Syllabes

Module 01 Introduction to Ethical Hacking

Module 02 Footprinting and Reconnaissance

Module 03 Scanning Networks

Module 04 Enumeration

Module 05 System Hacking

Module 06 Malware Threats

Module 07 Sniffing

Module 08 Social Engineering

Module 09 Denial-of-Service

Module 10 Session Hijacking

Module 11 Hacking Webservers

Module 12 Hacking Web Applications

Module 13 SQL Injection

Module 14 Hacking Wireless Networks

Module 15 Hacking Mobile Platforms

Module 16 Evading IDS, Firewalls, and Honeypots

Module 17 Cloud Computing

Module 18 Cryptography

Module 01 Introduction to Ethical Hacking

Hacking: دسترسی غیر مجاز به یک سیستم

انواع Haker:

Black Hat: دسته ای از هکر ها که به صورت غیر قانونی اقدام به تخریب و دزدیدنِ اطلاعات می کنند و از این کار لذت می برند.

White Hat: دسته ای از هکر ها که به صورت قانونی اقدام به تستِ نفوذ بر روی شبکهء سازمان ها می کنند و هدف آنها بالا بردنِ امنیت یک سازمان می باشد و نقطهء مقابلِ Black Hat می باشد.

Gray Hat: دسته ای از هکر ها که هم به صورتِ White Hat و هم به صورتِ Black Hat کار می کنند.

روش های تست:

Black Box Test: این روش زمانی به کار می رود که هکر هیچ اطلاعی از توپولوژیِ شبکه ندارد و با استفاده از reconnaissance اقدام به جمع آوری اطلاعات برای دسترسی به یک Target مشخص می کند.

White Box Test: این روش زمانی به کار می رود که هکر با داشتنِ مجوز های لازم و با داشتنِ اطلاعاتِ لازم در موردِ توپولوژی شبکه اقدام به تستِ نفوذ می کند (مثلا در سطح IT Department).

Gray (Blue) Box Test: زمانی که هکر اطلاعاتِ جزیی (و نه کامل) در رابطه با شبکه داشته و سطحِ دسترسی او به شبکه محدود می باشد (مثلا یک کاربر) (Blue عبارتی است که Microsoft به کار می برد).

Vulnerability (آسیب پذیری): نقاط ضعفی که می تواند در سخت افزار و نرم افزار وجود داشته باشد که یک هکر می تواند از این نقاز ضعف برای دسترسی به سیستم استفاده کند. ولی یک سری از این نقاط ضعف، توسط شرکت های سازنده، آگاهانه بر روی محصولاتشان قرار می گیرد تا بتوانند ساپورت لازم را برای محصولشان فراهم کنند (False Positive).

Exploit/Proof of Concept: Exploit، بهره برداری منفی از نقاط ضعفِ یک سیتم می باشد (مثلا دزدی حساب های بانکی). در حالیکه Proof of Concept، بهره برداری مثبت از نقاط ضعف یک سیستم به منظور بالا بردنِ امنیت آن سیستم می باشد.

ODay: Exploit ی است که برای اولین بار توسط یک هکر انجام شده و در بر دارندهء نقاط ضعفِ سیستم است.

Vulnerability Scan: روش ها و ابزار هایی جهت شناسایی نقاط ضعف سیستم می باشد مثل Nessus.

Penetration Test: روش ها و ابزار هایی که جهتِ تست نفوذ یک شبکه استفاده می شوند. در این رابطه باید Scope ی از تجهیزات شبکه که قرار است تست شوند و همچنینِ زمانِ مورد توافق و قرار داد رسمی، وجود داشته باشد.

Insider Threats

مشخصات Pure Insider:

- **Authorized Physical Access**
- **Network Logon**
- **Elevated Pure Insider (Admin)**

- **Employees + Contractors**
- **Greedy or Disgruntled (طماع یا ناراضی)**

اشخاصی درونِ شبکه می باشند که دارای سطح دسترسی لازم و مجاز به شبکه هستند و بنا به دلایلِ نارضایتی یا طمع اقدام به خرابکاری می کنند.

مشخصات Insider Associate:

- **Limited Authorized Physical Access**
- **No Network Logon**
- **Often Overlooked**
- **Potential Spies**
- **Exposed Papers …**
- **Maintenance guys…**

اشخاصی که درون شبکه می باشند اما از نظر قابلیت نفوذ، نادیده گرفته می شوند.

مشخصات Insider Affiliate:

- Has Connection to Employee (Spouse, GF, BF,…)
- Visitor
- Loaned Badge/PIN
- Borrowed Company Laptop
- Could cause legal trouble
- Can be Social Engineering

اشخاصی که به کارمندان شرکت نزدیکند مثل دوست، همسر،... و بایستی از Share کردنِ اطلاعات و Device های شرکت (مثل Laptop) با آنها خودداری کرد.

Types of Hackers

Black Hat/Cracker/Malicious
White Hat/Ethical Hacker/Pen Tester
Grey Hat
Hacktivism: گروهی از هکر ها که بنا به دلایل سیاسی اعتراض خود را با هک کردن نشان می دهند.

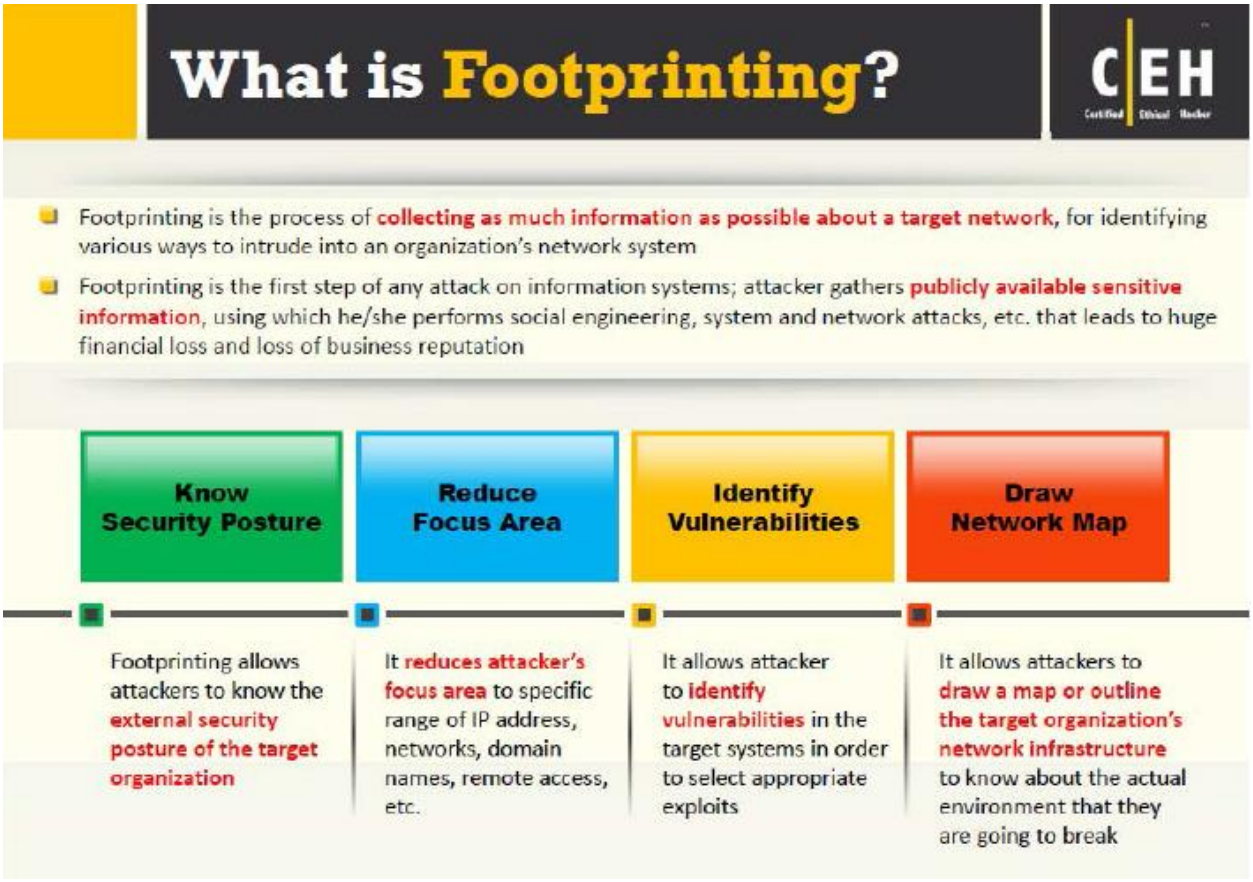
Suicide Hacker: هکر هایی که نسبت به عواقب کارشان (دست گیر شدن، ...) بی تفاوت هستند.

Script Kiddie: هکر های تازه کاری که از نتایج کار و ابزار های آماده استفاده می کنند (غیر خلاق).

Phreak: هکر هایی که دانش خوبی درباره سیست های تلفنی داشته و سعی می کنند که با هک کردن سیستم های تلفنی به صورت رایگان از آن استفاده کنند.

Red Team: تیمی از هکر هاست شامل یک سرپرست و افراد زیر مجموعه هر کدام با مسولیتی خاص؛ مثلا نوشتنِ Malware Code،...این تیم دارای یک قرار داد رسمی است و ملزم به ارایهء **Pen Test Report** به طرف قرار داد می باشد.

Module 02 Footprinting and Reconnaissance

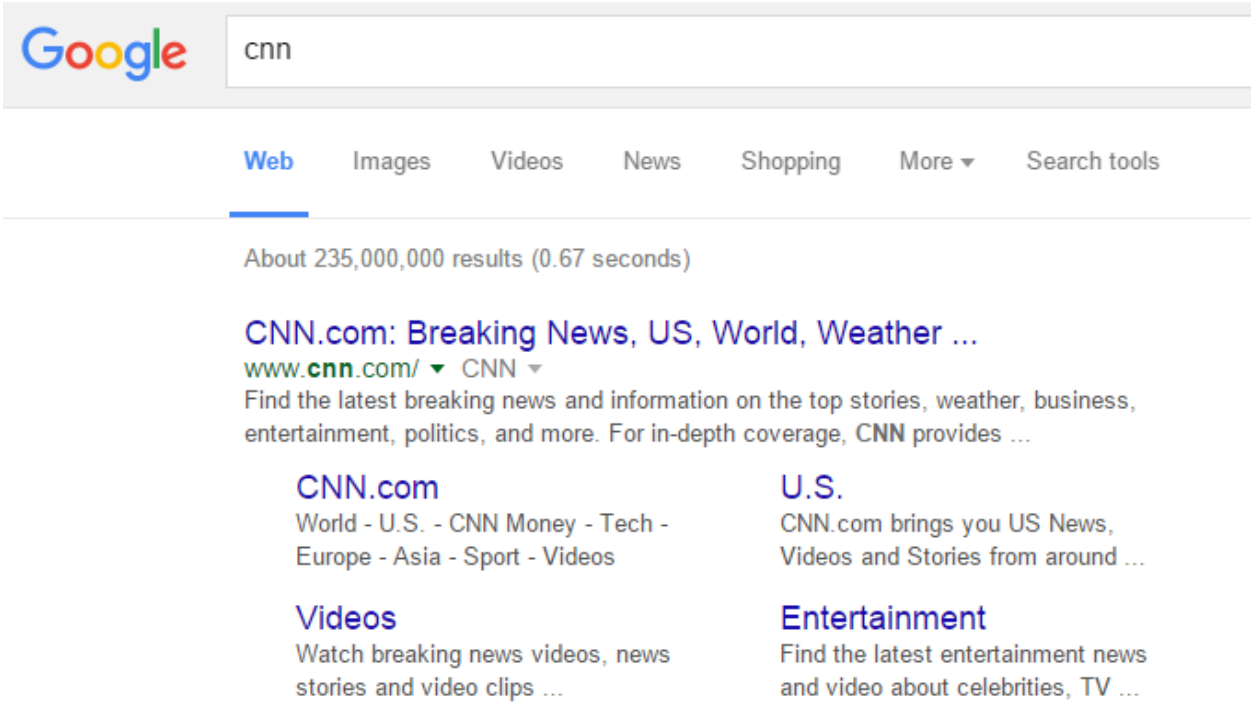


به جمع آوری اطلاعات در مورد سیستم هدف یا قربانی Footprinting گفته می شود که اولین ومهمترین مرحله جهت نفوذ به سیستم قربانی می باشد.

برای پیاده سازی Footprinting بهتر است به ترتیب زیر عمل شود:

- ✓ **شناسایی وب سایت قربانی با استفاده از موتورهای جستجو مانند Google**

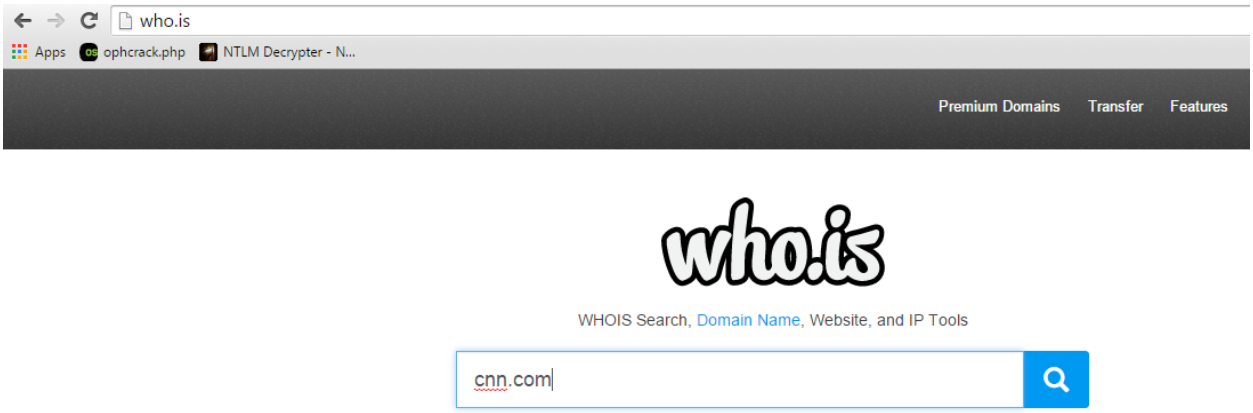
برای مثال ما قصد داریم که اطلاعاتی در مورد وب سایت CNN داشته باشیم برای این منظور به صورت زیر عمل می کنیم:



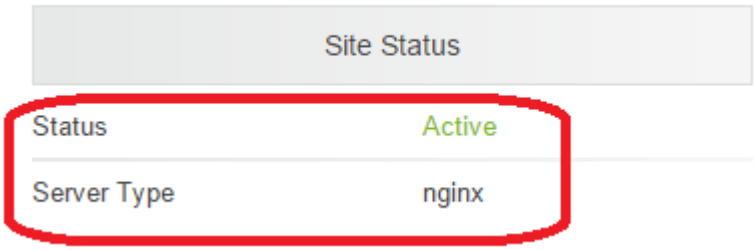
✓ بدست آوردن اطلاعات جزیتر در مورد وب سایت هدف

در این مرحله شما می توانید از وب سایتی به نام who.is.com برای بدست آوردن اطلاعات بیشتری برروی سایت قربانی بدست آورید.

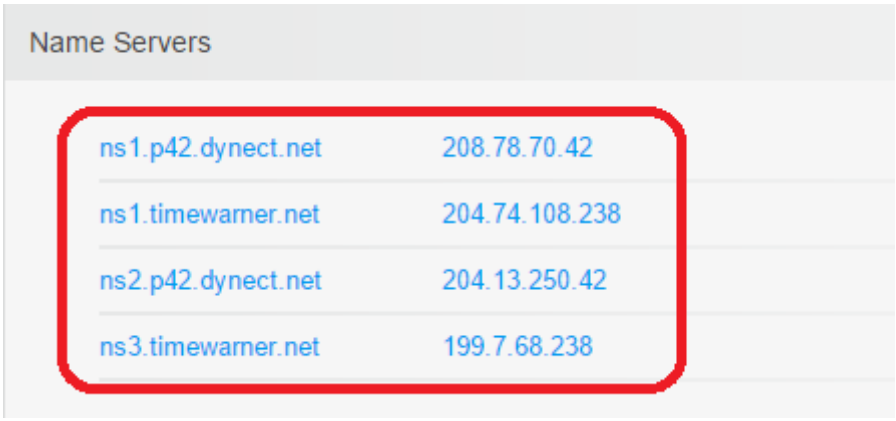
هدف وب سایت CNN



بدست آوردن نوع وب سروری که وب سایتCNN برروی آن راه اندازی شده است:



بدست آوردن نام Name Server هایی که وب سایت CNN بروی آنها ثبت شده است:



- ✓ بدست آوردن اطلاعات در مورد وب سایت با استفاده از NSlookup

Nslookup یک ابزار Command Line می باشد و برای Query از رکوردهای یک DNS می باشد.

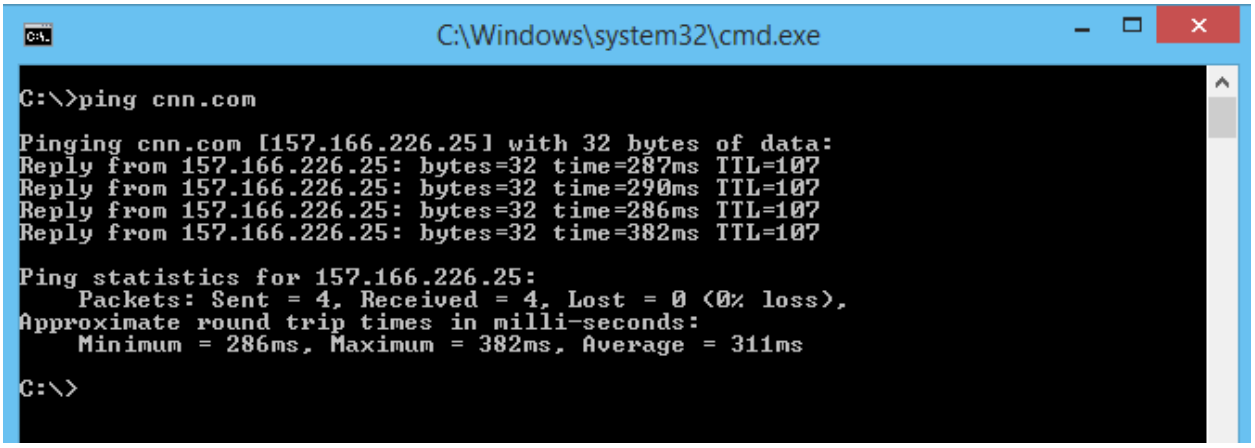
برای مثال قصد داریم تا یکسری اطلاعات را درباره وب سایت CNN با استفاده از nslookup بدست آوریم.

```
C:\>nslookup -type=a cnn.com 8.8.8.8
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    cnn.com
Addresses:  157.166.226.25
          157.166.226.26
```

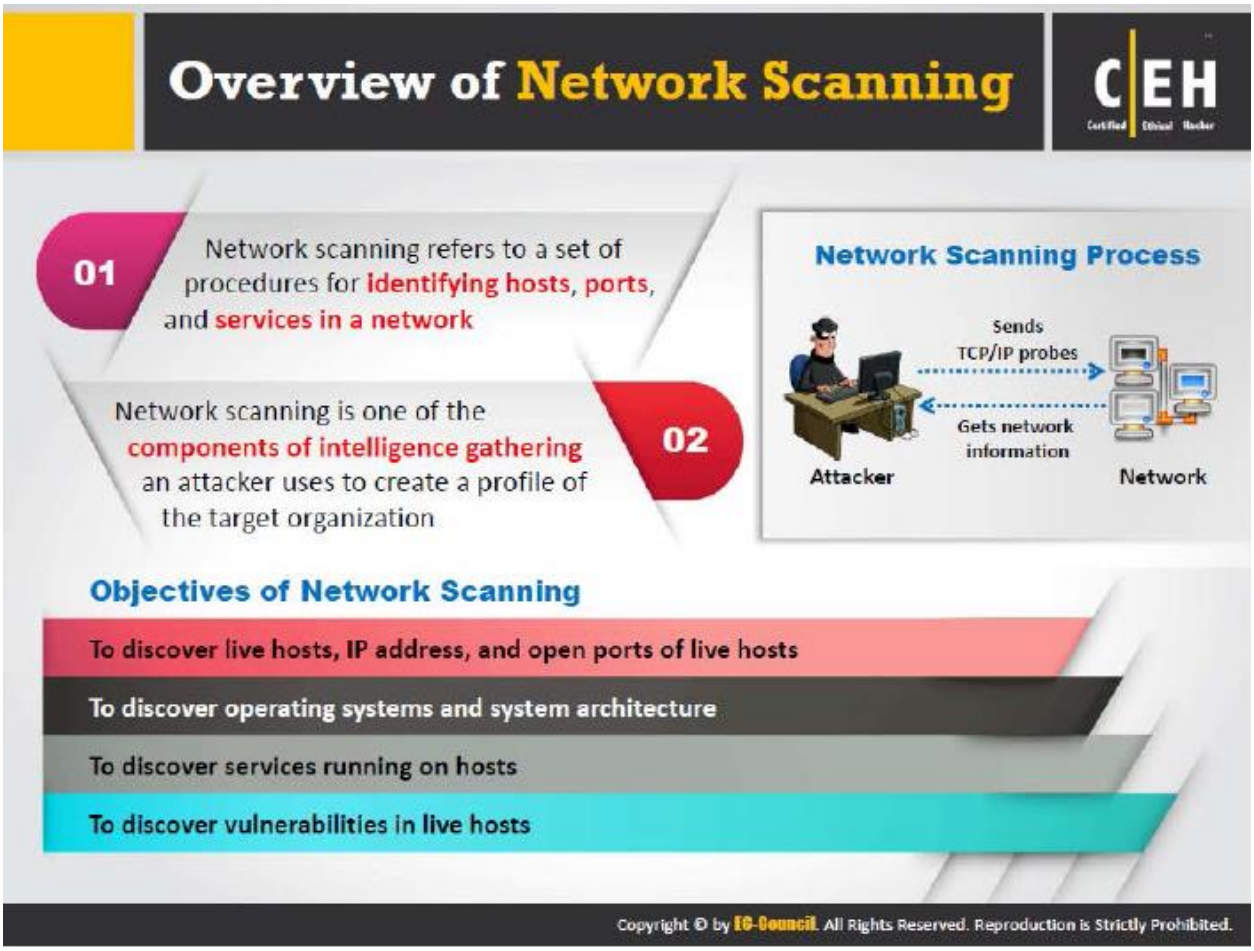
```
C:\>nslookup
Default Server:  Broadcom.Home
Address:  172.16.100.1

> server 4.2.2.1
Default Server:  a.resolvers.level3.net
Address:  4.2.2.1

> type=A
Server:  a.resolvers.level3.net
Address:  4.2.2.1

Non-authoritative answer:
Name:    type=A.Home
Addresses:  198.105.254.11
          198.105.244.11

> ccn.com
Server:  a.resolvers.level3.net
Address:  4.2.2.1

Non-authoritative answer:
Name:    ccn.com
Address:  69.172.201.208

> type=MX
Server:  a.resolvers.level3.net
Address:  4.2.2.1

Non-authoritative answer:
Name:    type=MX.Home
Addresses:  198.105.254.11
          198.105.244.11

> ccn.com
Server:  a.resolvers.level3.net
Address:  4.2.2.1

Non-authoritative answer:
Name:    ccn.com
Address:  69.172.201.208
```

✓ بدست آوردن اطلاعات با استفاده از Ping

سایت هدف cnn.com



Module 03 Scanning Networks



عملیات Scanning به فرآیند بررسی سیستم هدف و یا شبکه هدف گفته میشود. که هدف از این کار بدست آوردن اطلاعات اساسی در مورد نوع سیستم عامل و ورژن آنها و سرویس پک و پورتهای باز آنها و سرویس های که بر روی آنها در حال اجرا می باشد.

در ویندوز شما می توانید از مسیر زیر پورتهای مهم را شناسایی کنید.

%System root%\system32\drivers\etc

در مسیر بالا کافیست فایل Services را باز کنید تا پورتها و سرویسهای مرتبط با آنها را مشاهده کنید.

فرآیند Scanning شامل مراحل زیر می باشد:

- ✓ **مرحله Check For Live System**

(شناسایی سیستم های فعال در شبکه می باشد)

- ✓ **Check For Open Port**

(شناسایی پورت باز بر روی سیستم های فعال می باشد)

- ✓ **مرحله Service Identificate**

(شناسایی سرویس هایی که بر روی پورتهای باز قرار دارند)

- ✓ **مرحله Banner Grabbing /OS Finger Printing**

(شناسایی نوع سیستم عامل بر روی سیستم های فعال می باشد)

- ✓ **مرحله Vulnerability Scanning**

(شناسایی نقاط ضعف و آسیب پذیرها بر روی سیستم های فعال می باشد)

- ✓ **مرحله Vulnerability Host Draw Network Diagram of**

(ترسیم نقشه شبکه از Host های آسیب پذیر می باشد)

- ✓ **مرحله Prepare Proxy**

(در این مرحله هکر از یک proxy برای پنهان کردن آدرس IP خود استفاده می کند)

دو نوع Scanning از لحاظ عملیاتی وجود دارد:

- ✓ عملیات Scanning در شبکه داخلی
- ✓ عملیات Scanning در شبکه اینترنت

در عملیات Scanning در شبکه های داخلی قدم اول شناسایی سیستم های فعال می باشد.

ابزارهایی های معروفی که می توانند برای اسکن شبکه استفاده شوند به صورت زیر دسته بندی می شوند:

- ✓ NMAP
- ✓ Angry IP Scanner
- ✓ Hping V3
- ✓ Solarwinds Toolset

عملیات Scanning در شبکه اینترنت

یکی از روشهایی که برای عملیات Scanning در شبکه های اینترنت استفاده می شود Ping Sweep می باشد که در این روش یک رنجی از آدرس های IP در شبکه Ping می شود و در صورت reply یا پاسخ سیستم های فعال در شبکه شناسایی می شود.

ولی این روش جزو روشهای قدیمی می باشد که توسط فایروال های نرم افزاری و سخت افزاری شناسایی می شود.

بهترین ابزار برای Port Scan ابزاری است به نام NMAP که در لینوکس های BT و Kali موجود می باشدو کاملا رایگان می باشد.

برای دانلود آخرین نسخه NMAP می توانید از سایت زیر استفاده کنید.

WWW.insecure.org/nmap

نرم افزار NMAP قابلیت نصب بر روی سیستم عامل لینوکس و ویندوز را دارد.

ولی بهترین نتیجه را NMAP مربوط به لینوکس به ما می دهد.

دستور NMAP چندین نوع SCAN را به صورت زیر پشتیبانی می کند:

TCP Connect

(در این نوع Scan یک هکر یک ارتباط کامل TCP را با سیستم مقصد برقرار می کند ولی این نوع اسکن به راحتی شناسایی می شود)

Xmas Tree Scan

(در این نوع اسکن یک هکر سرویس های TCP را با استفاده از ارسال Packet های Xmas چک می کند. یک Packet Xmas شامل PSH و URG و Fin Flag می باشد که در این اسکن مقادیر تمامی این Flag ها یک ست می شود در صورتی پاسخ برگشتی شامل RST باشد به این معنی که پورت بسته می باشددر غیر این صورت پورت باز می باشد این نوع اسکن فقط برروی سیستم عامل های لینوکس و یونیکس قابل پیاده سازی است.)

Syn Stealth Scan

(که در اصطلاح به آن Half-Open Scan هم گفته میشود به عبارت دیگر اسکن نیمه باز می باشد. در این نوع اسکن، هکر یک درخواست Syn به سیستم هدف ارسال می

کند و سیستم هدف در پاسخ syn-Ack را به ما باز میگرداند ولی هکر در پاسخ تائید به سیستم هدف نمی دهد.

دقت کنید در صورتی که سیستم هدف با Syn-Ack پاسخ دهد به این معناست که پورت مورد نظر باز می باشد ولی در صورتی که پاسخ به صورت RST/ACK باشد به این معناست که پورت موردنظر بسته می باشد.)

NULL Scan

این نوع اسکن از اسکن های حرفه ای می باشد به دلیل اینکه اکثر Flag های آن OFF هستند امکان عبور آنها از فایروال وجود دارد و بر روی لینوکس قابل پیاده سازی است.)

Windows Scan

این نوع اسکن شبیه به ACK- Scan می باشد و پورتهای باز را شناسایی می کند.

ACK-Scan این نوع اسکن برای عبور از یک فایروال استفاده می شود و بر روی سیستم های لینوکس قابل پیاده سازی است.

سوئیچ هایی که در دستور nmap استفاده می شود به صورت زیر دسته بندی می شوند:

-sT Tcp connect Scan

- sS Syn Scan

- sF FIN Scan

- sX Xmas Tree Scan

- sN Null Scan

-sP Ping Scan

-sU UDP Scan

-sO Protocol Scan

-sA Ack Scan

-sW Windows Scan

-sR RPC Scan

-sL List / DNS Scan

-sI Idle Scan

-Po Don’t Ping

-PT TCP Ping

-PS Syn Ping

-PI ICMP Ping

-PB TCP and ICMP Ping

-PM ICMP Mask

-oN Normal output

برای بررسی پورتهای باز یک سیستم خاص از دستور زیر استفاده می کنیم :

```
root@kali:~# nmap 172.16.100.2

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-23 12:56 EDT
Nmap scan report for Fariborz.Home (172.16.100.2)
Host is up (0.00023s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 24:FD:52:39:28:C7 (Liteon Technology)
```

برای بررسی پورتهای باز چندین سیستم از دستور زیر استفاده می کنیم :

```
root@kali:~# nmap 172.16.100.2 172.16.100.9 172.16.100.10
```

برای بررسی پورتهای باز بر روی رنجی از آدرسهای شبکه از دستور زیر استفاده می کنیم :

```
root@kali:~# nmap 172.16.100.0/24
```

در صورتی که بخواهیم تعداد زیادی از سیستم ها را اسکن کنیم می توانیم آدرس آنها را در یک Text file ایجاد کرده و به صورت زیر در nmapاستفاده کنیم :

```
root@kali:~# touch list
root@kali:~# echo 172.16.100.2 > list
root@kali:~# echo 172.16.100.9 >> list
root@kali:~# echo 172.16.100.10 >> list
root@kali:~# cat list
172.16.100.2
172.16.100.9
172.16.100.10
root@kali:~# nmap -iL list
```

برای Exclude کردن یکسری از سیستم ها از اسکن با استفاده از دستور زیر استفاده می کنیم :

```
root@kali:~# nmap 172.16.100.0/24 --exclude 172.16.100.2
```

در صورتی که از دستور nmap برای ping یک Target استفاده می شود و در پاسخ با پیغام host seen down مواجه شوید به این معناست که یا سیستم هدف فعال نمی باشد و یا پشت فایروال قرار دارد و ping به آن سیستم بسته می باشد.

در حالت بالا بایستی از سوئیچ PN– استفاده شود به عبارت دیگر سیستم هدف یا target دیگر Ping نمی شود فقط عملیات پورت اسکن بر روی آن انجام می شود.

```
root@kali:~# nmap -PN 172.16.100.2
```

برای اسکن سیستم هدف یا Targetبا استفاده از ARP از دستور زیر استفاده می کنیم .

```
root@kali:~# nmap -PR 172.16.100.2
```

در شبکه های Lan معمولا پروتکل ARP باز می باشد و استفاده از دستور بالا مفید می باشد.

NMAP Banner Grabing

با استفاده از دستور زیر می توانید عملیات Banner Grabing را انجام دهید به عبارت دیگر می توانید بفهمید که پشت پورتی که باز است چه سرویسی و چه ورژنی از سرویس باز می باشد:

```
root@kali:~# nmap -sV 172.16.100.2

Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-25 02:02 EDT
Nmap scan report for Fariborz.Home (172.16.100.2)
Host is up (0.00045s latency).
Not shown: 989 filtered ports
PORT      STATE SERVICE         VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn
443/tcp   open  ssl/http        VMware VirtualCenter Web service
445/tcp   open  netbios-ssn
554/tcp   open  rtsp?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOA
P)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP
)
2869/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49155/tcp open  msrpc           Microsoft Windows RPC
MAC Address: 24:FD:52:39:28:C7 (Liteon Technology)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Telnet Banner Grabbing

با استفاده از دستور Telnet هم می توانید عملیات Banner Grabbing را انجام دهید:

```
C:\>telnet mail.kali.org 25

220 apollo.kali.org ESMTP Postfix
```