Fachhochschule Nordwestschweiz
Hochschule für Technik

Cyber Security Labor (cysL)

Fachhochschule Nordwestschweiz
Hochschule für Technik

Cyber Security Labor (cysL)

u.ä. auslagern (modularisieren verbessern)

Inhalt

Inhalt

Vorbereitung

Recherche

Versuchen sie doch einmal alle “Barriers” die ein OS aufzubieten hat zu kategorisieren. Welche Grenzen können einfach kontrolliert werden und welche nur schwer?

Zum lesen oder anschauen ...

Eine triviale Attacke auf den Speicher von XML: Billion Laughs
Eine triviale Attacke auf den Diskplatz: ZIP Bomb
Eine triviale Attacke auf die CPU: Fork Bomb
Ein kleiner Primer für Buffer Overflows: Smashing the Stack
Warnung: Die Beispiele für “Smashing the Stack” funktionieren nur auf einem 32-Bit OS unmodifiziert.

Begriffe

Buffer Overflow, Logic Bombs

Spass mit Sicherheit

Normale Leute haben ein Aquarium

Normale Leute haben ein Aquarium

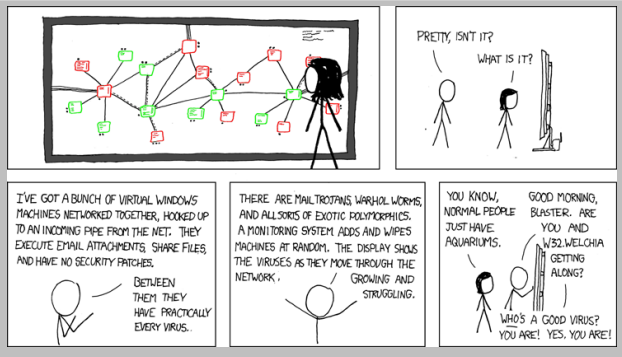

Abbildung: Andere haben ein Aquarium

Quelle: XKCD

Die lokalen, technischen Attacken

Die verschiedenen Buffer Overflows

Diverse Overflow-Attacken

- Stack Overflow
- Heap Overflow
- Format String Attacks
- Integer overflow

Die lokalen, technischen Attacken

Das Metasploit Framework (MSF)

Das Metasploit Framework (msf)

Metasploit ist ein Framework um Attacken verschiedenster Art vorzubereiten und durchzuführen. Es ist typischerweise ein Skript-Kiddy-Tool (ausser Personen beginnen selber Exploits zu schreiben).

Die lokalen, technischen Attacken

Angriffe

Angriffsszenarien

- Lokale HW
- Lokale Ausführung (“EXE” Ausführen)
- Netzwerkdienst (Service)
- Ein Netzwerksocket-Client oder dessen Plugins

Die lokalen, technischen Attacken

Angriffs-Detektion

Detektion

- Malware-Scanner
  - Pattern matching
  - Behavioural Detection
  - Statistical Detection
- HW Features
  - DEP
  - NX
- OS features
  - ASLR
- Applikationsfeatures
  - Canaries

Die lokalen, technischen Attacken

Detection Circumvention

Detection Circumvention

- Via dynamischem Code
- Harmlos aussehen
- Payload hiding
- Debugger detection
- Dynamic loading

Die lokalen, technischen Attacken

Gegenmassnahmen

Detektion

- Stufe 0: Sicheren Code schreiben
- Stufe 1: Programme (speziell Browser und Plugins) in Anzahl und komplexität minimieren und patchen.
- Stufe 2: Anti Malware
- Stufe 3: OS randomisation (Speicherverwürfelung/ASLR)
- Stufe 4: Zusätzliche OS Boudaries verwenden
- Stufe 5: HW boundaries (NX, DEP et.al.)

Aufgabe

Nächster Block

- Nehmen Sie die VM von //share/public/documents/CyslAufgabe1/nullbyte.ova und installieren Sie diese auf dem Rechner (das OVA-File stammt von VulnHub).
- Installieren Sie Kali-Linux
- Greifen Sie die Maschine an (sie dürfen einen Walkthrough wie `https://www.nuharborsecurity.com/blog/nullbyte-1-walkthrough` verwenden)

Repetition

Nächster Block

Nächster Termin

Einreichen Übung 1 vor Beginn der Lektion 8 am 04.11.2025 (in 82235 Tagen)