

# Neighbourhood Watch

- Wachsende Zahl von Angriffen erhöht das Risiko von Systemausfällen
- Darum müssen Systeme „abgedichtet“ werden
- Penetrationstests sind ein Mittel um dies zu unterstützen

## Penetrationstests (2/2)

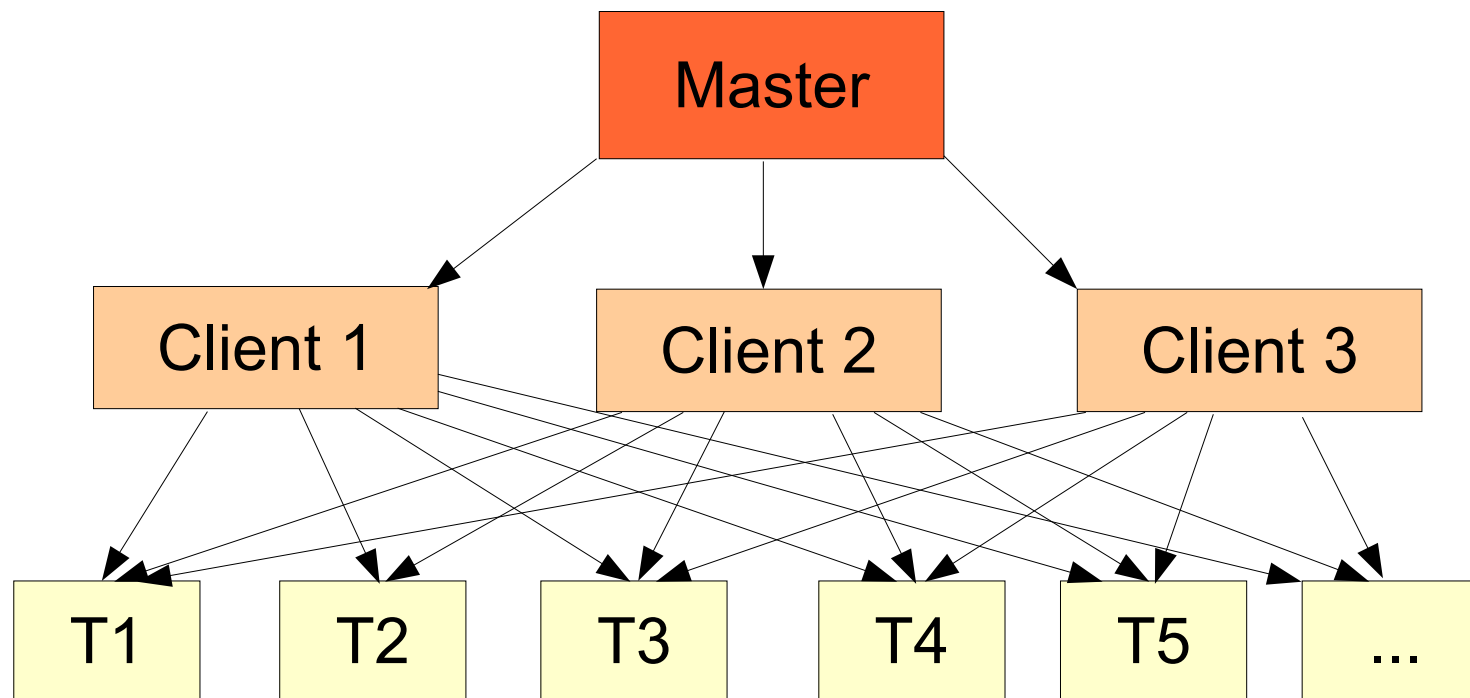
---

- Bereits einige Systeme für Pentests auf dem Markt
- Viele verwenden das OS-Tool Nessus
- In der Regel haben diese Systeme aber Nachteile
  - Hohe Netzlast durch Scan
  - Geringe Skalierbarkeit

- Scans werden über einen Monat verteilt ausgeführt
- Modulare Architektur
  - Neue Scantools jederzeit einbaubar
- Das Scannen selbst kann auf mehrere Rechner verteilt werden
  - bessere Skalierbarkeit
- Auch große Netzwerke mit verschiedenen Netzblöcken können bedient werden

- “Adhoc-Scans” („Notfallscans“)
  - bei akuter Gefahr kann NBHW über einen Tag verteilt scannen
- Umfassende Reportfunktion
  - differenziell, mit Advisoryreferenzen
- Sehr große Verbesserung der Sicherheit mit sehr wenig Aufwand
  - bedeutet aber auch: keine Spezial-/Einzeluntersuchung
  - 80/20-Regel

- Verteilung maximiert die Abstände zwischen zwei Scans auf einem Target
- Scans können einander bedingen und ausschließen
- Durch Scanklassen kann den Wünschen des Kunden sehr genau entsprochen werden



## Kleines Rechenbeispiel

---

<b>Netzwerk</b>	65534 Hosts
<b>Nessus-Scans</b>	72534 (inkl. gesamter Portscan)
<b>Datenmenge / Scan</b>	84 Bytes
<b>Datenmenge (ges.)</b>	372 GiB (399 GB)
<b>Verteilt über 20 Minuten</b>	2,7 GBit / s
<b>Verteilt über 6 Stunden</b>	147,9 MBit / s
<b>NBHW-Verteilung</b>	1,3 MBit / s

- NBHW wird noch ökonomischer durch weitere Scaneinsparung
- Verteiltheit wird noch weiter ausgebaut
- Höhere Interaktionsmöglichkeit

- Penetrationstests sind wichtig für ein sinnvolles Sicherheitskonzept
- NBHW bietet belastungsarme Pentests auch für große Netzwerke
- Dies ist nur der Anfang...

