מסמך מטלות סיום : קורס הגנת פרוטוקולים גרסה: 200.1

אוניברסיטת אריאל סמסטר ב תשפב

מבנה המטלת סיום:

א-ד משימות קטנות משותפות לכולם הצוותים (10*4 מתוך 100% נקודות למטלה זו)

ה. משימת חקר שמתחלקת לחלק תאורטי ולחלק מימושי 60% מתוך 100% נקודות למטלה זו ,
בתוך משימת החקר ישתנה האחוז בין המרכיב התאורטי והמרכיב המימושי .
כללית יתכנו הקלות ולכן כדאי להתחיל במשימת החקר ויש לעקוב (וגם לפנות ולשאול)
בבקשה לעקוב אחרי מספר הגירסה של מסמך המטלות.

חלק ממשימות החקר רחבות, וכמובן תינתן הדרכה מדויקת למיקוד ! אבל גם נשמר לכם חופש בחירה ומקום להצעות יצירתיות ! ולכן אין מיקוד קשיח מראש. !

בתוך משימת החקר: יתכן עידכון המרכיב המימושי עם התקדמות משימת החקר וההצלחה במימוש
(בהחלט יתכן גם ציון גבוה למרכיב מימוש שלא צלח במלואו ....)
בתוך משימות החקר יש לצרף ביביליוגרפיה רלונטית ורשימת מקורות
אבל גם רשימת מקורות שהם רקע לימודי וגם מקורות בנושא שהם פחות רלונטים ישירות למימוש לכם.

כללית : (בדומה לתרגיל ההגשה במהלך הסמסטר)
יש להריץ את המעבדה ולהגיש דו"ח+צילומי מסך, ע"פ הנחיות כלליות להגשת דו"ח משימה :
יש לודא טקטס קריא גם בתמונות. יש לצרף קוד פיתון מתועד כולל שמות המגישים. יש להגיש גם רשימת קבצים מוגשים.
צילומי המסך יהיו קריאים וממוספרים. (מספר רץ ואו שם משמעותי לכל צילום)
צילומים ושירטוטים יוגשו הן ב תוך דו"ח והן בנפרד. הגשה עי קובץ ZIP במודל. דוח במסמך MSWORD DOCX .
יש לתת שמות משמעותיים למחשבים , ל DOCKER IMAGES ול interfaces . Attacker, Victim etc
כל תת משימה : תתחיל עם כותרת ותכלול תיאור מיבני של 4 פיסקאות:

1) מבוא : רקע תאורטי קצר

2) תיעוד ביצוע המשימה

3) סיכום השלב

4) מבט להמשך:

משימות משותפות: יש להגיש דוח עם פירוט מבנה רשת צעדים עיקריים ופירוט רשת ומרכיבים כולל פירוט גרסאות תוכנה (מימוש במכונות וירטואליות בלינוקס ואו דוקרים)

הגשות: משימות א-ד בתיבות הגשה במודל

משימה ה. כולל דוחות חלקיים : במייל mordiaripp2022b@gmail.com

בכל מייל בבקשה לכלול :

בכותרת : שמות חברי הצוות ובגוף המייל: פירוט מלא של כל שמות חברי הצוות+תז+טלפונים ניידים_מייל

א. מימוש מתקפת Local DNS

אפשר לראות

Local DNS Attack Lab (seedsecuritylabs.org)

/https://seedsecuritylabs.org/Labs_16.04/Networking/DNS_Local

ב. מימוש מתקפת Remote DNS דן קמינסקי

אפשר להתסמך על

/https://seedsecuritylabs.org/Labs_20.04/Networking/DNS/DNS_Remote

https://seedsecuritylabs.org/Labs_20.04/Files/DNS_Remote/DNS_Remote.pdf

אבל יתקבלו גם מימושים אחרים

להעשרה:

https://en.wikipedia.org/wiki/Dan_Kaminsky

https://duo.com/blog/the-great-dns-vulnerability-of-2008-by-dan-kaminsky

http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

אפשר לראות גם : https://seedsecuritylabs.org/Labs_16.04/PDF/DNS_Remote_new.pdf

ג. מימוש מתקפת DNS Rebinding

ראו :

https://web.ecs.syr.edu/~wedu/seed/Labs_12.04/Networking/DNS_Remote/DNS_Remote.pdf

DNS_Rebinding.pdf (seedsecuritylabs.org)

https://seedsecuritylabs.org/Labs_20.04/Files/DNS_Rebinding/DNS_Rebinding.pdf

ד. מימוש מתקפת חטיפה BPG4 Hijacking בעזרת MiniNet בלינוקס

לממש הדגמה של BGP4 Hijacking בעזרת MiniNet , אפשר לראות הדגמה ב

BGP Path Hijacking Attack Demo - mininet - YouTube

https://www.youtube.com/watch?v=Ovh_ceqp63M

לחילופין יתכן שימוש בסימולאטור החדש של SeedLabs

כמובן מומלץ ללמוד על MiniNet (יתכן שיעור הסבר)

משימות חקר ומימוש

ביצוע בשלשות (אבל שיחת הצגה והערכה בעל פה)

משימות חקר (לצורך אישור נושא מראש כל צוות יודע על נושא בחירתו במייל+שמות השותפים+פרטיהם תז+טלפון+במייל , ויתכן שיתאפשר ביצוע אותה משימה עי יותר מצוות אחד)

מומלץ (וחלק מההערכה) לשלוח דוח חלקי עם תיאור התקדמות וכיונים לדיון במהלך העבודה

בכל משימה יש לתת תיאור רקע תיאורטי +רשימת מקורות
לפרט אלטרנטיבות מימוש ולנסות לממש
ינתן משקל שונה במשימות שונות למרכיב התאורטי מול מרכיב המימוש

מימושים בלינוקס עם SCAPY או ב בשפת Cאו CPP

יש גם לחפש מאמרים אקדמיים, באם קיימים בנושא ,במאגרי המידע האקדמיים שבספריית האוניברסיטה.

ההמשימות הן משימות חקר ויש לדווח בתחילת הבחירה ובאמצע ההתקדמות ועפ ההתקדמות יעודכנו היעדים – כל צוות ע"פ התמקדותו. במקרה של קשיי מימוש תהיה התחשבות ולא כל משימה צריכה להצליח במלואה ולחילופין ישנה גמישות ביצירתיות . (אבל רצוי בתיאום)
יש להציע כיוני המשך ו נקודות נוספות לבדיקה או בדיקה מתקדמת יותר במסגרת תת-תחום זה. (לביצוע עתידי שלא במסגרת משימה זו,אבל יראה על הבנה מעמיקה)

על כל חברי הצוות להיות בקיעים בנושאים התאורטיים או לפרט את תחומי

בהתחלה תהינה פגישות הסבר לכל הקורס ובהתחלה ובאמצע ופגישות הסבר אישיות יתכן שבסיום יהיה צורך להציג ולהסביר בזום.
מקורות והנחיות מדויקות יפורטו בהמשך. (לאחר לימודו ראשוני)

רשימת נושאים לחקר: יש לבחור אחד (או רעיונות דומים)

1) DNS FingerPrinting

בדיקת Cache של שרתי DNS לצורך איתור האם יש דרכו לקוחות שפנו לשרת מרוחק אחר.

יתכנו נושאים אחרים שקשורים לDNS FingerPrinting באופן שונה: מוזמנים להציע.

יש לאתר מאמרים בנושא ובפרט על הפרויקט של סיטיזן לאב הקנדית (ביל מרזק) באיתור שרתי התקיפה של חברת NSO ולאחר איתורם איתור שרתי DNS איזוריים ואיתור לקוחות עי

יש לכתוב רקע תאורטי ולנסות לממש כלי בפיתון לבדיקה של רשימת שרתי DNS לנוכחות שדה ב Cache שלהם בהשוואה ל פניה מרוחקת.

ניתן להתחיל במימוש סביבת בדיקה מקומית.
ראו:

HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries - The Citizen Lab

https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-/countries

The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender - The Citizen Lab

/https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae

אבל אולי לקבל רעיונות מ :

Effective DNS server fingerprinting method

Effective DNS server fingerprinting method | IEEE Conference Publication | IEEE Xplore

DNS-based Network Fingerprinting - RWTH AACHEN UNIVERSITY Research Group IT-Security - English (rwth-aachen.de)

https://www.itsec.rwth-aachen.de/cms/ITSEC/Forschung/Projekte/~fnvwz/DNS-based-Network-Fingerprinting/?lidx=1

2) היבטי אבטחה בפרוטוקול (RFC 9000) QUIC RTT

הצג שיקולי אבטחה ותקיפה ביחס ל QUIC ע"פ
0-RTT Attack and Defense of QUIC Protocol

https://ieeexplore.ieee.org/document/9024637
בפרט מתקפת 0 RTT
שיקלו הקמת מערכת (זמינות מימוש של הפרוטוקול) ונסו להדגים מיתקפה זו למשל בסיוע

0-RTT Attack and Defense of QUIC Protocol

השוו (כתבו פרק תאורטי)

QUIC has many benefits when compared to existing "TLS over TCP" scenarios:

אפשר לראות קוד מימוש של הפרוטוקול:
https://github.com/microsoft/msquic

רקע על הפרוטוקול:

QUIC RTT (RFC 9000)

QUIC is a secure general-purpose, encrypted, multiplexed, and low-latency transport protocol designed from the ground up to improve transport performance for HTTPS traffic. QUIC has become RFC standard (RFC 9000) (at May 2021) and is expected to become the dominant transport protocol in the Internet over TCP.
Most of QUIC packets are encrypted. The payload is encrypted and also most of the header fields.

ראו rfc9000

3) היבטי אבטחה ותקיפה בפרוטוקול IPV6 (מספר משימות שונות לקבוצות שונות)

לימדו על הדומה והשונה בין IPV6 ו IPV4
ראו את :
https://www.usenix.org/system/files/conference/woot14/woot14-ullrich.pdf
https://conference.apnic.net/34/pdf/ipv6-security_1346214191.pdf
A Complete Guide on IPv6 Attack and Defense (giac.org)
https://www.giac.org/paper/gsec/31795/complete-guide-ipv6-attack-defense/125363
IPv6 Security Guide: Do you Have a Blindspot? (varonis.com)
https://www.varonis.com/blog/ipv6-security
mitm6 – compromising IPv4 networks via IPv6 – Fox-IT International blog
/https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6

Scariest IPv6 attack scenarios | Computerworld
https://www.computerworld.com/article/2510866/scariest-ipv6-attack-scenarios.html

Mitigating IPv6 Poisoning Attacks | LMG Security
/https://www.lmgsecurity.com/mitigating-ipv6-poisoning-attacks

ראו כלי בשם THC : ואת תתי התקיפות שבתוכו.
GitHub - vanhauser-thc/thc-ipv6: IPv6 attack toolkit
https://github.com/vanhauser-thc/thc-ipv6

thc-ipv6 | Kali Linux Tools

/https://www.kali.org/tools/thc-ipv6

תארו מיתקפות ישנות וחדשות.
ביחרו מיתקפה אחת ונסו לממשה (למשל DAD מיתקפות DHCP6)

תתבצע חלוקת סוגי מיתקפות בין קבוצות שונות .
יפורט לעומק בהמשך.
למשל : מימוש מנגנון גילוי למיתקפה (רק גילוי)

4) היבטי גרסאות ואבטחה ותקיפה בפרוטוקול ב Https או openslll (מספר משימות שונות לקבוצות שונות) כולל היבטי Downgrade

(4 כולל 3 משימות שונות ונפרדות ל 3 קבוצות שונות 4.1 4.2 4.3)

4.1 כתיבת כלי לבירור הגרסאות של https ואו openslll בשרת מרוחק, כולל אופציה לכלי סריקה של רשימת שרתים רחבהבובפרט חיפוש שרתים העונים לקריטריונים מסוימים.

תתיכן הרחבה לבדיקת תכונות וגרסת סרטיפיקאט.

מומלץ גם להרים סביבת בדיקה (שרת WEB עם https) ואו openssl .

רקע ומבוא: (יורחב רבות)

https://opensource.com/article/19/11/internet-security-tls-ssl-certificate-authority

Checking SSL / TLS Version Support of a Remote Host from the Command Line | Max Chadwick

https://maxchadwick.xyz/blog/checking-ssl-tls-version-support-of-remote-host-from-command-line

יש לסקור גרסאות וגרסות של ספריות openssl .

4.2 מטלה חילופית בהקשר זה: כלי לזיהוי של סוגי openssl או מימושי SSL בשרת המרוחק

חישבו על רעיונות נוספים כלי לזיהוי של סוגי openssl או מימושי SSL בשרת המרוחק ויכולת ה Fallback שלו (אפשר סידרת צעדים)
Checking SSL / TLS Version Support of a Remote Host from the Command Line | Max Chadwick
https://maxchadwick.xyz/blog/checking-ssl-tls-version-support-of-remote-host-from-command-line
Test TLS Connection Ciphers TLS Version and Certificate with OpenSSL Command Line (djangocas.dev)

/https://djangocas.dev/blog/test-tls-connectivity-with-openssl
כולל סקר אתרים מובילים קטן .... + הצגת סטטיסטיקות

https://serverfault.com/questions/638691/how-can-i-verify-if-tls-1-2-is-supported-on-a-remote-web-server-from-the-rhel-ce

4.3 מטלה חילופית נוספת בהקשר זה:

סקירת פגיעויות ב SSH ברמה פנים ארגונית וכתיבת כלי זיהוי או בדיקה/סריקה/תקיפה.

Four SSH Vulnerabilities You Should Not Ignore (cyberark.com) (רשימה חלקית ....)

https://www.cyberark.com/resources/blog/four-ssh-vulnerabilities-you-should-not-ignore

5) חקר נוזקה בלינוקס שממומשת בעזרת eBPF

BPFDoor: Tool almost undetected for FIVE years in 'thousands' of systems (thestack.technology)

https://thestack.technology/bpfdoor-chinese-tool-almost-undetected/

היכרות עם המנגון : eBPF - Introduction, Tutorials & Community Resources

https://ebpf.io/

כתיבה דוגמה ב eBFF (למשל לחיפוש מחרוזת מסוימת בתעבורה באופן מהיר) וחסימת כל פאקטת UDP שמכילה חתימה זו . (בנית מיני FireWall)

תיאור הנוזקה הסינית ומנגנוניה

חיפוש מאמרים על נוזקות וכלים דומים (גם כלי איתור דוגמת tracee של אורקה –סקיוריטי)

BSidesTLV 2022 | Hunting kernel rootkits with eBPF

https://bsidestlv.com/agenda/hunting_kernel_rootkits_with_ebpf/

6) סקירת כלים ל DPI ומתקפות ReDirect של תעבורה העוברת דרך נכס בשליטת התוקף

קראו מאמרים של סיטיזן לאב בנושא וכתבו סקירה תאורטית.

נסו לכתוב תוכנה המבצעת http Redirect לשרת web אחר
לתעבורה העוברת דרך ראוטר שבשליטתכם .,

(למשל רק לבקשות get מסוימות להורדת קובץ) בהנחת תעבורה לא מוצפנת.

אופצינאלי (לא בשלב ראשון out of scope) הרחבה: בהנחת קיום root Certificate שלכם בקלינט
ואפשרות לזייף סרטיפיקאטים: להרחיב גם לתעבורת https מוצפנת.

BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads? (citizenlab.ca)

https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

Citizen Lab on Twitter: "NEW REPORT: Bad Traffic: Deep Packet Inspection Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads? https://t.co/5Ui7AQnPOT packetlogic-devices-deploy-government-spyware-turkey-syria https://t.co/x5BYl6wEwZ" / Twitter

https://twitter.com/citizenlab/status/971975585063780352

https://www.securityweek.com/internet-provider-redirects-users-turkey-spyware-report

https://myce.wiki/news/turkish-isp-caught-redirecting-specific-users-spyware-infected-downloads-83922/

7) מנהל הורדות חכם בהתבסס על TOR (שני פרויקטים)

א.

מנהל הורדות חכם בהתבסס על TOR כולל מודעות לרוחב הפס מול יעד מסוים והשוואת רוחבי פס של מעגל למעגל אחר והחלטה על בחירה בין השניים (כולל הפרעה בין הורדה במסלול אחד להורדה במסלול שני עקב עומס ביעד)

ב.

סורק מעגלים של TOR אל יעד מסוים תוך שמירת שני מעגלים והשוואה מי נותן רוחב פס יותר גבוה והשהייה קטנה יותר ,כולל ניסיון מיפוי יציאות ומטריקות מול יעד מסויים שידוע רק ע"פ כתובותו

8) חקר (כולל כלי סריקה ובנית DB) של תכונות של סרטיפיקאטים ופגיעויותיהם.

מסיבות של רגישות יפורט לצוות הרלונטי.

9) מהן ההגנות ב SSH כנגד מחשבים קוונטים בעתיד ?

נושא שני: נושא מתקדם , אין מימוש אלא רק רקע תיאורטי , יכול לבוא כהשלמה לבונוס

OpenSSH Moves to Prevent 'Capture Now, Decrypt Later' Attacks | SecurityWeek.Com

https://www.securityweek.com/openssh-moves-prevent-capture-now-decrypt-later-attacks

Protection Against Side-Channel Attacks Added to OpenSSH | SecurityWeek.C
https://www.securityweek.com/protection-against-side-channel-attacks-added-opensshom

10) VLAN Hooping

נושא שני: נושא קליל , יכול לבוא כהשלמה לבונוס .

https://www.techtarget.com/searchsecurity/definition/VLAN-hopping

https://www.netme.co.il/portfolio/vlan-hopping-attack/

What is VLAN hopping