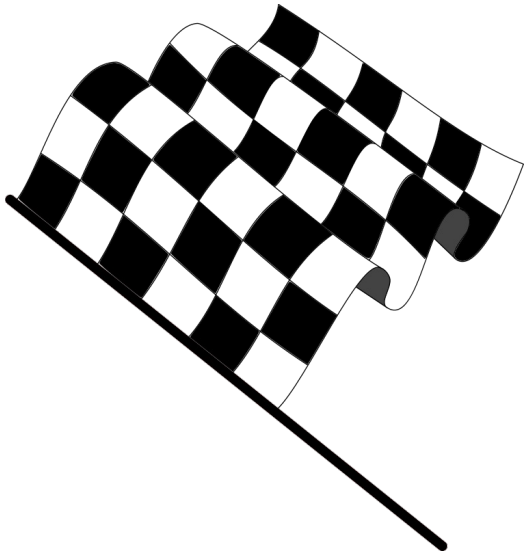
© Dr.-Ing. Fabian Ising, Prof. Sebastian Schinzel

FH MÜNSTER
University of Applied Sciences

Revokation (Zurückrufen) von X.509-Zertifkaten

- In diesem Projekt soll die Revokation-Infrastruktur weltweit bei allen gängigen Certificate Authories gemessen werden (für CRLs und OCSP).
  - Wie gut sind die Dienste für CRLs und OCSP erreichbar (Downtime)?
  - Wie schnell werden Zertifikate gesperrt, wenn sie als kompromittiert gemeldet werden?
  - Können Angreifer Zertifikate sperren lassen, die ihnen gar nicht gehören?
- Gefundene Sicherheitslücken melden wir an die CAs.
- Ziel: Erstellung und Veröffentlichung eines wissenschaftlichen Papiers!

© Dr.-Ing. Fabian Ising, Prof. Sebastian Schinzel



Interesse geweckt?

Melden Sie sich bei
Prof. Dr. Sebastian Schinzel per
Mattermost oder E-Mail:
schinzel@fh-muenster.de