הפקולטה להנדסה
המחלקה להנדסת מערכות מידע

אבטחת מחשבים ורשתות תקשורת - עבודה 1

מגישים: עידו סולומון ת"ז 308111160
ליאור פרי ת"ז 203722814

Part A

1. (via packet summery/information window)
   Attacker (Last router hop on route from actual attacker):
   IP: 98.114.205.102
   MAC: 00:08:e2:3b:56:01
   Domain: pool-98-114-205-102.phlapa.fios.verizon.net

   Victim:
   IP: 192.150.11.111
   MAC: 00:30:48:62:4e:4a
   Domain: wrasse.adobe.com
2. (via last packet listing)
   16.219218 seconds
3. (via first and last packet's information window)
   Start: Apr 20, 2009 06:28:28.374595000 Jerusalem Daylight Time
   End: Apr 20, 2009 06:28:44.593813000 Jerusalem Daylight Time
4. (via Protocol Hierarchy window)
   Transport Layer:
   - Transmission Control Protocol (TCP)

   Application Layer:
   - Socks Protocol
   - NetBIOS Session Service
   - SMB (Server Message Block Protocol)
   - SMB Pipe Protocol
   - Distributed Computing Environment / Remote Procedure Call (DCE/RPC)
5. (via Capture File Properties window)
   527.5B
6. (via filter box)
   a) tcp.srcport == 445 && ip.dst == 98.114.205.102

tcp.srcport == 445 && ip.dst == 98.114.205.102

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000464	192.150.11.111	98.114.205.102	TCP	62	445 → 1821 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
6	0.134878	192.150.11.111	98.114.205.102	TCP	62	445 → 1828 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
7	0.135193	192.150.11.111	98.114.205.102	TCP	54	445 → 1821 [ACK] Seq=1 Ack=2 Win=5840 Len=0
8	0.238169	192.150.11.111	98.114.205.102	TCP	54	445 → 1821 [FIN, ACK] Seq=1 Ack=2 Win=5840 Len=0
11	0.267735	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=1 Ack=138 Win=6432 Len=0
13	0.487136	192.150.11.111	98.114.205.102	SMB	143	Negotiate Protocol Response
15	0.602303	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=90 Ack=306 Win=7504 Len=0
16	0.723001	192.150.11.111	98.114.205.102	SMB	311	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
18	0.840419	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=347 Ack=528 Win=8576 Len=0
19	0.957617	192.150.11.111	98.114.205.102	SMB	175	Session Setup AndX Response
21	1.073174	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=468 Ack=626 Win=8576 Len=0
22	1.189374	192.150.11.111	98.114.205.102	SMB	114	Tree Connect AndX Response
24	1.307168	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=528 Ack=730 Win=8576 Len=0
25	1.424860	192.150.11.111	98.114.205.102	SMB	193	NT Create AndX Response, FID: 0x4000
27	1.542401	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=667 Ack=890 Win=9648 Len=0
28	1.670219	192.150.11.111	98.114.205.102	DCERPC	182	Bind_ack: call_id: 1, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 results: Acceptance
30	1.797886	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=795 Ack=2350 Win=11680 Len=0
32	1.804003	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=795 Ack=3810 Win=14600 Len=0
34	1.806001	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=795 Ack=4210 Win=17520 Len=0
38	2.134590	192.150.11.111	98.114.205.102	DSSETUP	162	DsRoleUpgradeDownlevelServer response[Long frame (20 bytes)]

b) ip.src == 98.114.205.102 || ip.dst == 98.114.205.102

ip.src == 98.114.205.102 || ip.dst == 98.114.205.102

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	98.114.205.102	192.150.11.111	TCP	62	1821 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2	0.000464	192.150.11.111	98.114.205.102	TCP	62	445 → 1821 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	0.119058	98.114.205.102	192.150.11.111	TCP	60	1821 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.134175	98.114.205.102	192.150.11.111	TCP	60	1821 → 445 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
5	0.134550	98.114.205.102	192.150.11.111	TCP	62	1828 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	0.134878	192.150.11.111	98.114.205.102	TCP	62	445 → 1828 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
7	0.135193	192.150.11.111	98.114.205.102	TCP	54	445 → 1821 [ACK] Seq=1 Ack=2 Win=5840 Len=0
8	0.238169	192.150.11.111	98.114.205.102	TCP	54	445 → 1821 [FIN, ACK] Seq=1 Ack=2 Win=5840 Len=0
9	0.251859	98.114.205.102	192.150.11.111	TCP	60	1828 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	0.267724	98.114.205.102	192.150.11.111	SMB	191	Negotiate Protocol Request
11	0.267735	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=1 Ack=138 Win=6432 Len=0
12	0.354302	98.114.205.102	192.150.11.111	TCP	60	1821 → 445 [ACK] Seq=2 Ack=2 Win=64240 Len=0
13	0.487136	192.150.11.111	98.114.205.102	SMB	143	Negotiate Protocol Response
14	0.602288	98.114.205.102	192.150.11.111	SMB	222	Session Setup AndX Request, NTLMSSP_NEGOTIATE
15	0.602303	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=90 Ack=306 Win=7504 Len=0
16	0.723001	192.150.11.111	98.114.205.102	SMB	311	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
17	0.840405	98.114.205.102	192.150.11.111	SMB	276	Session Setup AndX Request, NTLMSSP_AUTH, User: \
18	0.840419	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=347 Ack=528 Win=8576 Len=0
19	0.957617	192.150.11.111	98.114.205.102	SMB	175	Session Setup AndX Response
20	1.073151	98.114.205.102	192.150.11.111	SMB	152	Tree Connect AndX Request, Path: \\192.150.11.111\ipc$
21	1.073174	192.150.11.111	98.114.205.102	TCP	54	445 → 1828 [ACK] Seq=468 Ack=626 Win=8576 Len=0
22	1.189374	192.150.11.111	98.114.205.102	SMB	114	Tree Connect AndX Response
23	1.307145	98.114.205.102	192.150.11.111	SMB	158	NT Create AndX Request, FID: 0x4000, Path: \lsarpc

c) ip.ttl > 100 && tcp.ack == 0 && tcp.dstport != 445

ip.ttl > 100 && tcp.ack == 0 && tcp.dstport != 445

No.	Time	Source	Destination	Protocol	Length	Info
36	2.091833	pool-98-114-205-102…	wrasse.adobe.com	TCP	62	1924 → 1957 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
68	6.142326	pool-98-114-205-102…	wrasse.adobe.com	TCP	62	2152 → 1080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1

2 packets found

7. (via filter and the Displayed column in the Capture File Properties window)
   159 packets, 167332B
8. (via IO Graphs window)
   t = 10sec
   1.892e+04 B/sec
9. (via follow TCP on TCP session 3)
   ssms.exe
10. (via follow TCP on TCP session 3)
    User name is 1
    Password is 1
    FTP is not an encrypted protocol, thus the user name and password are available to us.
11. (via Statistics > Conversations)
    There are 5 TCP Sessions in the file.
    (via Flow Graph after filtering for Session 1 packets)
    Graph is in the following page.

Time	pool-98-114-205-102.phlapa.fios.verizon.net		wrasse.adobe.com	Comment
0.134550	1828	SYN →	445	Seq = 0
0.134878	1828	← SYN, ACK	445	Seq = 0 Ack = 1
0.251859	1828	ACK →	445	Seq = 1 Ack = 1
0.267724	1828	PSH, ACK - Len: 137 →	445	Seq = 1 Ack = 1
0.267735	1828	← ACK	445	Seq = 1 Ack = 138
0.487136	1828	← PSH, ACK - Len: 89	445	Seq = 1 Ack = 138
0.602288	1828	PSH, ACK - Len: 168 →	445	Seq = 138 Ack = 90
0.602303	1828	← ACK	445	Seq = 90 Ack = 306
0.723001	1828	← PSH, ACK - Len: 257	445	Seq = 90 Ack = 306
0.840405	1828	PSH, ACK - Len: 222 →	445	Seq = 306 Ack = 347
0.840419	1828	← ACK	445	Seq = 347 Ack = 528
0.957617	1828	← PSH, ACK - Len: 121	445	Seq = 347 Ack = 528
1.073151	1828	PSH, ACK - Len: 98 →	445	Seq = 528 Ack = 468
1.073174	1828	← ACK	445	Seq = 468 Ack = 626
1.189374	1828	← PSH, ACK - Len: 60	445	Seq = 468 Ack = 626
1.307145	1828	PSH, ACK - Len: 104 →	445	Seq = 626 Ack = 528
1.307168	1828	← ACK	445	Seq = 528 Ack = 730
1.424860	1828	← PSH, ACK - Len: 139	445	Seq = 528 Ack = 730
1.542389	1828	PSH, ACK - Len: 160 →	445	Seq = 730 Ack = 667
1.542401	1828	← ACK	445	Seq = 667 Ack = 890
1.670219	1828	← PSH, ACK - Len: 128	445	Seq = 667 Ack = 890
1.797873	1828	ACK - Len: 1460 →	445	Seq = 890 Ack = 795
1.797886	1828	← ACK	445	Seq = 795 Ack = 2350
1.803993	1828	ACK - Len: 1460 →	445	Seq = 2350 Ack = 795
1.804003	1828	← ACK	445	Seq = 795 Ack = 3810
1.805992	1828	PSH, ACK - Len: 400 →	445	Seq = 3810 Ack = 795
1.806001	1828	← ACK	445	Seq = 795 Ack = 4210
1.978646	1828	ACK →	445	Seq = 4210 Ack = 795
2.134590	1828	← PSH, ACK - Len: 108	445	Seq = 795 Ack = 4210
2.379299	1828	ACK →	445	Seq = 4210 Ack = 903
5.072673	1828	RST →	445	Seq = 4210

12. We believe that the attack was an automated one, as it only took the attacker ~16.2 seconds to execute it, and it is more plausible that it was performed by a pre-prepared script or a tool rather than by a human (The attacker entered 7 different command in that small time frame).
13. Victim's OS is Windows 2000 build 2195. Found by searching for the string "windows" in the packet detail. Following line found in SMB packet (packet #14) originating from victim: "Native OS: Windows 2000 2195".
    Screencap is in the following page.

```
> Frame 14: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits)
> Ethernet II, Src: Cisco_3b:56:01 (00:08:e2:3b:56:01), Dst: SuperMic_62:4e:4a (00:30:48:62:4e:4a)
> Internet Protocol Version 4, Src: pool-98-114-205-102.phlapa.fios.verizon.net (98.114.205.102), Dst: wrasse.adobe.com (192.150.11.111)
> Transmission Control Protocol, Src Port: 1828, Dst Port: 445, Seq: 138, Ack: 90, Len: 168
> NetBIOS Session Service
v SMB (Server Message Block Protocol)
  > SMB Header
  v Session Setup AndX Request (0x73)
      Word Count (WCT): 12
      AndXCommand: No further commands (0xff)
      Reserved: 00
      AndXOffset: 164
      Max Buffer: 4356
      Max Mpx Count: 10
      VC Number: 0
      Session Key: 0x00000000
      Security Blob Length: 32
      Reserved: 00000000
    > Capabilities: 0x800000d4, Unicode, NT SMBs, NT Status Codes, Level 2 Oplocks, Extended Security
      Byte Count (BCC): 105
    > Security Blob: 4e544c4d53535000010000009782 08e00000000000000000...
      Native OS: Windows 2000 2195
      Native LAN Manager: Windows 2000 5.0
      Primary Domain:
```

Part B

Question 1

ממספרים את הקבוצה מ-1 עד 20.

חבר משלחת מספר 1 בוחר מספר שרירותי לא עגול X_1, הגדול ממש (פי כמה פעמים) מכמות הזהב שאסף, ומעביר אותו בדיסקרטיות לחבר משלחת מספר 2.

חבר משלחת מספר 2 מוסיף ל-X_1 את כמות הזהב שאסף, ומעביר את X_2 לחבר משלחת מספר 3.

כך עבור כל חבר משלחת i יתקבל מספר X_{i-1}, אליו תתווסף כמות הזהב אותה אסף אותו חבר משלחת, ויועבר מספר X_i לחבר משלחת i+1.

חבר משלחת מספר 20 יעביר את X_{20} לחבר המשלחת הראשון, שבתורו יחסר מ-X_{20} את X_1, ויוסיף למספר החדש את כמות הזהב האמיתית שאסף, כשהתוצאה תהיה כלל הזהב שאספו חברי המשלחת.

Question 2

1. אמצעים בהם ניתן להשתמש כוללים שימוש בפרוטוקול SSL כדי לוודא את מהימנותו של האתר בעת התחברות אליו (התחברות מאובטחת), חינוך ציבור המשתמשים לזיהוי אתרים מתחזים והודעות דיוג הנשלחות אליהם, קניית כתובות (URL) הדומות לכתובת האתר המקורי (עקב שגיאות כתיב ושחלוף/החסרת אותיות) ולנתב מהן את התעבורה לאתר (כמובן שצעד זה לא יעיל מול כתובות דומות שכבר נמצאות בבעלות זרה), ושימוש באמצעים טכנולוגיים באתר בהם המשתמש מגדיר מראש תמונה הייחודית לו, המוטמעת בטפסי ההתחברות לאתר – אתרים זדוניים שהעתיקו את מבנה האתר לא יכולים להעתיר תמונות אלו לכל משתמש, וכך נחשפים כמרמה למשתמש.
2. www.globes.co.il
   a) cmd: theharvester –d globes.co.il –b all
      eli6@globes.co.il
      eronen@globes.co.il
      shlomitlan@globes.co.il
      eli@globes.co.il
      yairo@globes.co.il
      michal@globes.co.il

hagitpr@globes.co.il
ariel@globes.co.il
matigolan@globes.co.il
leonid@globes.co.il
daliat@globes.co.il
meir…@globes.co.il
hashuk@globes.co.il
peled@globes.co.il
roeid@globes.co.il
katavm@globes.co.il
ellaj@globes.co.il
avishay_o@globes.co.il
kesef@globes.co.il
dafi@globes.co.il
glik@globes.co.il

b) cmd: theharvester –d globes.co.il –b linkedin
Eldar Gilad
Shmulik Cohen
Yuval Perelman
Ran Oz
Sholem Lougov
Asaf Shapira
Ilan Goldschmidt
Shalom Daskal
Kfir Hayoun
Alon Levin
Lital Vinogradsky
Ronan Vinograd
Doron Hoch
Shahar Brimer
Yaron Eli

c) cmd: theharvester –d globes.co.il –b all
new.globes.co.il
images.globes.co.il
m.globes.co.il
smile.globes.co.il
wink.globes.co.il
duns100.globes.co.il
emagazine.globes.co.il
dns.globes.co.il
dns2.globes.co.il
digital.globes.co.il

3. digital.globes.co.il
cmd: nmap digital.globes.co.il –O
OS: Linux 2.4.X|3.X
Open TCP ports: 80, 443
cmd: nmap digital.globes.co.il –sU
Open UDP ports: all UDP ports are open