

# گزارش کار آزمایش 10- آزمایشگاه امنیت شبکه

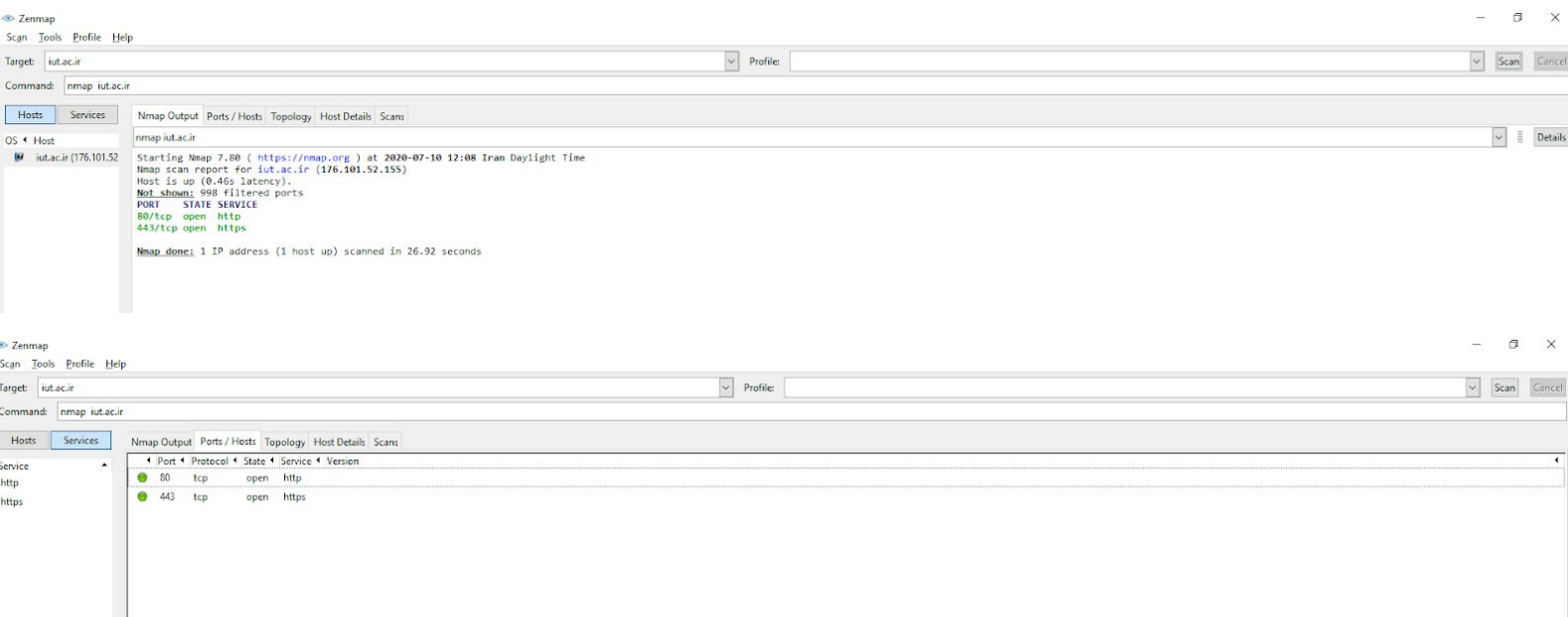
## محیا جمشیدیان

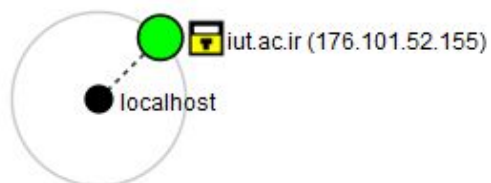
### 9525133

#### 1 - الف - nmap [domain name\IP]

هدف از استفاده از این دستور بررسی پورتهای باز یک سیستم با یک نام دامنه و یا IP مشخص است. دستور زیر که برای هر دو سایت مذکور اعمال شده است، نتایج ساده ای مانند پورتهای باز یا پشتیبانی از ipv6 را نشان میدهد.

-----iut-----  
-----





☐ iut.ac.ir (176.101.52.155)

☐ **Host Status**

State: up

Open ports: 2



Filtered ports: 998

Closed ports: 0

Scanned ports: 1000

Up time: Not available

Last boot: Not available

☐ **Addresses**

IPv4: 176.101.52.155  
IPv6: Not available  
MAC: Not available

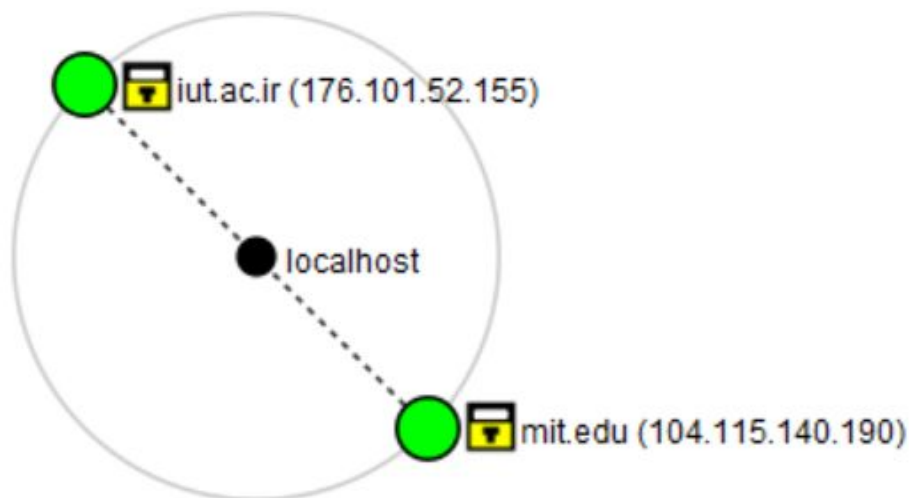
☐ **Hostnames**

Name - Type: iut.ac.ir - user

☐ **Comments**

-----mit-----  
-----

Hosts		Services													
Service		Nmap Output	Ports / Hosts	Topology	Host Details	Scans									
http		nmap mit.edu													
https		<p>Starting Nmap 7.80 ( <a href="https://nmap.org">https://nmap.org</a> ) at 2020-07-10 12:11 Iran Daylight Time</p> <p>Nmap scan report for <a href="https://mit.edu">mit.edu</a> (104.115.140.190)</p> <p>Host is up (0.33s latency).</p> <p>rDNS record for 104.115.140.190: <a href="https://a104-115-140-190.deploy.static.akamaitechnologies.com">a104-115-140-190.deploy.static.akamaitechnologies.com</a></p> <p><u>Not shown:</u> 998 filtered ports</p> <table><thead><tr><th>PORT</th><th>STATE</th><th>SERVICE</th></tr></thead><tbody><tr><td>80/tcp</td><td>open</td><td>http</td></tr><tr><td>443/tcp</td><td>open</td><td>https</td></tr></tbody></table> <p><u>Nmap done:</u> 1 IP address (1 host up) scanned in 21.35 seconds</p>					PORT	STATE	SERVICE	80/tcp	open	http	443/tcp	open	https
PORT	STATE	SERVICE													
80/tcp	open	http													
443/tcp	open	https													



نتیجه این دستور ساده برای دو سایت فوق، این است که هر دو پورت وب سرویسهای 80 و 443 باز هستند و با تفاوت این که mit.edu از ipv6 هم پشتیبانی میکند که این دستور در یک اطلاعیه آدرس IP آنها را نشان میدهد.

ب - nmap -v [domain name\IP]

این دستور جزئیات بیشتری را در اختیار کاربر قرار میدهد، که اطلاعات مربوط به زمان اسکن کردن است.

-----iut-----

Zenmap

Scan Tools Profile Help

Target: iut.ac.ir Profile:

Command: nmap -v iut.ac.ir

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

- mit.edu (104.115.14)
- iut.ac.ir (176.101.52)

nmap -v iut.ac.ir

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-07-10 12:13 Iran Daylight Time  
Initiating Ping Scan at 12:13  
Scanning iut.ac.ir (176.101.52.155) [4 ports]  
Completed Ping Scan at 12:13, 1.22s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 12:13  
Completed Parallel DNS resolution of 1 host. at 12:13, 0.49s elapsed  
Initiating SYN Stealth Scan at 12:13  
Scanning iut.ac.ir (176.101.52.155) [1000 ports]  
Discovered open port 443/tcp on 176.101.52.155  
Discovered open port 80/tcp on 176.101.52.155  
Completed SYN Stealth Scan at 12:13, 23.38s elapsed (1000 total ports)  
Nmap scan report for iut.ac.ir (176.101.52.155)  
Host is up (0.48s latency).  
Not shown: 998 filtered ports

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

Read data files from: C:\Program Files (x86)\Nmap  
Nmap done: 1 IP address (1 host up) scanned in 26.28 seconds  
Raw packets sent: 2014 (88.592KB) | Rcvd: 58 (2.552KB)

-----mit-----

Zenmap

Scan Tools Profile Help

Target: mit.edu Profile:

Command: nmap -v mit.edu

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

- mit.edu (104.102.90)
- mit.edu (104.115.14)
- iut.ac.ir (176.101.52)

nmap -v mit.edu

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-07-10 12:14 Iran Daylight Time  
Initiating Ping Scan at 12:14  
Scanning mit.edu (104.102.90.162) [4 ports]  
Completed Ping Scan at 12:14, 1.01s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 12:14  
Completed Parallel DNS resolution of 1 host. at 12:14, 0.31s elapsed  
Initiating SYN Stealth Scan at 12:14  
Scanning mit.edu (104.102.90.162) [1000 ports]  
Discovered open port 80/tcp on 104.102.90.162  
Discovered open port 443/tcp on 104.102.90.162  
Completed SYN Stealth Scan at 12:14, 18.12s elapsed (1000 total ports)  
Nmap scan report for mit.edu (104.102.90.162)  
Host is up (0.28s latency).  
rDNS record for 104.102.90.162: a104-102-90-162.deploy.static.akamaitechnologies.com  
Not shown: 998 filtered ports

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

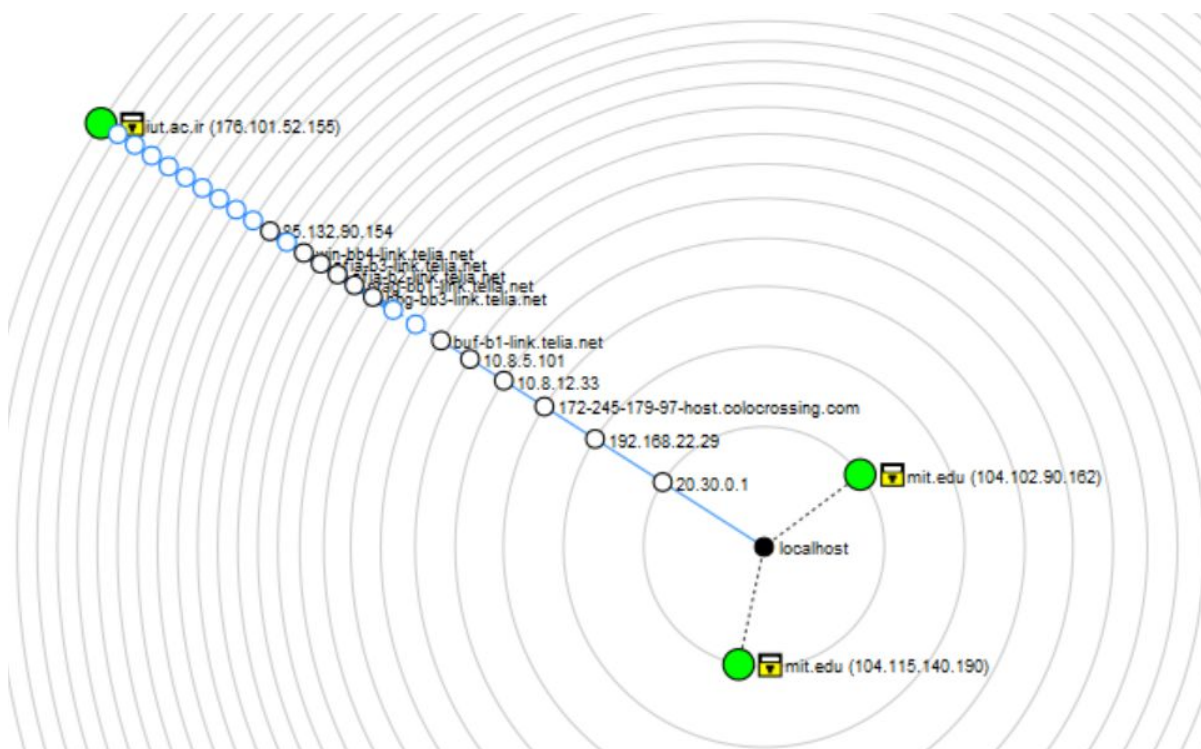
Read data files from: C:\Program Files (x86)\Nmap  
Nmap done: 1 IP address (1 host up) scanned in 20.43 seconds  
Raw packets sent: 2010 (88.416KB) | Rcvd: 38 (1.656KB)

تفاوت معناداری در نتایج بین دو دستور دیده نمیشود.

پ - nmap -A [domain name \ IP]

-----iut-----

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -A iut.ac.ir				
Starting Nmap 7.80 ( <a href="https://nmap.org">https://nmap.org</a> ) at 2020-07-10 12:15 Iran Daylight Time				
Nmap scan report for iut.ac.ir (176.101.52.155)				
Host is up (0.47s latency).				
Not shown: 998 filtered ports				
PORT	STATE	SERVICE	VERSION	
80/tcp	open	http	nginx (reverse proxy)	
_ http-server-header:				
_ ASPA-WAF				
_ nginx/1.18.0				
_ http-title: Did not follow redirect to <a href="https://iut.ac.ir/">https://iut.ac.ir/</a>				
443/tcp	open	ssl/http	nginx (reverse proxy)	
_ http-server-header: ASPA-WAF				
_ http-title: 400 The plain HTTP request was sent to HTTPS port				
_ ssl-cert: Subject: commonName=*.iut.ac.ir/countryName=IR				
_ Subject Alternative Name: DNS:*.iut.ac.ir, DNS:iut.ac.ir				
_ Not valid before: 2020-03-01T04:29:53				
_ Not valid after: 2022-03-01T04:29:53				
_ ssl-date: TLS randomness does not represent time				
_ tls-alpn:				
_ h2				
_ http/1.1				
_ tls-nextprotoneg:				
_ h2				
_ http/1.1				
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port				
Device type: general purpose				
Running (JUST GUESSING): Linux 2.6.X (86%)				
OS CPE: cpe:/o:linux:linux_kernel:2.6				
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (86%)				
No exact OS matches for host (test conditions non-ideal).				
Network Distance: 25 hops				



-----mit-----

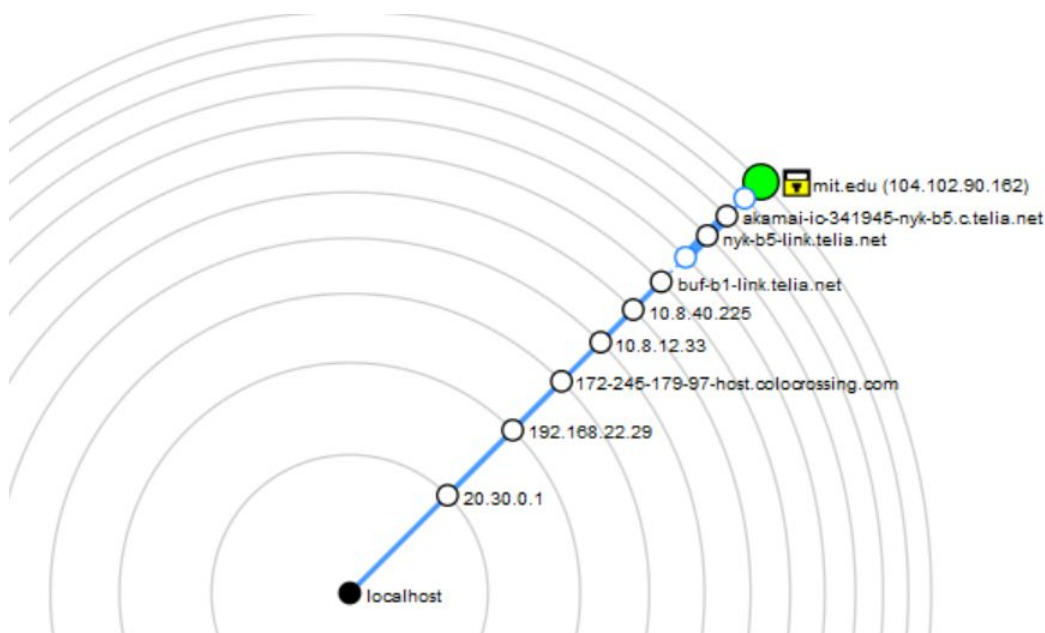


```

Nmap Output  Ports / Hosts  Topology  Host Details  Scans
nmap -A mit.edu

Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-10 12:36 Iran Daylight Time
Nmap scan report for mit.edu (104.102.90.162)
Host is up (0.19s latency).
rDNS record for 104.102.90.162: a104-102-90-162.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_ http-title: Did not follow redirect to http://web.mit.edu/
443/tcp    open  ssl/http  AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_ http-title: Did not follow redirect to https://web.mit.edu/
|_ ssl-cert: Subject: commonName=web.mit.edu/organizationName=Massachusetts Institute of Technology/stateOrProvinceName=Massachusetts/countryName=US
|_ Subject Alternative Name: DNS:web.mit.edu, DNS:mit.mit.edu, DNS:giving.mit.edu, DNS:news.mit.edu, DNS:emergency-dev.mit.edu, DNS:www.mit.edu, DNS:events-static.mit.edu, DNS:emergency.mit.edu, DNS:www-mit.mit.edu, DNS:www.mit.edu, DNS:img.mit.edu, DNS:www-cert.mit.edu, DNS:swartz-report.mit.edu, DNS:www.mit.edu, DNS:swartz-documents.mit.edu, DNS:web-forms.mit.edu, DNS:w.mit.edu, DNS:alum.mit.edu, DNS:alum-dev.mit.edu, DNS:www.web.mit.edu, DNS:news-office.mit.edu, DNS:web.mit.edu, DNS:web-cert.mit.edu, DNS:mit.edu, DNS:www.news-office.mit.edu, DNS:w3.mit.edu, DNS:betterworld.mit.edu, DNS:emergency.mit.edu
|_ Not valid before: 2019-07-01T00:00:00
|_ Not valid after: 2020-09-29T12:00:00
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_   http/1.1
|_   tls-nextprotoneg:
|_     http/1.1
|_     http/1.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.10 (90%), Crestron XPanel control system (89%), Linux 3.16 (88%), HP P2000 G3 NAS device (86%), ASUS RT-N56U WAP (Linux 3.4) (86%), Linux 3.1 (86%), Linux 3.2 (86%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (86%), Linux 3.10 - 4.11 (85%), Linux 3.13 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

```



این دستور سعی می کند تا جای ممکن سرویس های موجود روی هاست های موجود را بررسی کند و اطلاعاتی از قبیل سرویسهای مورد استفاده و ورژن آنها را با استفاده از الگوهای از پیش تعیین شده مشخص کند.

با توجه به اطلاعات به دست آمده، واضح است که این دستور اطلاعات بیشتری از iut استخراج کرده است. این در حالی است که mit حتی ورژن http را هم در اختیار کاربران قرار نداده است. ولی اطلاعات iut شامل اطلاعات سیستمها، کش ها، زبانهای مورد استفاده و ... است.

## Nmap -O [domain name \ IP] - ت

این دستور، با بررسی اطلاعات موجود در تلاش است که نوع یا ورژن سیستم عامل‌های مقصد را تشخیص دهد.

-----iut-----

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-10 12:38 Iran Daylight Time
Nmap scan report for iut.ac.ir (176.101.52.155)
Host is up (0.49s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.41 seconds
```

-----mit-----



The screenshot shows the Nmap GUI interface with the 'Nmap Output' tab selected. The scan was performed on mit.edu (88.221.9.235) at 2020-07-10 13:15 Iran Daylight Time. The output text is as follows:

```
nmap -O mit.edu

Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-10 13:15 Iran Daylight Time
Nmap scan report for mit.edu (88.221.9.235)
Host is up (0.22s latency).
rDNS record for 88.221.9.235: a88-221-9-235.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.10 (92%), Crestron XPanel control system (90%), Linux 3.16 (89%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%), Android 4.1.1 (86%), Linux 3.10 - 4.11 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.74 seconds
```

توجه کنید که باز هم iut اطلاعات کاملی از نوع و فرمور و کرنل‌های لینوکس در اختیار ما قرار داده است، در حالی که اطلاعات زیادی از نتیجه کار روی mit به دست نمی‌آوریم.

2- برای مقایسه نتیجه این دو اسکن، به زیر توجه میکنیم.

```

-Nmap 7.80 scan initiated Fri Jul 10 13:49:32 2020 as: nmap -O -A -v mit.edu
+Nmap 7.80 scan initiated Fri Jul 10 13:50:54 2020 as: nmap -O -A -v iut.ac.ir

-a104-102-90-162.deploy.static.akamaitechnologies.com, mit.edu (104.102.90.162):
-Host is up.
-Not shown: 998 filtered ports
-PORT      STATE SERVICE VERSION
-80/tcp    open  http      AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
-443/tcp   open  http      AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
-OS details:
-  Linux 4.10
-  Crestron XPanel control system
-  Linux 3.16
-  ASUS RT-N56U WAP (Linux 3.4)
-  Linux 3.1
-  Linux 3.2
-  AXIS 210A or 211 Network Camera (Linux 2.6.17)
-  HP P2000 G3 NAS device

+iut.ac.ir (176.101.52.155):
+Host is up.
+Not shown: 998 filtered ports
+PORT      STATE SERVICE VERSION
+80/tcp    open  http      nginx (reverse proxy)
+443/tcp   open  http      nginx (reverse proxy)
+OS details:
+  Linux 2.6.18 - 2.6.22

```

به طور کلی، به نظر میاید سیستم امنیتی دانشگاه صنعتی از سادگی پیروی میکند و دانشگاه mit تصمیم گرفته است پروتکل ها و برنامه های خود را از دید سایرین مخفی کند.

3- سیستمهای جدید از ipv6 پشتیبانی میکنند، ولی به دلیل آن که تقریباً تمام سیستمهای آن ها بر روی ipv4 صورت میگیرد، دقتی به کانفیگ سیستم برای ipv6 نمیکند.

نکته ای که باید به آن توجه داشته باشیم این است که ipv6 از لایه دو استفاده میکنند و از پروتکلی مثل ARP برای یافتن IP ها استفاده نمیکند. وقتی این نوع سیستمها به شبکه متصل میشوند، بسته های خود را یا یک آدرس IP و مک آدرس سیستم مشخص میکنند. در نهایت، منظر بسته های مولتی کست روتر ها میمانند تا شناسایی شوند. در نتیجه اگر تصمیم بگیریم این سیستمها را شناسایی کنیم، باید بسته های مولتی کست در شبکه پخش کنیم و منتظر جواب باشیم، چرا که حتماً سیستمهای ipv6 باید به این بسته ها پاسخ دهند.



برای آن که TCP syn ها را از IDS ها رد کنیم، چون به صورت معمول تعداد زیادی از این بسته به منزله یک حمله توسط IDS ها تشخیص داده میشود، لازم است که با استفاده از روش TCP tiny fragmentation، بسته های TCP را به قدری کوچک کنیم که بدون defrag کردن معنی خاصی ندهند، که باعث خواهد شد از سیستمهای تشخیص نفوذ به راحتی عبور کند.

4- برای گذشتن از چنین فایروالی، لازم است که از ipv6 تونلینگ استفاده کنیم. بدین منظور، با یک درخواست http get و داخل یک بسته UDP و پروتکل ipv6 برای یک سروری که این پروتکل را فعال دارد شروع میکنیم. فایروال چون دنبال فلگ TCP است، این نکته را تشخیص نمیدهد به آن اجازه ورود میدهد. علاوه بر آن، استفاده از بسته های برادکست که در قسمت قبل گفتم نیز کاربرد دارد. چرا که لازم است حتما به این بسته ها پاسخ دهند.

برای ارسال اطلاعات به یک مقصد خاص که توسط فایروال بسته شده است، لازم است از یک پراکسی سرور استفاده کنیم. بدین منظور، ابتدا بسته را به پراکسی سروری که برای فایروال بسته نیست ارسال میکنیم، و سپس پراکسی بسته را برای هدف اصلی فوروارد میکند.

5 - کد به پیوست قرار گرفته است. توجه کنید که استفاده از زبان پایتون و کد بهینه نشده ما خیلی از nmap کندتر عمل میکند. علاوه بر آن، nmap میتواند پاسخ هاست هایی که مستقیما پاسخ نمیدهد را بررسی کند و به طور کلی دقیق تر باشد.

