IT-Sicherheit2 - Praktikum 1 - Durchführung

Inhaltsverzeichnis

1 Teil 1 + 2 Reconnaissance, Portscans mit NAMP und Angriffe mit CAIN

1. Teil: Aktives Reconnaisance - Portscans mit NMAP

ITS2-1-1-3

Mit welcher NMAP-Version arbeiten Sie? 6.46

Richtig!

Auswerten

ITS2-1-1-4

Angenommen die IP-Adressen der Systeme die Sie pingen wollen wären 10.0.0.1 und 10.0.0.3.

Welche Befehle verwenden Sie?

Befehl 1: ping 10.0.0.1

Befehl 2: ping 10.0.0.3

Richtig!

Auswerten

ITS2-1-1-6

Welchen Befehl verwenden Sie?

- (●) nmap –sT [ip-adresse]
- ( ) nmap –iL [ip-adresse]
- ( ) nmap T [ip-adresse]
- ( ) nmap sT [ip-adresse]
- ( ) nmap –F [ip-adresse]
- ( ) nmap –PO [ip-adresse]
- ( ) nmap –P [ip-adresse]

Richtig!

Auswerten

ITS2-1-1-7

Welche offenen TCP Ports hat NMAP gefunden?

- [x] 23
- [ ] 53
- [x] 80
- [ ] 123
- [x] 135
- [x] 139
- [ ] 443
- [x] 445
- [x] 1025
- [x] 1026
- [ ] 2009
- [x] 3389
- [ ] 4888

Richtig!

Auswerten

ITS2-1-1-8

Wie lautet der benötigte Filterstring? tcp.port==1111

Richtig!

Auswerten

ITS2-1-1-9

Wenn Sie nur das Paket, das nmap sendet, aufzeichnen wollen, muss im Filterstring noch die IP Adresse berücksichtigt werden. (Hinweis: die IP-Adresse sei 10.0.0.2)

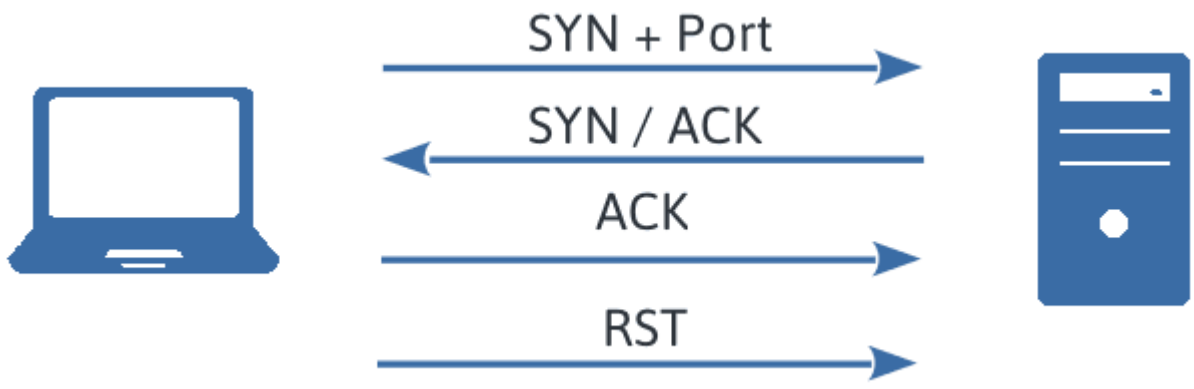
Wie lautet dieser Filterstring? (tcp.port==1111)and ip

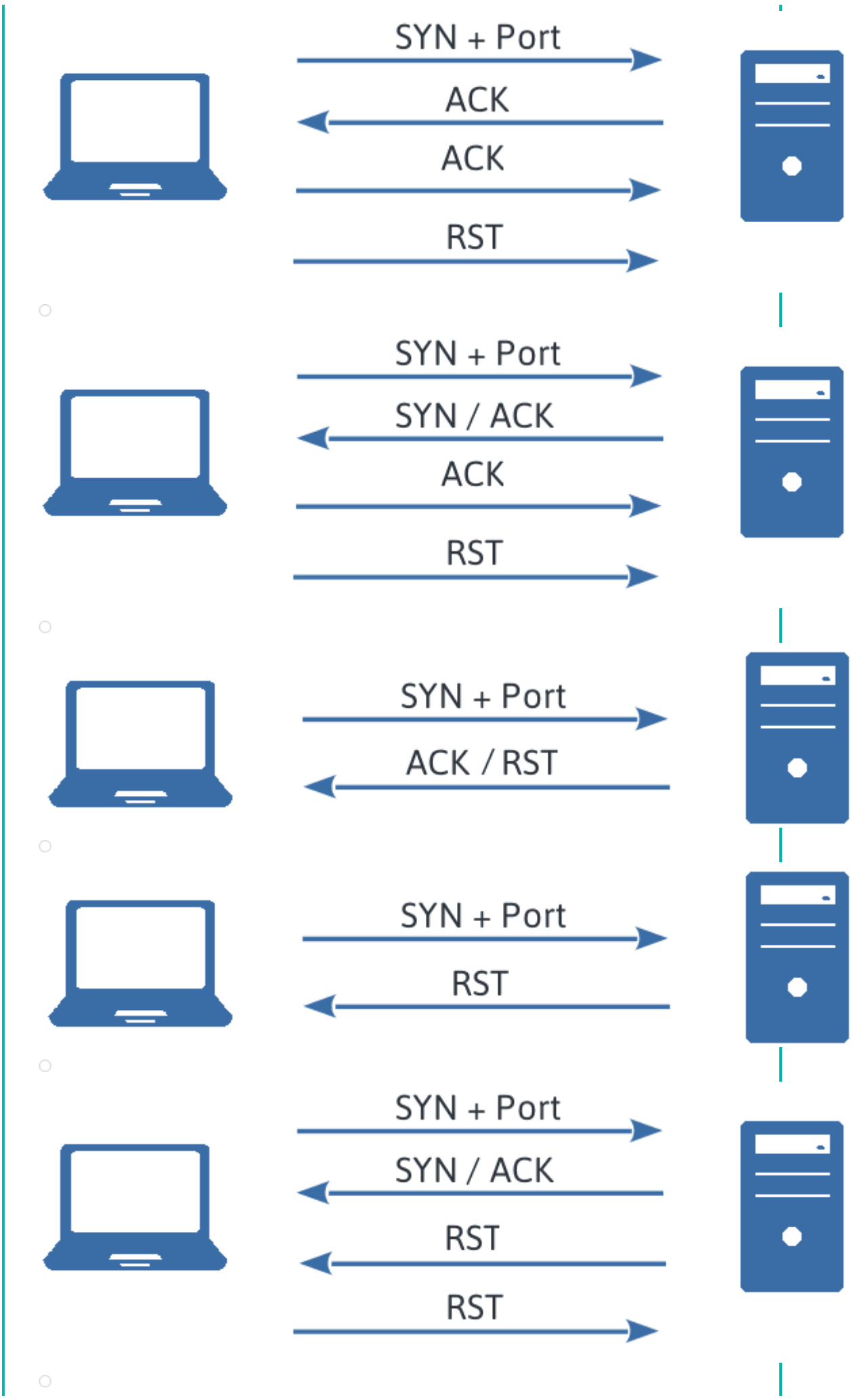
Richtig!

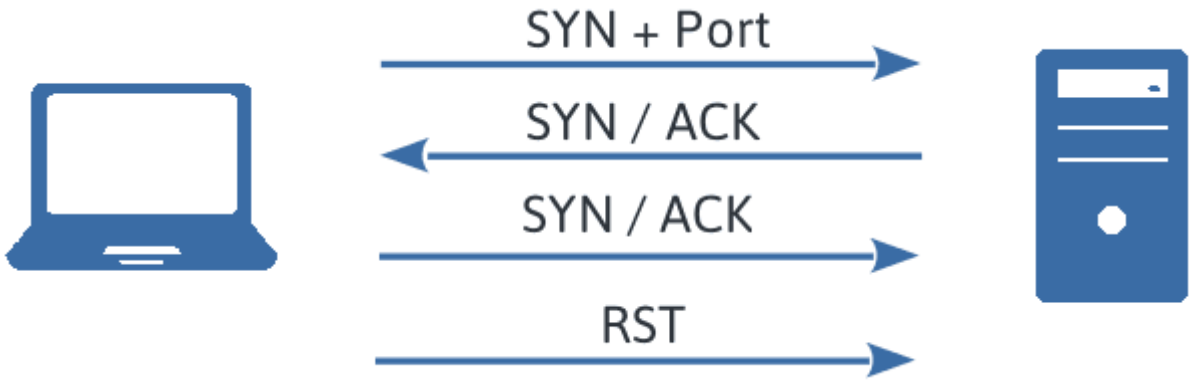
Auswerten

ITS2-1-1-10

Welches Bild stellt den Kommunikationsablauf eines TCP-Scans mit geöffneten TCP Ports dar?




SYN + Port
ACK
ACK
RST
SYN + Port
SYN / ACK
ACK
RST
SYN + Port
ACK / RST
SYN + Port
RST
SYN + Port
SYN / ACK
RST
RST

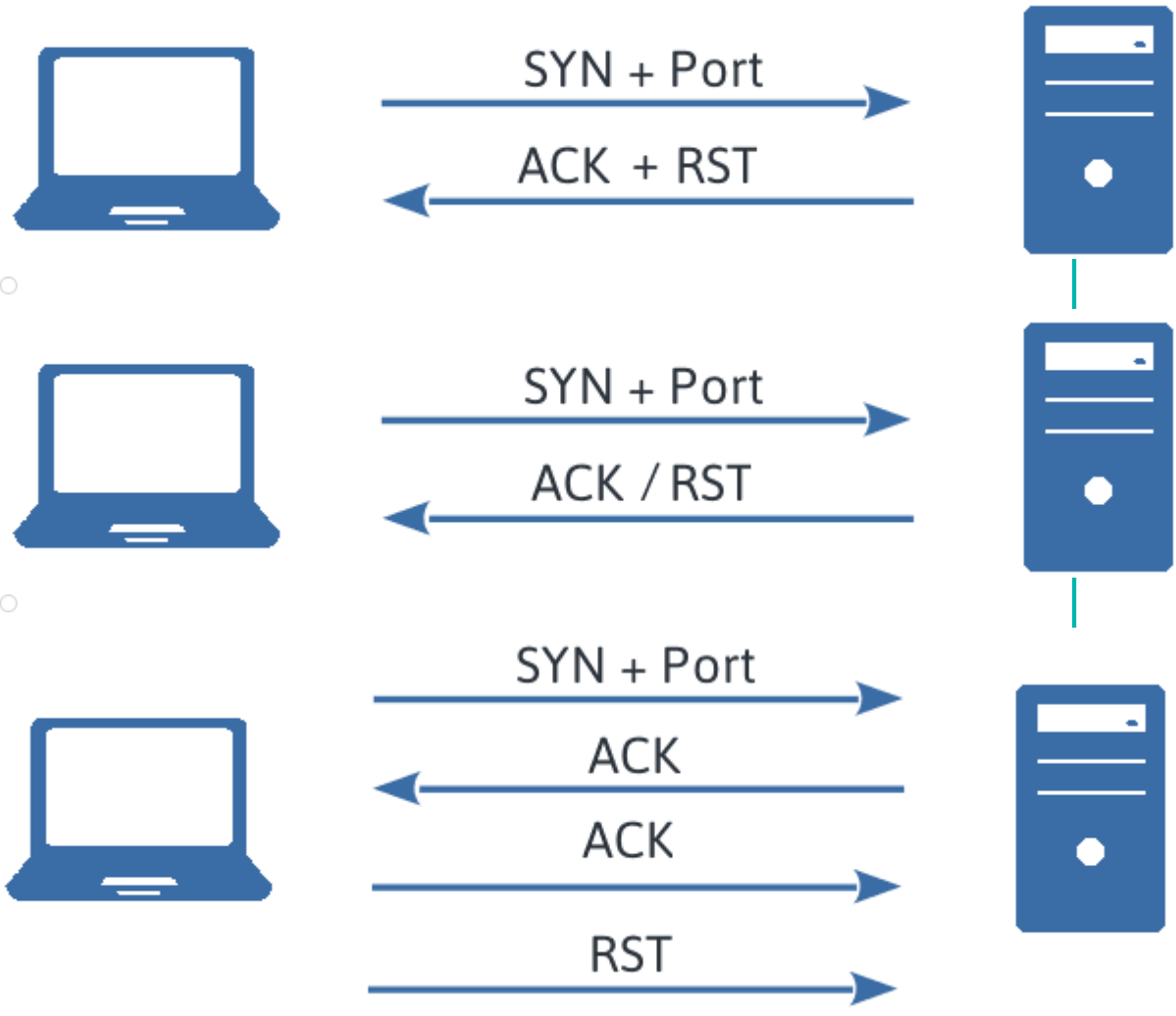


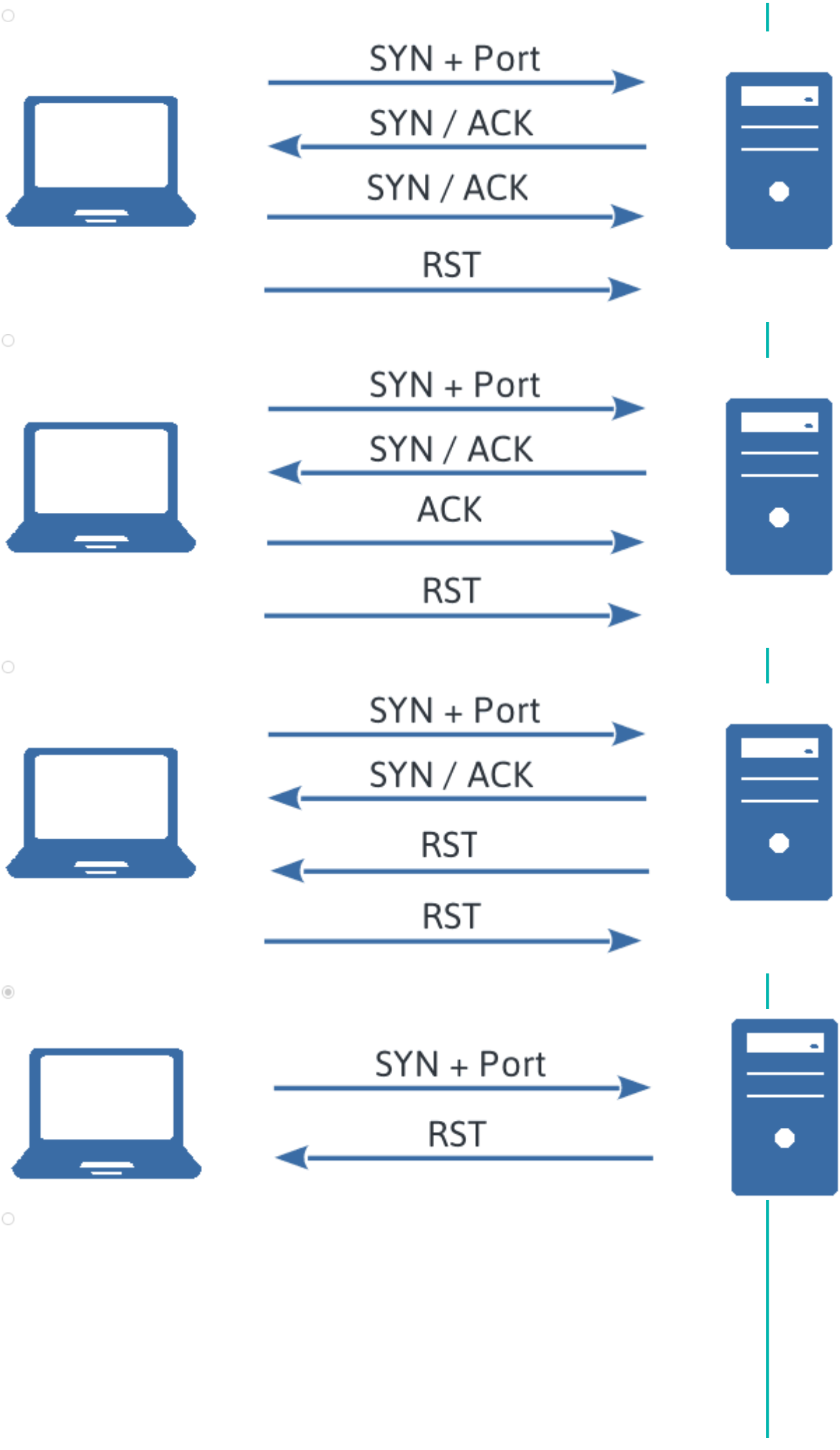
Richtig!

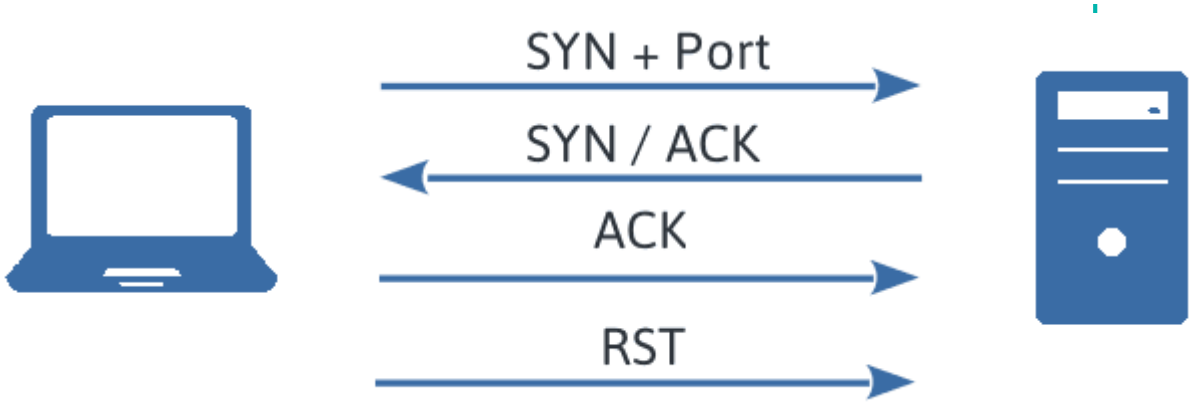
Auswerten

ITS2-1-1-11

Welches Bild stellt den Kommunikationsablauf eines TCP-Scans mit geschlossenem TCP Ports dar?




SYN + Port
SYN / ACK
SYN / ACK
RST
SYN + Port
SYN / ACK
ACK
RST
SYN + Port
SYN / ACK
RST
RST
SYN + Port
RST



Richtig!

Auswerten

ITS2-1-1-12

Wie viele Verbindungen baut NMAP (etwa) pro Sekunde zum Server auf?

- ca. 70-100
- ca. 1-5
- ca. 40-70
- ca. 100-140
- ca. 5-40

Richtig!

Auswerten

ITS2-1-1-13

In welchem Abstand werden die Scans bei dem Parameter –T1 gestartet?

- ca. 10 Scans pro Sekunde
- ca. 5 Scans pro Sekunde
- ca. 1 Scan pro Sekunde
- ca. 1 Scan in 5 Sekunden
- ca. 1 Scan in 10 Sekunden

ca. 1 Scans in 20 Sekunden

ca. 1 Scans in 30 Sekunden

ca. 1 Scan pro Minute

ca. 1 Scan in 2 Minuten

Richtig!

Auswerten

ITS2-1-1-14

Welchen Befehl müssen Sie verwenden (ohne IP-Adresse)?

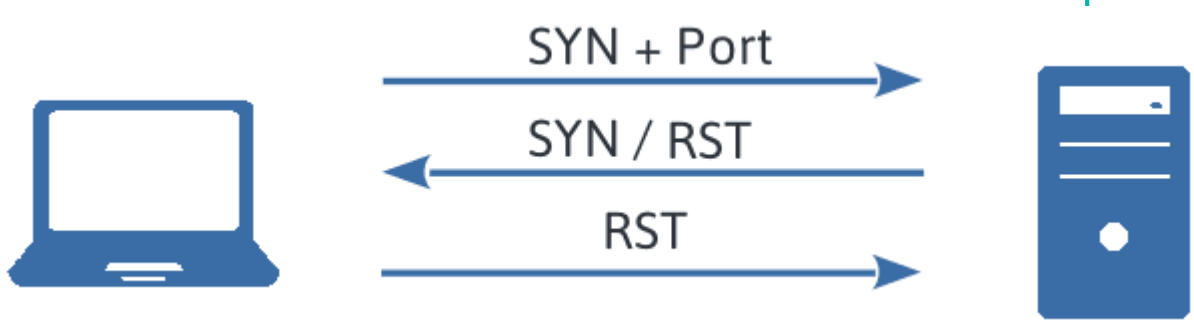
Befehl: nmap -sS

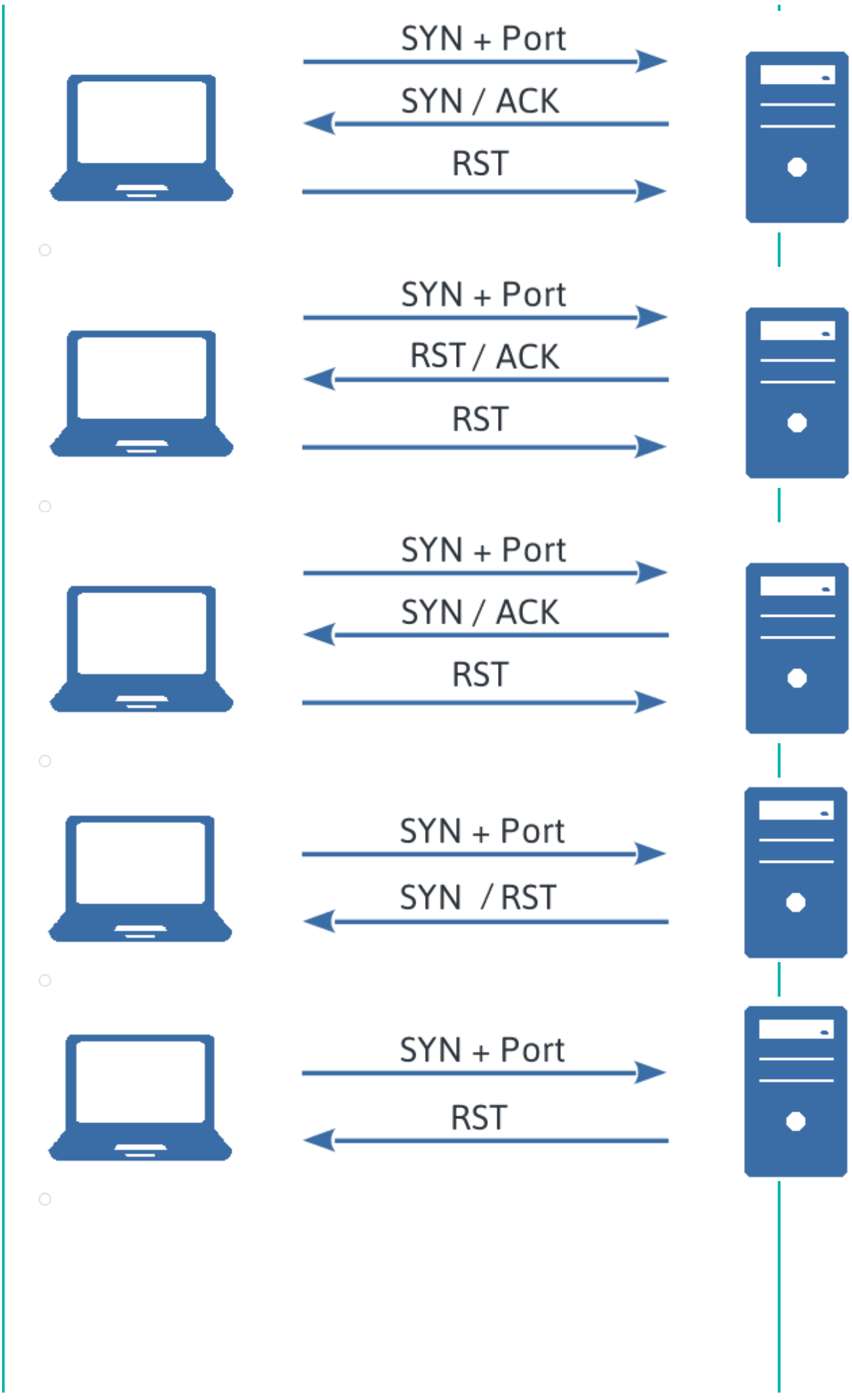
Richtig!

Auswerten

ITS2-1-1-15a

Welches Bild stellt den Kommunikationsablauf eines Stealth Scans mit geöffneten TCP Ports dar?



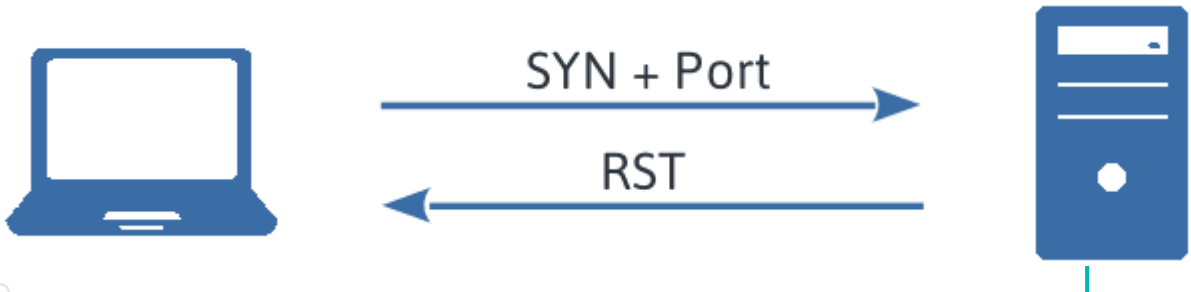

SYN + Port
SYN / ACK
RST
SYN + Port
RST / ACK
RST
SYN + Port
SYN / ACK
RST
SYN + Port
SYN / RST
SYN + Port
RST

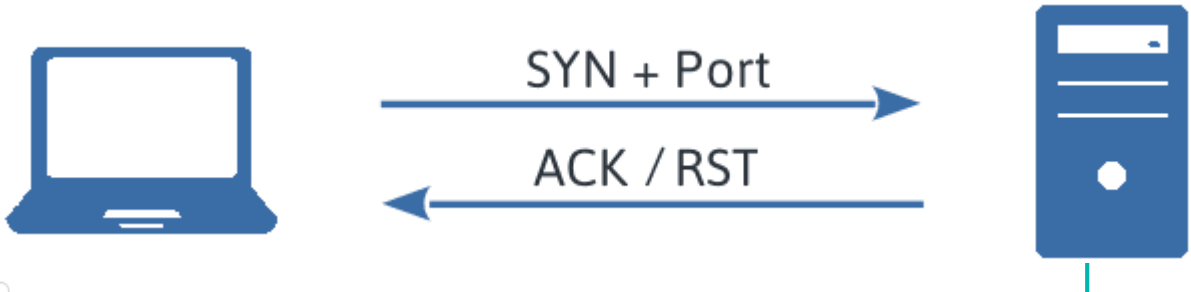
Richtig!

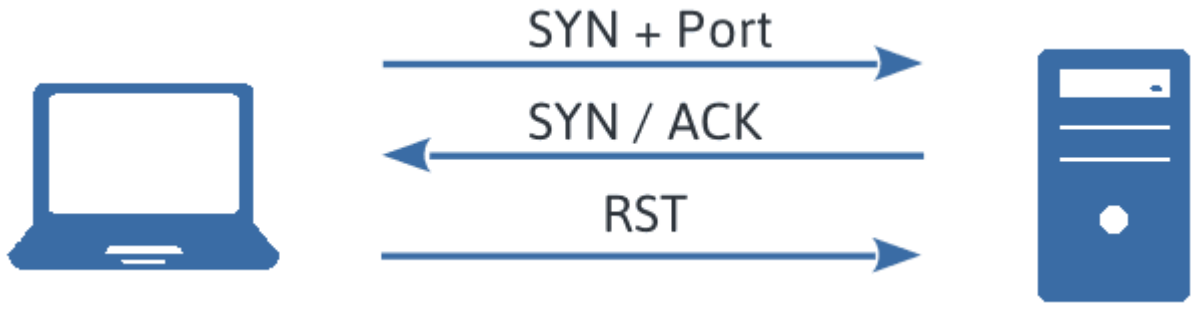
Auswerten

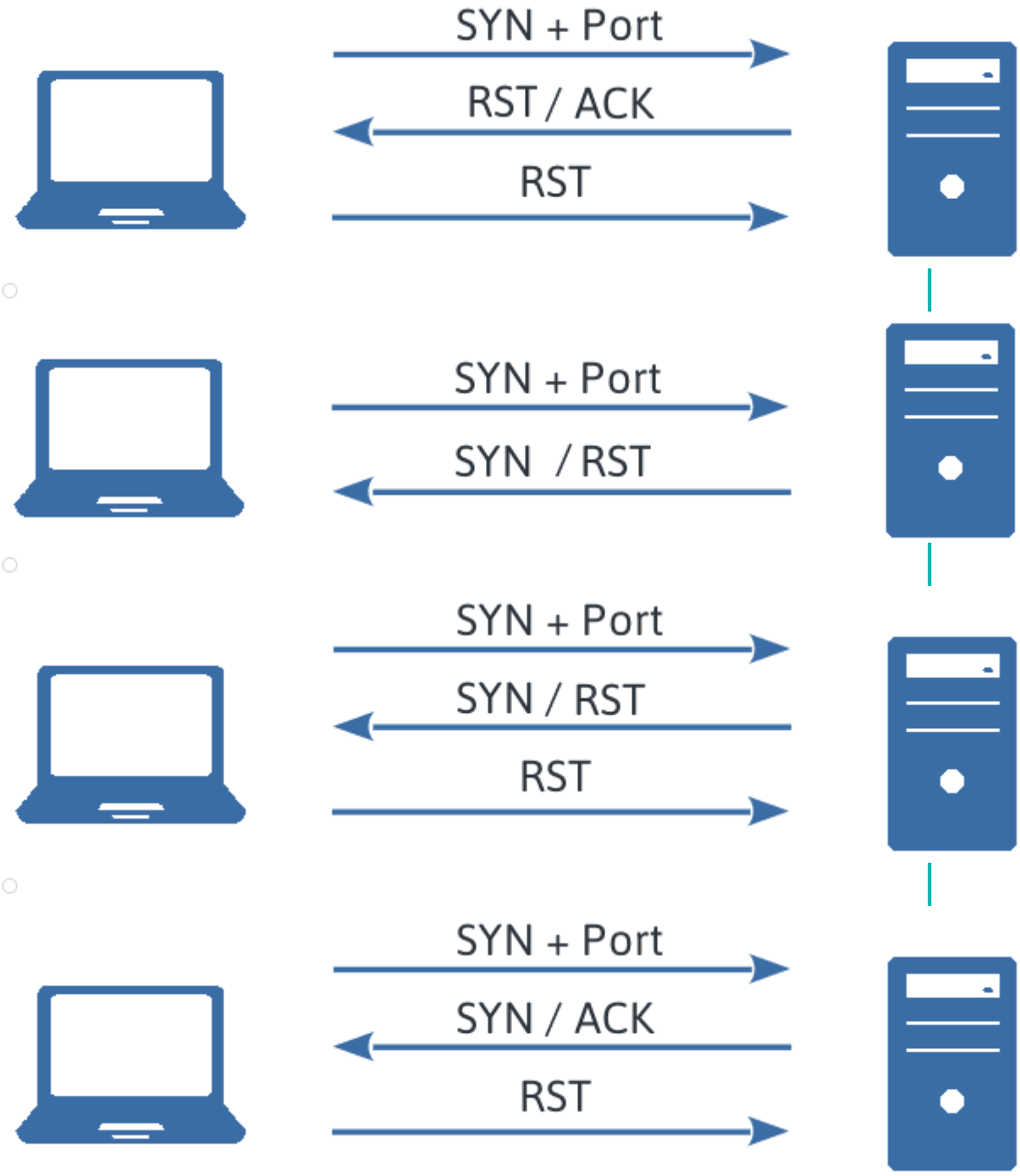
ITS2-1-1-15b

Welches Bild stellt den Kommunikationsablauf eines Stealth Scans mit geschlossenen TCP Ports dar?









Richtig!

Auswerten

ITS2-1-1-16

Wie lautet der entsprechende Befehl (ohne IP Adresse)?

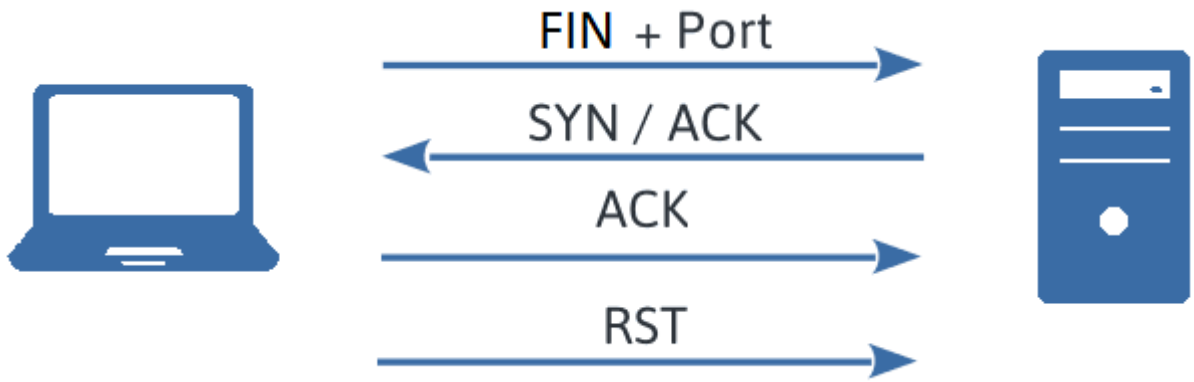
Befehl: nmap -sF

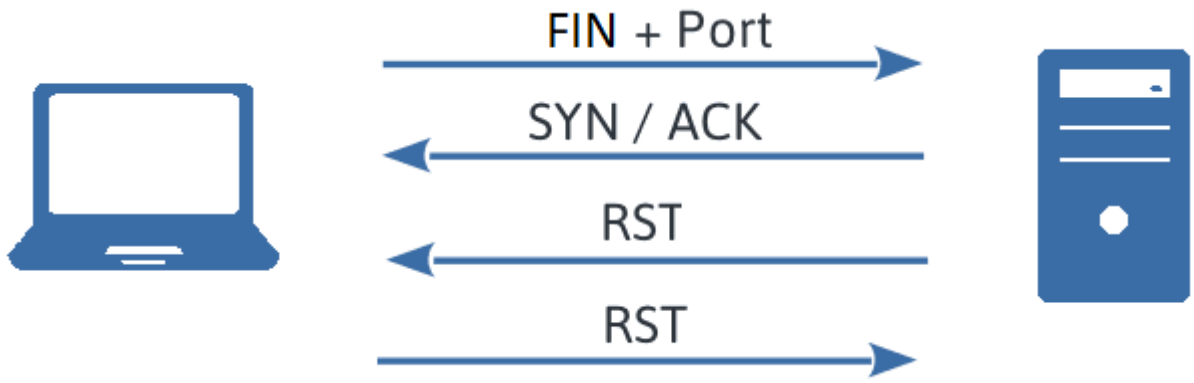
Richtig!

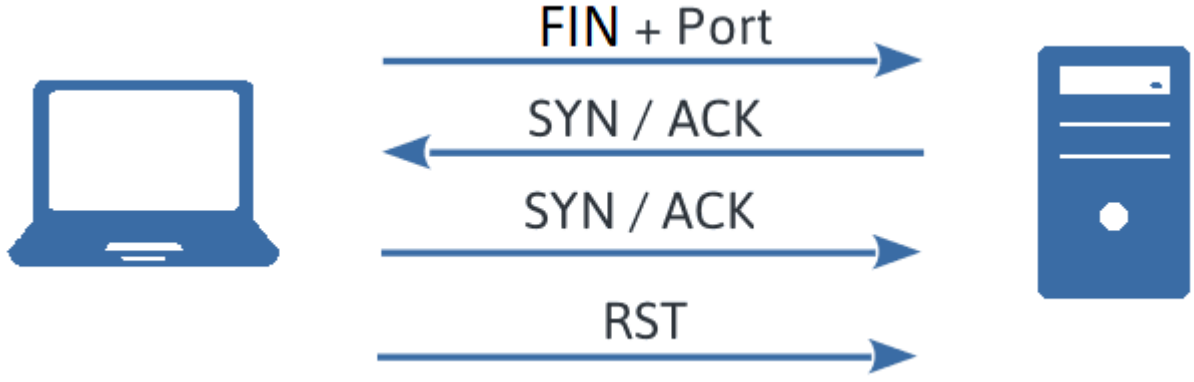
Auswerten

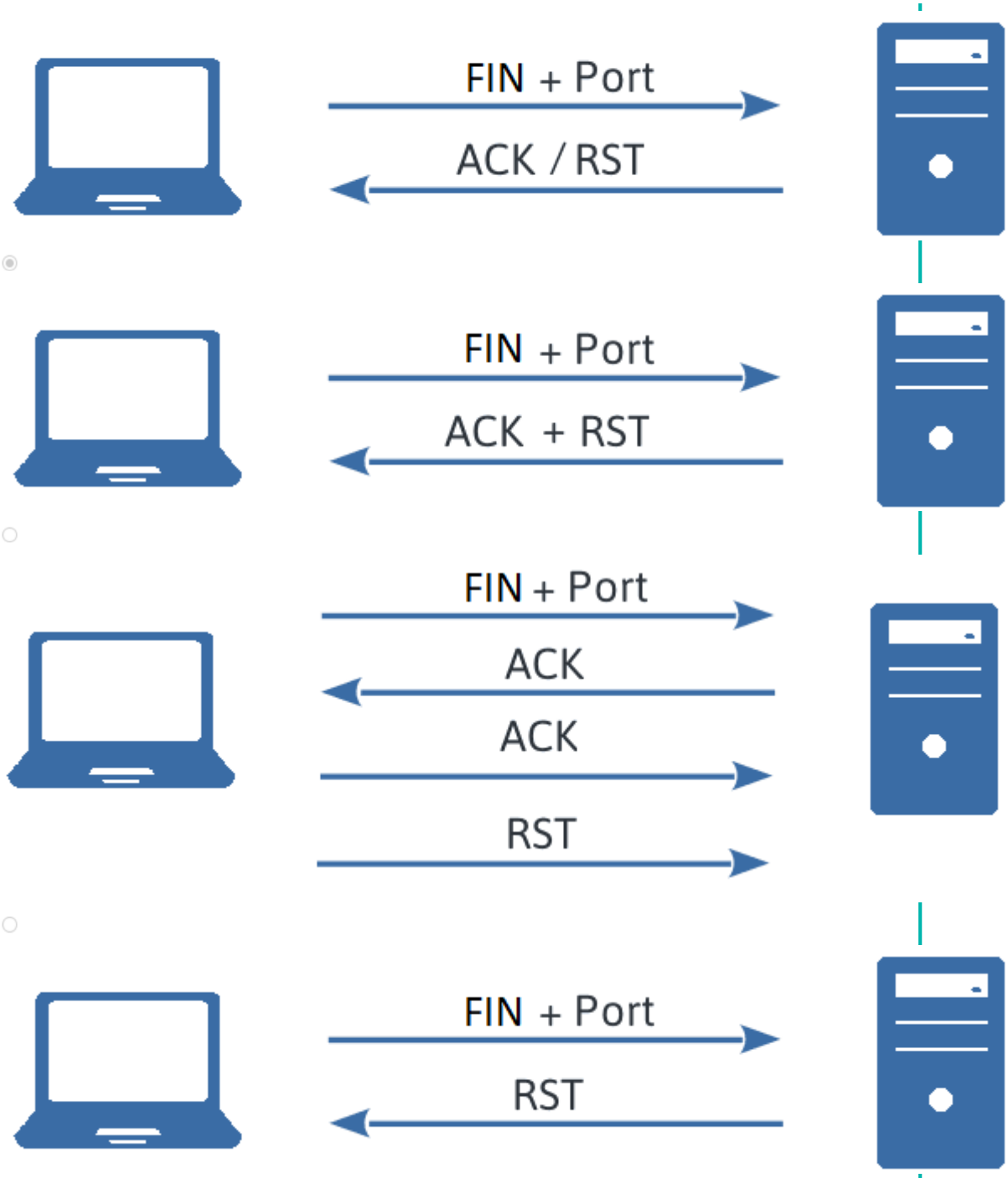
ITS2-1-1-17a

Welches Bild stellt den Kommunikationsablauf eines FIN Scans mit geschlossenen TCP Ports dar?







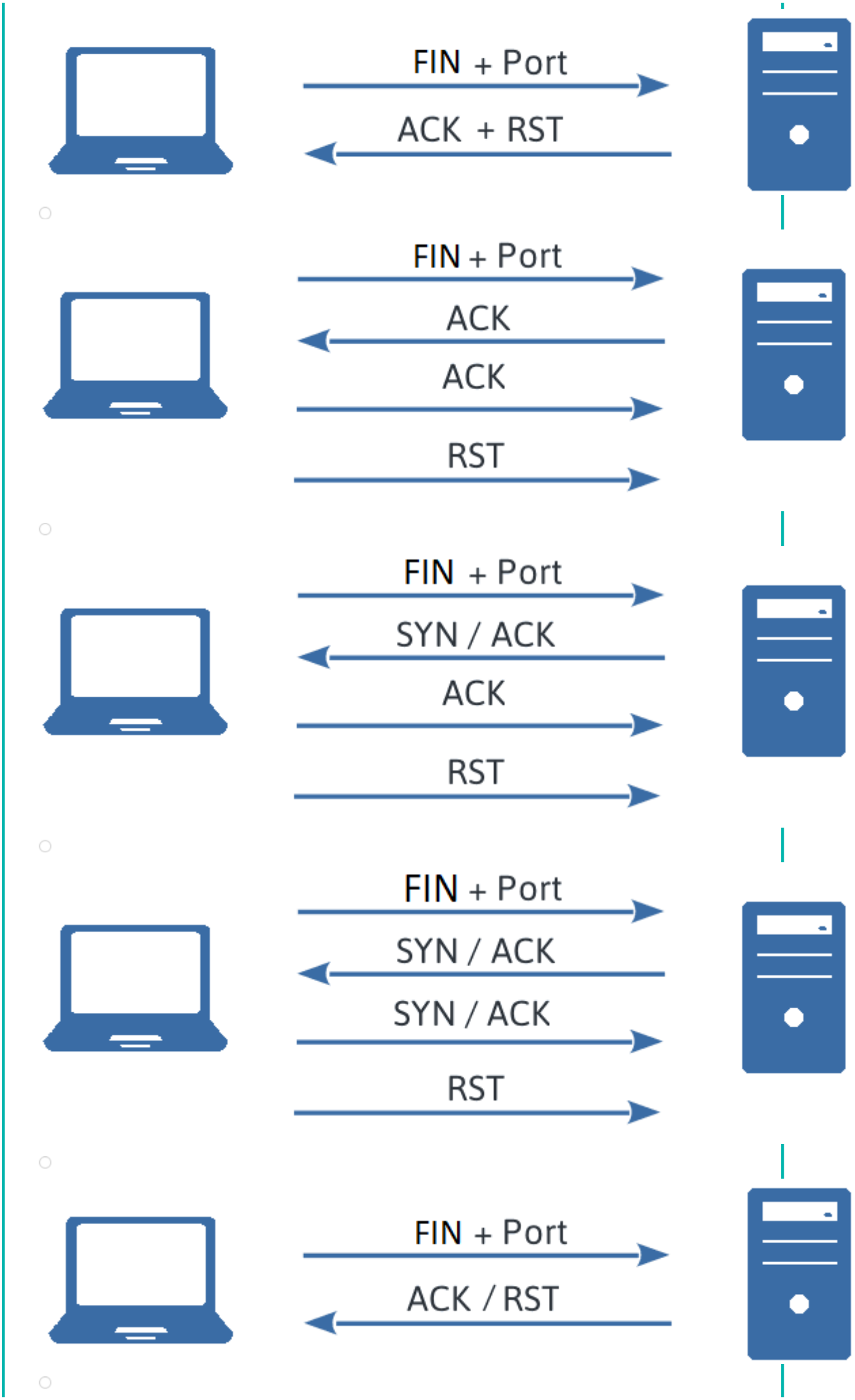


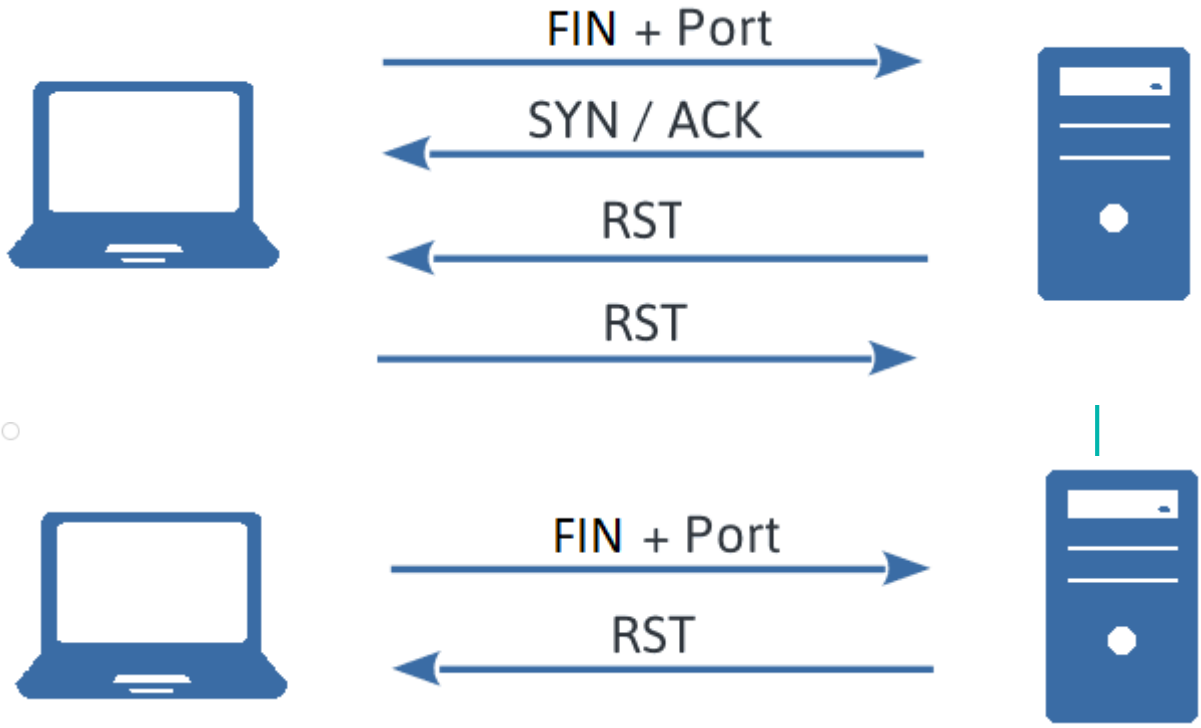
Richtig!

Auswerten

ITS2-1-1-17b

Welches Bild stellt den Kommunikationsablauf eines FIN Scans mit geschlossenen TCP Ports dar?


FIN + Port
ACK + RST
FIN + Port
ACK
ACK
RST
FIN + Port
SYN / ACK
ACK
RST
FIN + Port
SYN / ACK
SYN / ACK
RST
FIN + Port
ACK / RST



Richtig!

Auswerten

ITS2-1-1-18

Finden Sie offene Ports?

Ja, aber nur die Well Known Port.

Nein! Bei Windows werden nie offene Ports mit dem FIN Scangefunden!

Ja, alle offenen Ports wurden gefunden.

Nein, die Window-Firewall filtert die Anfrage.

Nein! Es sind keine Port offen.

Ja, aber nicht alle, weil die Firewall filtert.

Richtig!

Auswerten

ITS2-1-1-19

Was ist der Vorteil eines FIN-Scans?

Bitte wählen Sie maximal 2 von 6 Antworten!

- [ ] Die Nachrichten können nicht von einer Firewall gefiltert werden.
- [ ] Dieser Test kann auch auf der OSI-Schicht 3 ausgeführt werden.
- [x] Es werden nur sehr wenige Nachrichten ausgetauscht (Netzbelastung).
- [ ] Es können TCP und UDP Verbindungen gleichzeitig getestet werden.
- [x] Es werden keine Verbindungen aufgebaut, die normalerweise von Logserver aufgezeichnet werden.
- [ ] Es können auch geschlossene Ports getestet werden.

Richtig!

Auswerten

ITS2-1-1-20

Was ist der Nachteil eines FIN-Scans?

Bitte wählen Sie maximal 2 von 7 Antworten!

- [ ] Der Test ist nicht sehr zuverlässig.
- [x] Benutzer muss Adminrechte haben, um diese, nicht TCP/IP-konformen Pakete zu erzeugen.
- [ ] Es müssen pro Scan 5 (wohl sehr kurze) Nachrichten ausgetausct werden
- [x] Funktioniert nicht mit Microsoft Betriebssystemen.
- [ ] Der Scan funktioniert nicht mit allen LINUX Distributionen.
- [ ] Es können nur geschlossene Ports getestet werden.
- [ ] Der FIN-Scan funktioniert nur mit UDP.

Richtig!

Auswerten

2. Teil: Angriffe mit CAIN – Der ARP-Spoof Angriff

ITS2-1-2-13

Welcher VM gehört diese MAC-Adresse?

Es ist die des Angreifers

Es ist eine unbekannte MAC Adresse

Es ist die des Angegriffenen

Es wird keine MAC-Adresse angezeigt

Richtig!

Auswerten

ITS2-1-2-14

Welchen Weg nehmen Daten vom Server zum Host?

Den direkten Weg

Über den Angreifer

Richtig!

Auswerten

3. Abschlussfragen

Abschlussfrage 1

Woran kann man ein gespooftes Paket beim ARP Spoofing erkennen?

Die MAC-Adresse ist die des Angreifers.

Das Paket ist deutlich länger unterwegs als die anderen Pakete der Verbindung.

Die IP Adresse gehört nicht zur MAC Adresse im Paket.

Die Ziel-IP Adresse liegt nicht im LAN.

Quell- und Ziel-MAC Adresse sind gleich.

Quell- und Ziel IP Adresse haben einen unterschiedlichen Netzteil.

Quell- und Ziel-IP Adresse sind gleich.

Die Quell-IP Adresse liegt nicht im LAN.

Das IP-Spoofing Flag ist gesetzt.

Quell- und Ziel-IP Adresse haben eine unterschiedliche Subnetzmaske.

Richtig!

Auswerten

Abschlussfrage 2 Was ist der **promiscuous** mode?

- In diesem Modus verabeitet eine Netzwerkkarte nur Pakete, deren Ursprung im einen LAN sind.
- In diesem Modus verarbeitet eine Netzwerkkarte keine Pakete.
- In diesem Modus ändert eine Netzwerkkarte die IP Adresse im Paket.
- In diesem Modus arbeitet eine Netzwerkkarte als Proxy.
- In diesem Modus verarbeitet eine Netzwerkkarte alle Daten.
- In diesem Modus verarbeitet eine Netzwerkkarte alle Pakete, die an das Default Gateway gesendet wurden.
- In diesem Modus verarbeitet eine Netzwerkkarte nur gespoofte Pakete.

Richtig!

Auswerten

2 Teil 3 Angriff auf Web-Anwendungen

Fragen

Frage 1a Welche Dateien aus dem aktuellen Verzeichnis werden mit angezeigt?

Bitte wählen Sie maximal 3 von 7 Antworten!

- [x] help
- [ ] view
- [x] source
- [x] index.php
- [ ] index.html
- [ ] robots.txt
- [ ] html.cfg

Richtig!

Auswerten

Frage 1b Welcher Befehl wurde insgesamt auf dem Opfer ausgeführt?

- ping -c 3 [IP-Adresse] && ls
- ping -c 3 [IP-Adresse]; ls
- ping [IP-Adresse] && ls
- ping -c 3 [IP-Adresse] and ls

Richtig!

Auswerten

Frage 2 Unter welchem Benutzer läuft die Webseite?

- root-www
- www-admin
- www-data
- www
- www-root
- admin
- root
- admin-www

Richtig!

Auswerten

Frage 3 In welchem aktuellen Verzeichnis befinden Sie sich?

- /var/www/dvwa/vulnerabilities
-

/var/www/dvwa/exec

/var/www/dvwa/vulnerabilities/exec

/var/www/vulnerabilities/exec

/var/dvwa/vulnerabilities/exec

/www/dvwa/vulnerabilities/exec

Richtig!

Auswerten

Frage 4 Welche Kernelversion wird verwendet?

2.4.24-16

2.6.24-16

2.6.16

2.6.14-16

2.6.24-18

2.16.24

2.6.4-6

Richtig!

Auswerten

Frage 5 Welche **uid** hat der Account?

- 66
- 33
- 90
- 60
- 30
- 99
- 11

Richtig!

Auswerten

Frage 6a Welche **uid** hat der Benutzer *msfadmin*?

- 500
- 333
- 1
- 999
- 123456
- 1000
- 047983

Richtig!

Auswerten

Frage 6b Finden Sie Passwort-Hashes in der Datei?

Ja

Nein

Richtig!

Auswerten

Frage 7 Was wird von der Datei **/etc/shadow** angezeigt?

Nur die ersten 10 Usernamen

Nichts

Nur die Passwort-Hashes, keine Usernamen

NUr Usernamen, keine Passwort-Hashes

Eine Fehlermeldung

Richtig!

Auswerten

Frage 8 Suchen Sie den Speicherort der Datei **nc**.

Welchen Befehl geben Sie dazu nach dem "&&" ein? find / -name nc

Welche Ergebnisse finden Sie? (Reihenfolge wie in der Ausgabe!)

1. Ergebnis /bin/nc

2. Ergebnis /etc/alternatives/nc

3. Ergebnis /var/lib/dpkg/alternatives/nc

Richtig!

Auswerten

Frage 9 Welche Bedeutung haben die Parameter des Befehls **netcat -v -e /bin/bash -l -p 3333**

-v: Es werden mehr Informationen ausgegeben

-e: Netcat wird mit einem bestimmen Programm verbunden

-l: Netcat wird im Listen-Modus gesetzt

-p: Netcat arbeitet auf Port 3333

Richtig!

Auswerten

Frage 10 Wie lautet der gesamte Befehl der vom System ausgeführt wird?

- 127.0.0.1 && netcat -v -e /bin/bash -l -p 3333
- 127.0.0.1 netcat -v -e /bin/bash -l -p 3333
- 127.0.0.1 and netcat -v -e /bin/bash -l -p 3333
- 127.0.0.1 && netcat -v -l -p 3333
- 127.0.0.1 && netcat -v -e /bin/bash -l

Richtig!

Auswerten

Frage 11 Bauen Sie die vom Skript gestellte Abfrage an die Datenbank zusammen.

Anordnung zurücksetzen

7
4
6
8
3
5
2
1
user_id=
FROM
'$id'
last_name

SELECT
WHERE
first_name,
users

Richtig!

Auswerten

Frage 12

Wie viele Benutzer sind in der DB gespeichert? 5

Richtig!

Auswerten

Frage 13 Welches Ergebnis erhalten Sie?

```
ID: 'or 1=1#
First name: admin
Surname: admin

ID: 'or 1=1#
First name: Gordon
Surname: Brown

ID: 'or 1=1#
First name: Hack
Surname: Me

ID: 'or 1=1#
First name: Bob
Surname: Picasso

ID: 'or 1=1#
First name: Pablo
Surname: Smith
```

```
ID: 'or 1=1#
First name: admin
Surname: admin

ID: 'or 1=1#
First name: Gordon
Surname: Brown

ID: 'or 1=1#
First name: Hack
Surname: Smith

ID: 'or 1=1#
First name: Pablo
Surname: Picasso

ID: 'or 1=1#
First name: Bob
Surname: Me
```

```
ID: 'or 1=1#
First name: admin
Surname: Brown

ID: 'or 1=1#
First name: Gordon
Surname: admin

ID: 'or 1=1#
First name: Hack
Surname: Me

ID: 'or 1=1#
First name: Pablo
Surname: Picasso

ID: 'or 1=1#
First name: Bob
Surname: Smith
```

```
ID: 'or 1=1#
First name: admin
Surname: admin

ID: 'or 1=1#
First name: Gordon
Surname: Brown

ID: 'or 1=1#
First name: Hack
Surname: Me

ID: 'or 1=1#
First name: Pablo
Surname: Picasso

ID: 'or 1=1#
First name: Bob
Surname: Smith
```

Richtig!

Auswerten

Frage 14

Wie viele Spalten hat die Tabelle? 2

Geben Sie die ganze Tabelle, einmal nach Spalte 1 und einmal nach Spalte 2 geordnet, mit 2 Befehlen aus.

Welche Befehle verwenden Sie?

1. Befehl: 1' or 1=1 order by 1#

2. Befehl: 1' or 1=1 order by 2#

Richtig!

Auswerten

Frage 15 Welche Daten werden ausgegeben?

Datenbank: Dvwa

Version: 5.0.51a-3ubuntu5

Richtig!

Auswerten

Frage 16

Welche Daten liefert dieser Befehl?

First name: root@%

Surname: root@localhost

Richtig!

Auswerten

Frage 17 Welche Datei wird ausgelesen?

Die Datei **etc**

Die Dateien im Verzeichnis **/etc/passwd**

Die Länge der Datei **passwd**

Die Datei **passwd**

Richtig!

Auswerten

Frage 18a

Welche UserID (Wert in der 3. Spalte) hat der User 'mail'? 8

Richtig!

Auswerten

Frage 18b

Welches (gehashte) Passwort hat der User 'pablo'?

0d107d09f5bbe40cade3de5c71e9e9b7

Richtig!

Auswerten

Frage 19 Was ist richtig für XSS? **Hinweis: Googlen Sie falls Sie die Antworten nicht wissen...**

Bitte wählen Sie maximal 5 von 11 Antworten!

- [x] Es greift nicht direkt die anfällige Webanwendung selbst an.
- [ ] Mit XSS können keine Benutzerkonten kompromittiert werden.
- [ ] Mit XSS können keine Cookies gestohlen werden werden.
- [ ] Es gibt den XSS-Typ StandUp
- [ ] Mit XSS können keine Trojaner aktiviert werden.
- [x] Mit XSS können Cookies gestohlen werden werden.
- [x] Mit XSS können Benutzerkonten kompromittiert werden.
- [ ] Es gibt den XSS-Typ Restricted
- [x] XSS schleust schädlichen Code in eine anfällige Webanwendung ein.
- [x] Mit XSS können Trojaner aktiviert werden.
- [ ] XSS greift die anfällige Webanwendung selbst an.

Richtig!

Auswerten

Frage 20a Was gilt für **Stored XSS**?

Bitte wählen Sie maximal 3 von 6 Antworten!

- [ ] Kann nur für ein Opfer genutzt werden
- [ ] Wird nach dem Angriff gelöscht
- [x] Ist lange wirksam
- [x] Schadcode wird auf dem Server gespeichert
- [x] Ist persistent

☐ Wird reflektiert

Richtig!

Auswerten

Frage 20b Was gilt für **Reflected XSS**?

Bitte wählen Sie maximal 3 von 6 Antworten!

☑ Pro Angriff immer nur ein Opfer
☑ Eingaben werden nicht abgespeichert
☐ Wird auf dem Server gespeichert
☑ Eingaben werden vom Server reflektiert
☐ Ist persistent
☐ Ist lange wirksam

Richtig!

Auswerten

Frage 20c Welchen XSS-Angriff verwenden Sie in welchem Szenario?

Anordnung zurücksetzen

Reflectred XSS
Stored XSS
Angriff über eine Email an das Opfer
Angriff über ein Kommentarfeld auf dem Server

Richtig!

Auswerten

Frage 21 Was sind Ziele eines XSS-Angriffs?

Bitte wählen Sie maximal 3 von 7 Antworten!

☐ Email-Adressen von Webseiten sammeln
☑

Cookies stehlen

Server zum Absturz bringen (DoS)

Preise in der DB eines Webshops manipulieren

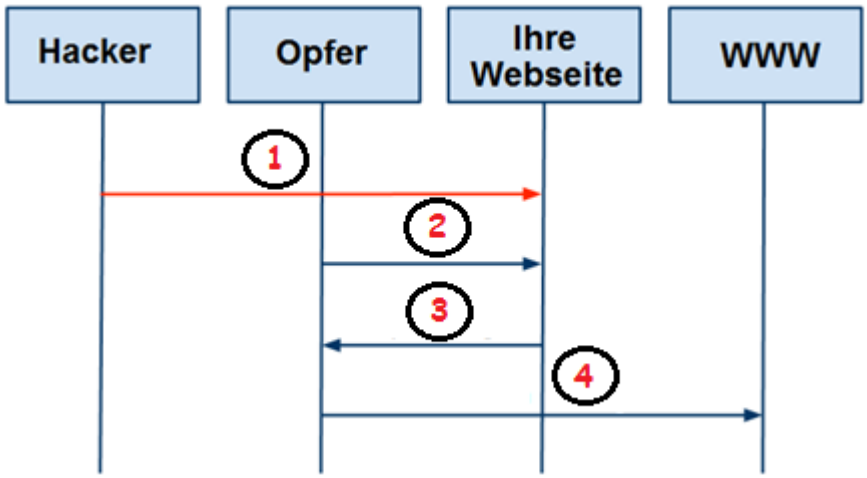
Serverpassworte direkt aus der passwd stehlen

Falsche Werbung machen

Einstellungen im Client-Browser ändern

Richtig!

Auswerten



Frage 22 (siehe Bild oben) Stored XSS: Welche Aktion gehört zu welcher Zahl?

Anordnung zurücksetzen

angreifen
Script einfügen
Mit Script infizieren
besucht
1
2
3
4

Richtig!

Auswerten

Frage 23b Wie kann ein Cookieklau einfach verhindert werden?

- ○ Verwenden von Secure-JavaScript
- ◉ Verwenden des **HttpOnly**-Flags
- ○ Verwenden von Verschlüsselung
- ○ Verwenden eines Secure-Webservers
- ○ Verwenden von **document.cookie**
- ○ Verwenden von PHP anstelle von JavaScript

Richtig!

Auswerten

Frage 24 Kopieren Sie den Inhalt der Datei XSS-Login-1.txt (auf dem Ili-Server) in das Eingabefenster von XSS reflected bei DVWA. **Hinweis: Diese Datei ist die gleiche Datei wie XSS-Login.txt, es wurden nur alle CR entfernt.**

Was geschieht in diesem Fall? Es wird ein neues Loginfenster erzeugt.

Überlegen Sie, was Sie mit diesem Angriff erreichen könnten...

Richtig!

Auswerten

Frage 25a Nach dem Klicken auf Sign Guestbook, was passiert?

Bitte wählen Sie maximal 2 von 6 Antworten!

- [ ] Das Script wird nicht ausgeführt.
- [x] Es wird ein Fenster mit Nachricht angezeigt.
- [ ] Der Webserser stürzt ab.
- [ ] Nichts.
- [x] Das Script wird ausgeführt.
- [ ] Es wird eine Fehlermeldung angezeigt.

Richtig!

Auswerten

Frage 25b Schießen Sie das Fenster und wechseln Sie zur Seite **Brute Force**. Danach wieder auf die Seite **XSS Stored**. Was passiert?

- ( ) Nichts.
- (•) Das Fenster wird erneut angezeigt.
- ( ) Ein Fenster mit anderem Inhalt als vorher wird angezeigt.
- ( ) Der Websever zeigt eine Fehlermeldung an.

Richtig!

Auswerten

Frage 25c Loggen Sie sich auf DVWA aus (Logout) und direkt danach wieder mit **admin/password** ein. Gehen Sie wieder auf die Seite XSS stored. Was passiert?

- ( ) Nichts.
- ( ) Der Browser stürzt ab.
- ( ) Der Webserver zeigt eine Fehlermeldung an.
- ( ) Der Webserver stürzt ab.
- (•) Das Alarmfenster wird erneut angezeigt.

Richtig!

Auswerten

Frage 25d Was müssen Sie tun, um das angezeigte Fenster wieder los zu werden?

- Hostrechner resetten.
- Die Datenbank resetten.
- Browser resetten.
- Webserver resetten.

Richtig!

Auswerten

Frage 26 Ändern Sie die *DVWA Security* auf **medium** und versuchen Sie den gleichen Angriff noch einmal. Was passiert?

Bitte wählen Sie maximal 3 von 6 Antworten!

- [x] Die script-Tags sind gelöscht worden.
- [ ] Die Hochkommata sind ersatzlos gelöscht worden.
- [x] Hochkommata wurden mit einem Backslash "Escaped".
- [x] Das Script wird nicht ausgeführt.
- [ ] Das Verhalten ist wie vorher.
- [ ] Nur die eckigen Klammern sind gelöscht worden.

Richtig!

Auswerten