Prüfungsprotokoll Vertiefungspüfung VVS 1, VVS 2, Forensik (nach Buch), Datenkommunikation (nach Buch) bei Prof. Freiling in Mannheim

Lars Hermerschmidt

12.2.2007

Die Prüfung war eine Verbesserungsprüfung und wurde mit 1,0 bewertet. Prüfungsathmosfäre war sehr entspannt, ich habe nicht alle Fragen komplett beantwortet, zum Teil hat Prof. Freiling sie auch selber beantwortet.

1 VVS 2

- FLP, was man damit zeigt und den gesamten Beweis mit Preposition 1
- Pseudo Consensus Algo, unendlichen Pfad zeigen. Was kann man machen wenn man P hat? *Man kann auf die Nachrichten der korrekten Prozesse warten*
- Wenn man Ω hat, was macht man dann? *Man wartet auf den trusted Prozess den Ω ausgibt*
- Was ist wenn man das selber ist? *Dann werden die anderen auf einen warten, man muss sich um nichts kümmern*
- Wenn man $\Diamond$ W hat, wie emuliert man dann Ω?

2 Datenkommunikation

- In der Praxis nimmt man an, das das Internet ein Asynchrones System ist. Man kann also keinen Consensus machen, aber er wird doch täglich implementiert. Ist das ein Wiederspruch? *Nein, da in der Praxis die Algorithmen in ein paar Spezialfällen nicht funktionieren. (Bsp. 2 Phase NBAC, manchmal stürzt der Rechner einfach ab) Man hat aber in der Realität Timeouts die nicht überschritten werden können.*
- Wenn man in der Praxis jetzt einen Fehlerdetector implementieren will und man kennt den Timeout wie macht man das, z.B. in C? *Wenn man kann Ping benutzen oder UDP*
- Warum UDP? *Das sind rohe IP Pakete, da kann man machen was man will. TCP macht ja FIFO from Socket to Socket, aber puffert die Daten. Bei TCP müsste man also immer das Push Flag setzen, damit die I'm alive Nachricht des Fehlerdetektors auch gesendet wird.*
- Wie ist denn das bei TCP wenn keine Daten gesendet werden, sendet TCP dann selber Daten damit die Verbindung nicht Timeouted? *Ja wird es wohl*
- Kann man denn TCP Pakete ohne Daten senden? *Ja, z.B. beim 3 Wege Handshake wird das gemacht*

3 VVS 1

- Wenn man zwei Rechner hat, die so einen Fehlerdetektor mit TCP machen, wie kann man den einen lahmlegen und den anderen glauben lassen, das alles in Ordnung ist? *RST-Daemon auf einen, dann TCP Verbindung mit seiner Adresse als Absender machen und sagen: "Ich bins, ich war kurz down, aber jetzt ist wieder alles in Odnung". Man könnte auch Konnection Hijacking machen*
- Wie funktioniert Fragmentierung bei IP? *IPID, Router fragmentieren, Empfänger defragmentiert*

- Holt ein Codefragment aus dem Hackerpraktikum raus. Was kann man hier machen? *Eins war ein Bufferoverflow, da musste man sich überlegen in welchen Buffer man jetzt was überschreiben kann wenn man keinen Code einschleusen will sondern die Authentifizierung austrixen will (Stack Aufbau). Das ander war eine Racecondition.*

4 Forensik

- Wie ist das Forgehen wenn man an einem Tatort Beweise sichern soll? *Bla Bla, kommt drauf an wie der Computer zu dem Verbrachen steht, gehört er dem Täter/Opfer.*

- Mal speziell, wenn ein Hacker von dem Rechner aus ein Unternehmen angegriffen hat und gerade von der Tastatur weggezerrt wurde. *netstat -anp, Prozesse mit gcore dumpen, Uhrzeit des Rechners festhalten, Dokumentieren mit Kamera, das man nichts verändert. Per Netcat Ausgaben von Kommandos auf sicheren Rechner pipen. Wenn die Festplatten verschlüsselt sind und gemountet sind, sollte man versuchen die Schlüsseln aus dem Arbeitsspeicher zu dumpen.*

- Was ist wenn der Rechner ein Rootkit hat? *Wenn der Hacker es noch aktivieren konnte, hat er warscheinlich alle Spuren damit verwischt (Speicher dumpen liefert auch nur noch Nullen, wenn er das will). Man würde nur sehen das da ein Rootkit läuft, wenn man sich die Festplatte in einem sicheren OS anschaut, was ja nicht geht wenn sie verschlüsselt ist.*