אוניברסיטת תל-אביב
מדעי המחשב

מבוא לאבטחת מידע
שאלות לדוגמה

סמסטר ב' תשע"ג

מרצה: ערן טרומר ואבישי וול

<u>הנחיות:</u>

- מותר להשתמש בכל חומר עזר כתוב על גבי נייר בלבד.
- המבחן כולל 6 שאלות. מספר הנקודות מופיע לידי כל שאלה.
- כתבו את תשובותיכם <u>על גבי טופס המבחן</u> במקום המוקצה לכך.
  <u>מומלץ מאד</u> לכתוב תחילה את התשובה במחברת הטיוטה שקיבלתם ורק אחר כך להעתיק אותה, בצורה ברורה וקריאה, לטופס המבחן. תשובות במחברת לא יקראו.
- נמקו בקצרה אך בבהירות את כל טענותיכם. כל שאלה לא נימוק לא תזכה בניקוד.
- ניתן לענות בעברית או באנגלית

השאלות הכתובות באנגלית ניתנות לצורך תרגול, והן קשות במקצת מהצפוי בבחינה.
בבחינה, כל השאלות ישאלו בעברית.

בנוסף, יתכנו שאלות הגדרת מושגים.

שאלה 1 (18 נק')

בנתבים ביתיים נהוג שימוש ב-NAT (Network Address Translation) על מנת לשתף מספר משתמשים בכתובת IP בודדת. נהוג כי הרשת הביתית נמצאת בטווח הכתובות 192.168.10.1 – 192.168.10.254.
בתצורה זו, כל מחשב ברשת יכול להוציא קישורי TCP ולהעביר מנות UDP החוצה מהרשת, כאשר הנתב הביתי מבצע תרגום כתובות בין הכתובת הפומבית (הכתובת האינטרנטית) ובין הכתובות הפנימיות.

בנוסף, קיים על נתבים רבים שירות של Port Forwarding אשר מאפשר להגדיר בצורה סטטית מפת תרגום בין פורטי TCP ו\או UDP אשר יש לקדם בצורה שקופה אל מחשב ספציפי ברשת הפנימית, כך שניתן יהיה לחשוף שירות רשת פנימי לעולם הרחב (לדוג': שרת HTTP ביתי, שרת Minecraft, וכיוב').

לבסוף, קיים שירות בשם PUPnP (Psuedo Universal Plug and Play), אשר ממומש מעל מנות UDP ופועל לפי הפסאודו-קוד הבא:

```
(buffer,ipudp_header) = recvfrom_udp_packet(UPNP_PORT);
if buffer[0:5] == "PUPNP":
   if buffer[5:13] == "ACTIVATE":
      (internal_ip, internal_port, external_port) =
        get_ports_and_ips_from_buffer(buffer[13:]);
      turn_on_port_forwarding_for(internal_ip, internal_port,
                                  external_port)

   elif buffer[5:13] == "DEACTIVA":
      (external_port) = get_externl_ports_from_buffer(buffer[13:])
      turn_off_port_forwarding_for(external_port)
```

א. [8 נק'] בהינתן הקוד הנ"ל, כיצד יוכל תוקף הנמצא מחוץ לרשת (אך נגיש לתווך האינטרנטי) לגשת לשירות פנימי ברשת?

ב. [6 נק'] בגרסא חדשה של המוצר, הקוד עודכן –

```
(buffer,ipudp_header) = recvfrom_udp_packet(UPNP_PORT);
if get_udp_packet_source_ip_from(ipudp_header) AND get_local_LAN_netmask() !=
                get_udp_packet_source_ip_from(ipudp_header):
   return
if buffer[0:5] == "PUPNP":
   if buffer[5:13] == "ACTIVATE":
      (internal_ip, internal_port, external_port) =
        get_ports_and_ips_from_buffer(buffer[13:])
      turn_on_port_forwarding_for(internal_ip, internal_port, external_port)
   elif buffer[5:13] == "DEACTIVA":
      (external_port) = get_externl_ports_from_buffer(buffer[13:])
      turn_off_port_forwarding_for(external_port)
```

כיצד תוכל להתגבר על בדיקה זו ? הסבר בצורה ברורה.

ג. [4 נק'] בגרסא חדשה (עוד יותר) של המוצר, הודעות ה-UPNP עוברות מעל קישורי TCP. האם תוכל עדיין לנצל את החולשה?

שאלה2 (37 נק')

לתוכנית מסוימת (הרצה במכונת Linux) ניתן להכניס קלט אשר יועבר כפרמטר לפונקציה הבאה:

```
.text:08048434                 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:08048434
.text:08048434                 ; Attributes: bp-based frame
.text:08048434
.text:08048434                 sub_8048434  proc near               ; CODE XREF: .text:08048376p
.text:08048434
.text:08048434                 var_88       = dword ptr -88h
.text:08048434                 var_6C       = byte ptr -6Ch
.text:08048434                 var_4        = dword ptr -4
.text:08048434                 arg_0        = dword ptr  8
.text:08048434
.text:08048434  55                           push    ebp
.text:08048435  89 E5                        mov     ebp, esp
.text:08048437  53                           push    ebx
.text:08048438  83 EC 74                     sub     esp, 74h          ; Integer Subtraction
.text:0804843B  8B 45 08                     mov     eax, [ebp+arg_0]
.text:0804843E  80 38 61                     cmp     byte ptr [eax], 61h ; Compare Two Operands
.text:08048441  75 1C                        jnz     short loc_804845F ; Jump if Not Zero (ZF=0)
.text:08048443  8D 50 02                     lea     edx, [eax+2]      ; Load Effective Address
.text:08048446  52                           push    edx
.text:08048447  68 50 85 04 08               push    offset aHandledDataS ; "Handled data: %s\n"
.text:0804844C  0F BE 40 01                  movsx   eax, byte ptr [eax+1] ; Move with Sign-Extend
.text:08048450  8D 5D 94                     lea     ebx, [ebp+var_6C] ; Load Effective Address
.text:08048453  50                           push    eax               ; size_t
.text:08048454  53                           push    ebx               ; char *
.text:08048455  E8 F6 FE FF FF               call    _snprintf         ; Call Procedure
.text:0804845A  89 1C 24                     mov     [esp+88h+var_88], ebx
.text:0804845D  EB 08                        jmp     short loc_8048467 ; Jump
.text:0804845F                 ; ---------------------------------------------------------
.text:0804845F
.text:0804845F                 loc_804845F:                              ; CODE XREF: sub_8048434+Dj
.text:0804845F  83 EC 0C                     sub     esp, 0Ch          ; Integer Subtraction
.text:08048462  68 62 85 04 08               push    offset aUnknownType ; "Unknown type\n"
.text:08048467
.text:08048467                 loc_8048467:                              ; CODE XREF: sub_8048434+29j
.text:08048467  E8 B4 FE FF FF               call    _puts             ; Call Procedure
.text:0804846C  83 C4 10                     add     esp, 10h          ; Add
.text:0804846F  8B 5D FC                     mov     ebx, [ebp+var_4]
.text:08048472  C9                           leave                     ; High Level Procedure Exit
.text:08048473  C3                           retn                      ; Return Near from Procedure
.text:08048473                 sub_8048434  endp
.text:08048473
.text:08048473                 ; ---------------------------------------------------------
```

א. [8 נק'] הנדסו לאחור את הפונקציה הבאה, ותארו את פעולתה בצורה קצרה ומדויקת.

ב. [4 נק'] בהתבסס על הקוד, תארו את מבנה המחסנית של התוכנה.

ג. [5 נק'] זהו חולשה בתוכנה והסבר בקצרה כיצד ניתן לנצל אותה (הנח שמנגנוני ASLR ,DEP אינם פעילים).

ד. [5 נק'] השתמשו ב- shellcode הבא על מנת לנצל את החולשה. תארו כיצד צריך להראות הקלט כולו על מנת שזה יעבוד. (הניחו שכתובת המחסנית בכניסה לפונ' היא 0xDEADBEEF.)

```
seg000:00000000  B8 18 FF F7 B7          mov     eax, 0B7F7FF18h ; "/bin/sh"
seg000:00000005  50                      push    eax
seg000:00000006  B8 30 E4 E5 B7          mov     eax, 0B7E5E430h ; system
seg000:0000000B  FF D0                   call    eax             ; Indirect Call Near Procedure
seg000:0000000D  B8 B0 1F E5 B7          mov     eax, 0B7E51FB0h ; exit
seg000:00000012  FF D0                   call    eax             ; Indirect Call Near Procedure
```

[2 נק'] כעת מניחים שכתובת הבסיס של המחסנית ידועה רק בקירוב(±0x30 בתים), הוסיפו לקלט NOP-ים על מנת שהחולשה תמיד תעבוד.

ה. [5 נק'] לאחר שהאדמיניסטרטור של המחשב גילה על החולשה הוא מיד הפעיל את האופציה של DEP בקרנל. באמצעות המידע שכבר ברשותך, בנה קוד ROP (Return Oriented Programming) שמספק את אותו הפונקציונליות כמו של ה- shellcode מסעיף ד' ועצב את הקלט מחדש. כל ההנחות עד עכשיו עדיין תקפות.

ו. [3 נק'] לאחר בחינה של התוכנה נתגלה לתוקף שיש מס' גרסאות פגיעות לתוכנה הפועלות באותו אופן, בכל אחת מהן שונה גודל הBUFFER במעט (השינויים בקוונטות של 4 בתים) פתור את הבעיה של התוקף ע"י שימוש בנתונים הקיימים בשאלה.

ז. [5 נק'] לאחר שהאדמינסטרטור גילה בשנית את הבעיה הוא הפעיל את ה ASLR בקרנל, בהנחה שיש בידך אמצעי לעקוף מנגנון זה ע"י הדלפת מידע, ציין אילו קטעים בקלט ייצטרכו לעבור שינוי דינמי, והסבר מדוע.

שאלה 3 (20 נק')

בשאלה זו ניתן להניח כל הנחה סבירה, כל עוד היא מצויינת במפורש.

ב- headers של כל packet בשכבת IP קיים שדה של 16-ביט בשם Identification. התקן של IP מחייב שתוכן שדה ה-Identification יהיה בעל ערך שונה עבור כל packet בין שולח S למקבל D. דרך פשוטה למימוש שדה ה-Identification במערכות הפעלה היא שהשולח יחזיק מונה יחיד, גלובאלי, שמוגדל ב-1 עם כל packet שנשלח על ידו (ללא חשיבות לזהות המקבל).

א. נניח שמערכת ההפעלה במחשב P מממשת את שדה Identification ע"י מונה גלובאלי כפי שתואר למעלה. נניח עוד כי P עונה להודעות ping. בשליטתכם מחשב A. הציעו שיטה לבדוק אם מחשב P שלח packet אחד או יותר למחשב כלשהו (שאיננו A) במשך הדקה האחרונה. מותר לכם לשלוח הודעות כרצונכם מ-A ל-P.

_____

_____

_____

_____

ב. נמשיך בתנאים של סעיף א. מטרתכם כעת היא לגלות אם מחשב קורבן V מאזין על TCP port 23, באופן חשאי: אסור לכם לשלוח packets רגילות מ-A ל-V. מותר לשלוח packets מ-A ל-V רק אם מזייפים בהן את כתובת השולח לכתובת שאיננה של A (כלומר מותר לשלוח רק spoofed packets). תארו איך אפשר לנצל את מחשב P כדי להשיג את המטרה. רמזים על התנהגות TCP:

- מחשב שמקבל SYN packet לפורט TCP פתוח (שהוא מאזין עליו) מחזיר לכתובת השולח SYN/ACK packet
- מחשב שמקבל SYN packet לפורט TCP סגור מחזיר לכתובת השולח RST packet
- מחשב שמקבל SYN/ACK packet שהוא לא ממתין לה מחזיר לכתובת השולח RST packet
- מחשב שמקבל RST packet לא מחזיר שום תגובה

_____

_____

_____

_____

ג. רישמו בטבלה את סדרת ההודעות שישלחו ע"י השחקנים השונים (A, V, P) לפי סדרן. מלאו שורות ע"פ הצורך, לפי מספר ההודעות שנשלחות.

עיקרי ההודעה	Destination	Source	שולח אמיתי

ד. הציעו שינוי במימוש TCP/IP במערכת ההפעלה של P שיקלקל את ההתקפה. זכרו כי אסור לכם לחרוג מההתנהגות המוכתבת על ידי התקן, אבל מותר לשנות את פרטי המימוש.

_____

_____

_____

_____

_____

Question 4 (15%)

A given Linux computer serves multiple users. Unfortunately, all files on the system must be world-readable (so that some badly-designed backup software can read them; we can't change that). Each user, however, wishes his files to remain secret from other users.

1. (7) The system supports Systrace. How can the system administrator configure Systrace it to enforce the above requirement?

2. (8) Systrace is unavailable, but the system has a TPM. Propose a way for users to use the TPM to protect their files (without users having to remember passwords).
   You can ask the system administrator to make some small, local change to the system if needed. You may assume that only one user is logged in any any given time, and that the system can be rebooted every time a different user wishes to log in. Assume that the TPM functionality is exposed to user-space via suitable system calls.

Answers:

1. The system administrator can set a policy which, effectively, neutralizes the “world-readable” bit on user files:
    - Deny all file reads by default
    - Allows reads by each user from files that he, owns or files belonging to a group of which he is a member
    - Allow reads to needed globals, e.g., shared libraries and data under /usr
    - Allow the backup system (i.e., a specific user) read access to all files
2. A possible solution:
   Change the system so that, after a successful login of a user and before granting user access to the system, the login process calls TPM_extend, extending the PCRs with the user’s (unique) user-name. A user could now use TPM_seal/unseal to seal/unseal a key.
   After the sealing of a key with a non-tampered system by a user, it is guaranteed that only he, using the same system, can unseal the resultant blob.

Question 5 (10%)

In the following TPM question, please (unrealistically) assume there are no covert channels or implementation bugs in the system.

a. (5) Achilles is using the Amazon EC2 cloud service to run Windows 7 in a virtual machine. He is concerned about his VM's vulnerability to hackers from faraway Troy who may have remotely broken into Amazon's infrastructure. While installing Windows, Achilles noticed the option to enable BitLocker, Microsoft's implementation of disk encryption using TPM sealing. After enabling the option, Windows reported that BitLocker with TPM sealing has been successfully activated.

   Can Achilles rest on his laurels, knowing that his data can be accessed only as permitted by the Windows access control mechanism?

b. (5) Achilles decided to use a physical machine instead. He bought a trustworthy computer, carefully configured it with BitLocker TPM functionality, and then shipped it to a high-bandwidth data center operated by hosting service Crackspace. Late at night, a Trojan spy infiltrated the Crackspace data center carrying a screwdriver and a piece of wire of just the right size to short out the TPM "reset" pin. What can the spy do?

Answers:

a. Amazon's VMM can read the memory of Achilles, including his decrypted data. The TPM offers no protection since it is (or could be) virtualized by Amazon's VMM. (TPM measurements are only meaningful if the full real boot sequence is protected). Another consideration is architectural side channels.
b. The spy can reboot the machine into malicious code of its choosing, reset the TPM by shorting its reset pin (now the PCRs are zero), extend the PCRs to the "correct" values of the Windows version Achilles installed, and then unseal the disk decryption key.

Question X3 (10%)

A user downloaded from the Internet a program that is supposed to add bunnies to photos. He doesn't trust the program, so he would like to try running it on one of his image files without letting the program access any other file on the computer.

a. (5) Can the user do this in a system based on capabilities? Explain.

b. (5) Can the user do this in a system based on access control lists? Explain.

Answers:

a. Yes. Give the program the capability to access the image file, and nothing else. In particular, the program must not be able to talk to other processes and obtain additional capabilities from those; hence, such talking must be controlled by capabilities as well. (Most answers omitted this last part.)

b. We can try to create a new user account (subject) for running the program, and give this user access only to the image file. But this is difficult to enforce with Discretionary Access Control based on ACLs. For example, there could be some files in the system that are accessible by any user account according to their ACL; or other human users on the system may change ACLs on files they own to permit access to the new user. (With Mandatory Access Control, we could enforce the requisite permissions.)