Team 10 - Moritz Rupp, Viktor Brandl

Frage 5.1

Bei vielen Anwendungen spricht man von Server und Client. Wie heißen die jeweiligen Pendants im Domain Name System?

Nameserver und **Client**

Frage 5.2

Wo wird der Client unter Linux konfiguriert?

unter /etc/resolv.conf

Frage 5.3

Welche Funktionen hat openssl? (Hinweis: Es sind viel mehr als es auf den ersten Blick erscheint.)

- Erstellung und Management von Public keys, Private keys und dazugehörigen parametern.
- Erstellung von X.509 Zertifikaten, CSRs und CRLs
- Berechnung von MD 4,5 etc.
- Verschlüsselung und Entschschlüsselung von chiffren
- SSL/TLS Client und Server Tests
- Zeitstempel requests, Generierung und Verifizierung

Frage 5.4

Welche Arten von Ressource Records kennen Sie und was für Rückschlüsse lassen sich anhand dieser auf das Gesamtsystem ziehen?

- **A** Ipv4-Adresse
- **AAAA** Ipv6-Adresse
- **HINFO** CPU und OS des Hosts
- **MX** Info unter welcher Domain ein Mailserver zu erreichen ist.
- **CNAME** Name eines Alias
- **NS** Autorativer Name-Server
- **PTR** Pointer zu einem anderen Teil des Domain Name Space
- **SOA** Informatonen zur DNS-Zone.
- **CERT** Public Key-Zertifikate
- **TXT** Zusätzliche Informationen. Häufig um weitere Dienste zu Identifizieren.

Frage 5.5

> Was ist ein Zonentransfer und weshalb kann er zur Erkundung eines Systems interessant sein (Thema reconnaissance beim Pentest)?

Beim Zonentransfer überträgt, ein DNS-Server eine Zone mittels AXFR, auf einen anderen. Dieß ist z.B. für den Ausfallschutz nützlich. Mittels eines Zonentransfers können häufig Informationen zur Netzwerkinfrastruktur gesammelt werden ohne das IDS oder IPS auszulösen, da der DNS-Traffic oft nicht überwacht wird.

Frage 5.6

> Wie läuft ein TCP Scan bei nmap technisch ab? Wo liegt der Unterschied beim TCP-Connect-Scan und beim TCP-Syn-Scan? Kennen Sie weitere Arten mit nmap zu scannen?

Nmap versucht eine TCP Verbinding zu angegebenen Ip Adressen bzw. Port anhand eines SYN Packets aufzubauen. Folgt keine Antwort ist der Port Firewalled. Ist die Antwort ein RST Packet ist der Port zu. Ist es ein ACK(SYN/ACK) Packet ist der Port offen.

Der TCP-Connect Scan stellt eine komplette Verbindung mit dem Zielhost her, wobei der TCP-SYN Scan nur eine teilweisige Verbindung aufbaut.

Beispiel TCP-SYN SCAN:
SYN —>
SYN/ACK <—
RST —>

Beispiel TCP-Connect Scan:
SYN —->
SYN/ACK <——
ACK —->
<—— DATA
RST —->
Weitere Arten mit nmap zu scannen:
- UDP Scan
- Idle Scan
- RPC Scan
- FIN Scan
- Ping Scan

Frage 5.7

> Im Praktikum haben Sie sich vor allem mit TCP beschäftigt. Viele der Netzwer- kinfrastrukturdienste sind jedoch keine TCP Dienste.

Worauf sollten Sie bei der Erkundung eines Systems ebenso achten?

Ebenso sollte darauf geachtet werden, ob Dienste über UDP laufen.