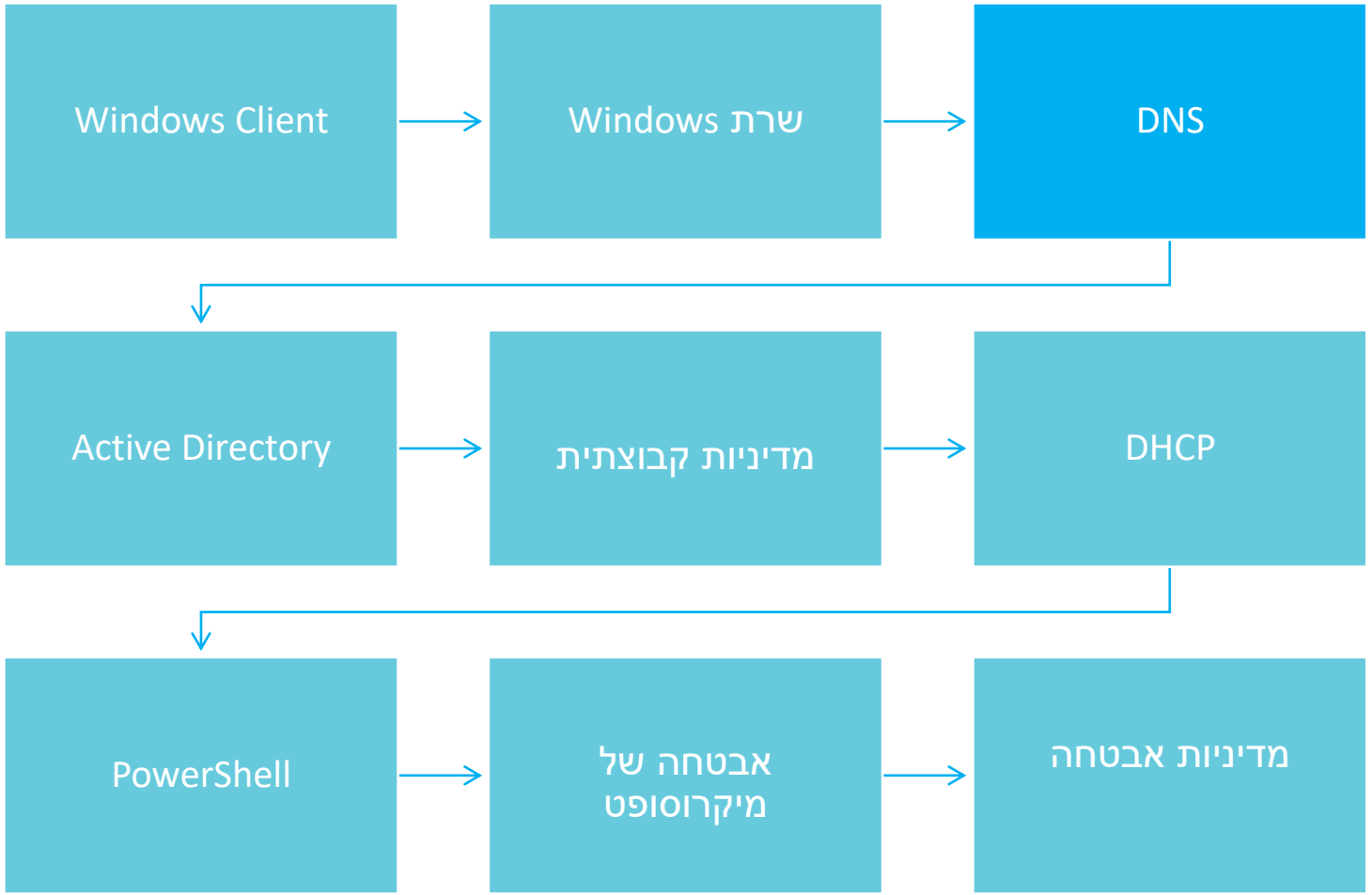
שיעור 3

אבטחת מערכות הפעלה

Domain Name System

CYBER SCHOOL

מסלול הקורס



CYBER SCHOOL

סקירה כללית

למד אודות הבנה של מבנה התחום, רמות הניהול וכלי ה DNS והבנתם.

- יסודות
- אזורי ורשומות DNS
- תצורת DNS
- Link-Local Multicast Name Resolution

CYBER SCHOOL

CYBER SCHOOL

שיעור 3

אבטחת מערכות הפעלה

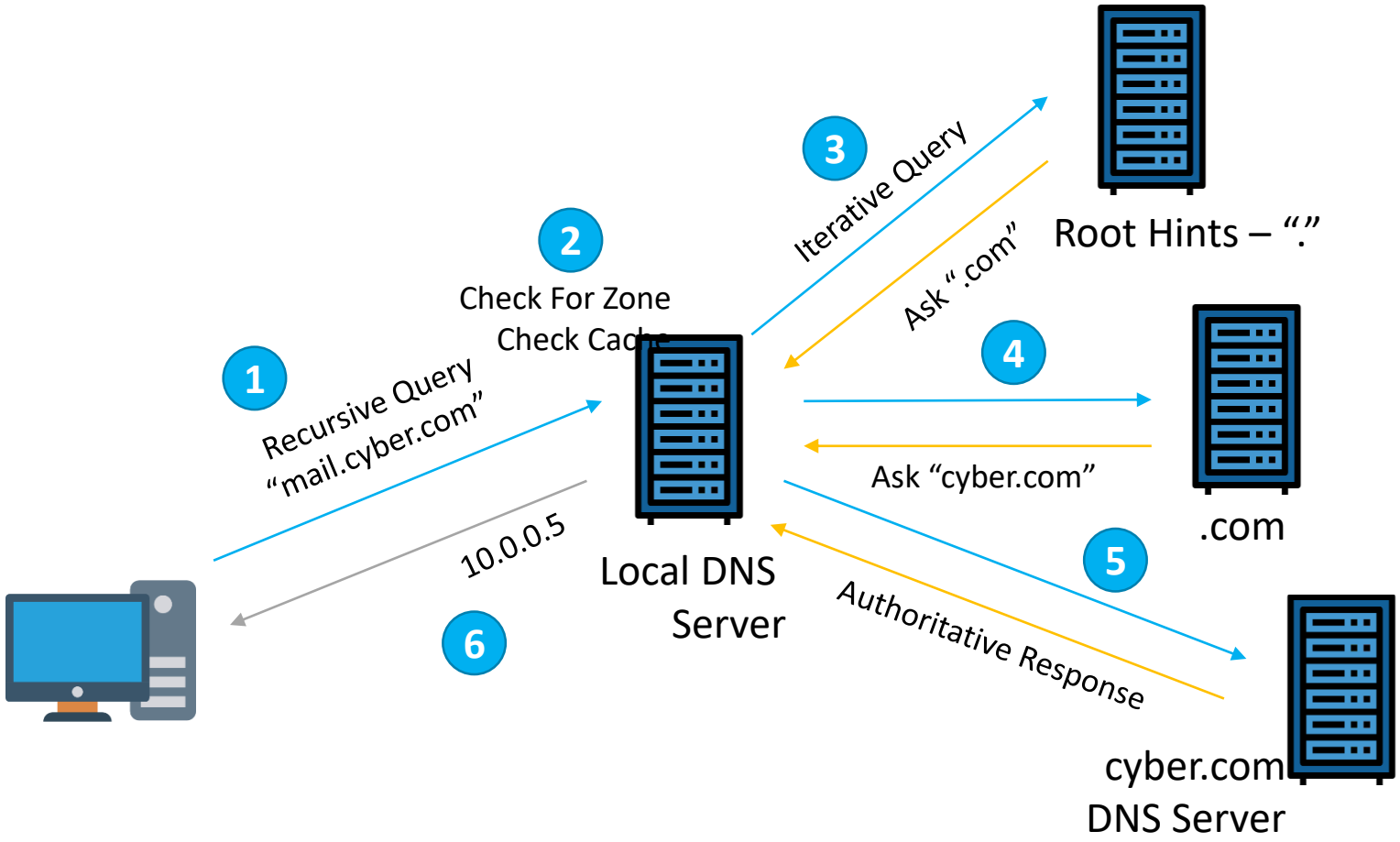
יסודות

הגדרת DNS

DNS נותן שירות המספק מיפוי של שם למספר (כתובת IP).

הוא יוצר טבלת DB לחיפושים.

יש שלושה סוגים של שאילתות: רקורסיבי, לא רקורסיבי, איטרטיבי.



CYBER SCHOOL

DNSSEC

תוסף DNS המספק הגנה מפני התקפות נפוצות, כגון MITM ו - DNS tunneling .

CYBER SCHOOL

CYBER SCHOOL

שיעור 3

אבטחת מערכות הפעלה

אזורי ורשומות DNS

סוגי Record

Host Record
הרשומה הנפוצה ביותר, האחראית לתרגום IP

MX Record
מציין שרת דואר אלקטורני SMTOP עבור ה Domain ,
ניתוב הדואר האלקטורני יוצא אל היעד שלו.

SRV Record
מספק שירותים נוספים לשרת

CYBER SCHOOL

סוגי Record

NS Record

מציין name server סמכותי ומספק את התכובת של הname server

PTR Record

Reverse-lookup pointer

מאפשר מתן כתובת IP ומקבל שם מארח

CNAME Record

מצביע על HOSTNAME ומשמש ככינוי.

CYBER SCHOOL

סוגי Zone

Forward Lookup Zone

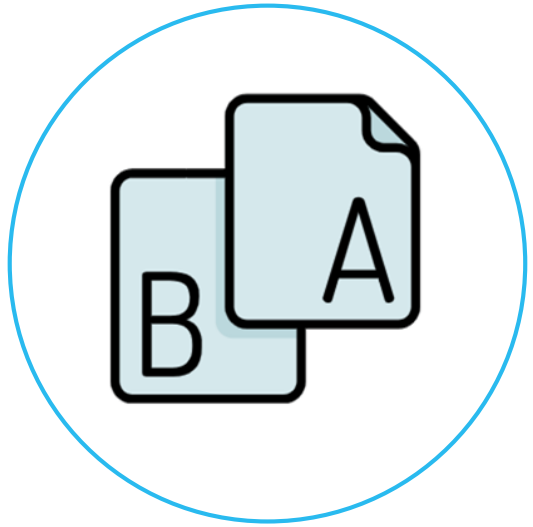
- מיפוי שם לIP.
- ניתן ליצור באופן אוטומטי בעת קידום שרת ל DC.

Reverse Lookup Zone

- מיפוי IP-TO-NAME.
- מכיל רשומות PTR.

CYBER SCHOOL

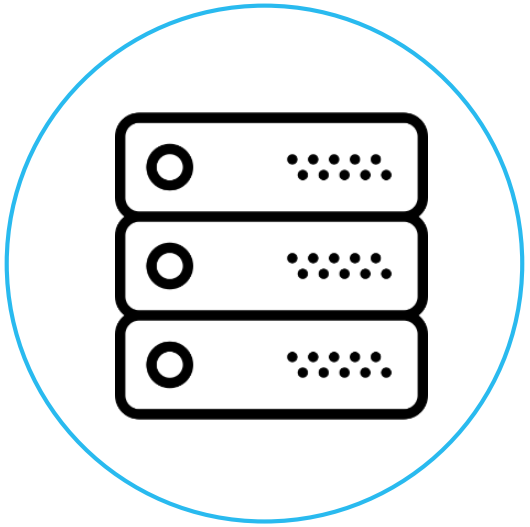
Primary Zone



- יכולות להיות בעלות הרשאות קריאה וכתיבה.
- ניתן להעתיק רשומות Primary Zone לSecondary Zone למטרות גיבוי.
- Secondary Zone מוגדר כאזור לקריאה בלבד.

CYBER SCHOOL

Stub Zone



מכיל רק רשומות הדרושות לזיהוי ה DNS הסמכותי לאזור זה.

כולל :

- SOA, NS, and host records. .
- IP addresses of master servers. .

CYBER SCHOOL

DNS and Active Directory

DNS יכול להשתלב עם Active Directory.

שילוב זה מספק אפשרות לעדכונים דינמיים מאובטחים.

CYBER SCHOOL

CYBER SCHOOL

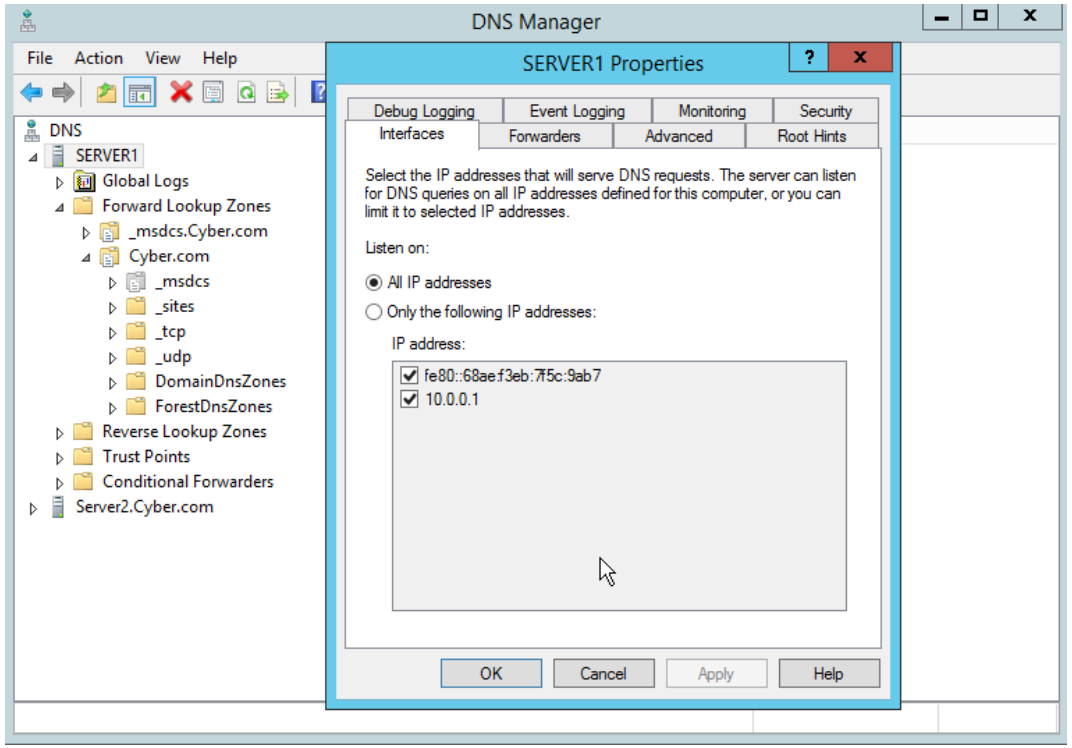
שיעור 3

אבטחת מערכות הפעלה

תצורת DNS

Server Configuration

כרטיסיות מאפייני שרת

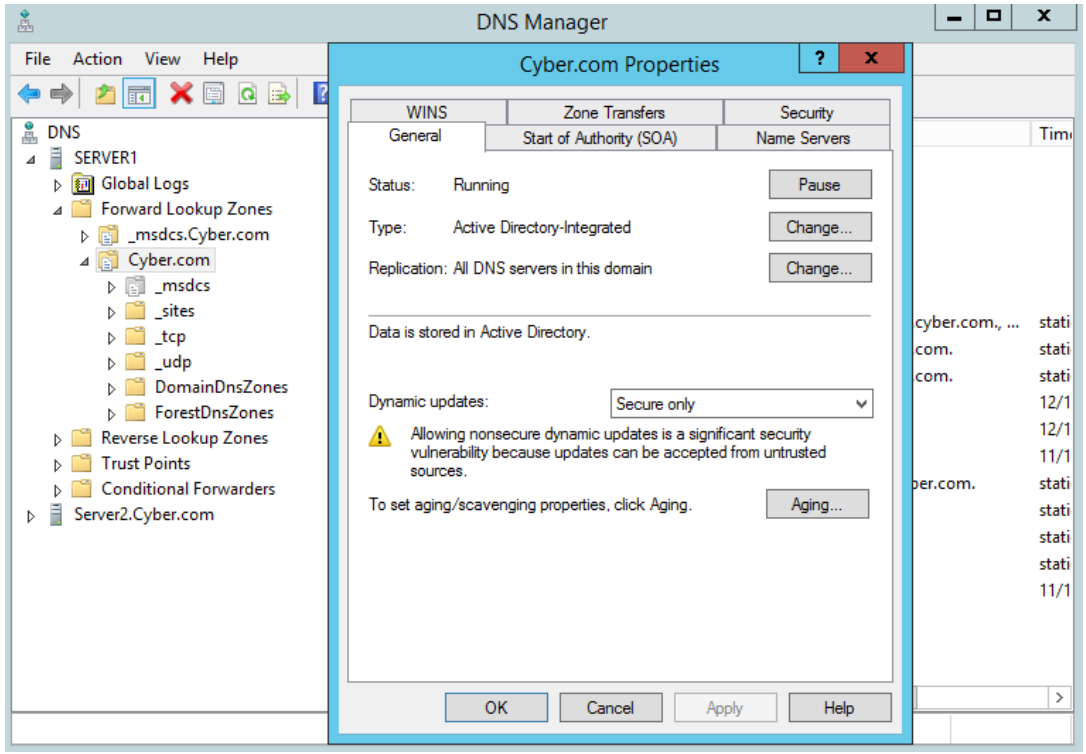


- ממשקים
- משלחים
- Advanced
- Root Hints
- רישום באגים
- רישום אירועים
- מעקב
- אבטחה

CYBER SCHOOL

Zone Configuration

כרטיסיות מאפייני אזור Cyber.com:



- כללי
- SOA
- Name Servers
- WINS
- Zone Transfers
- אבטחה

CYBER SCHOOL

מעבדה 1

Configuring DNS

1-1.5 שעות

המשימה

קבע את התצורה של DNS כשרת DNS ראשי, והוסף רשומות.

השלבים

- צור אזור חדש
- הוסף רשומות שרת .

כלים

Windows Server 2012 R2 GUI

קבצים קשורים

- MS-03-L1 Configuring DNS

CYBER SCHOOL

CYBER SCHOOL

שיעור 3

אבטחת מערכות הפעלה

Link-Local Multicast Name Resolution

LLMNR Protocol

- מבצע רזולוציית שמות עבור Hosts באותה ה LAN
- Multicast on Layer 2, port 5355.
- ניתן לבטל באמצעות GPO

CYBER SCHOOL

המשימה

- לכוד סיסמת לקוח ברשת באמצעות פרטוקול LLMNR (תהליך בדיקת שם דומיין).
- התקפה מוצלחת תסתיים בגילוי הסיסמא הנכונה של הקורבן.

LLMNR Attack

20-40 דק'

CYBER SCHOOL

קורס CSRP

שיעור 3

אבטחת מערכות הפעלה

שאלות?