مطالعه‌ی ابزارهای برتر شنود شبکه و مقایسه کاربردی Wireshark و Cain and Abel

سارا سعادت[۱]، هایده باقری پور[۱]

[۱]دانشجوی دکتری رشته مهندسی فناوری اطلاعات، پردیس بین‌المللی ارس دانشگاه تهران
{ssaadat,bagheripou}@ut.ac.ir

چکیده

این مقاله مطالعه‌ای بر روی بهترین ابزارهای نفوذ شبکه می‌باشد که از بین آنها Wireshark و Cain and Abel انتخاب‌شده‌اند و اینکه چگونه می‌توان حفره‌های امنیتی و انجام حملاتی مانند شکستن رمز عبور، حمله مرد میانی، شنود ترافیک کاربران و غیره را با این ابزارها آشکار کرد. آزمایش‌ها برای شواهد عملی از طریق ایجاد آزمایشگاه مجازی انجام شده‌است. هدف از این مقاله برای نشان دادن این مهم بود که چگونه می‌توان با آشکار کردن حفره‌های امنیتی مختلف در سیستم مبتنی بر ویندوز، سیستم شخص را به‌راحتی هک کرد. نتایج نشان‌می‌دهد که در صورت کم‌توجهی، سوءاستفاده از یک سیستم یا کشف رمز عبور چقدر ساده است و به‌راحتی می‌توان به امنیت و ایمنی سیستم خدشه وارد کرد. از آنجایی که سیستم‌ها هرگز نمی‌توانند همیشه از حملات در امان باشند، بنابراین دانستن این تهدیدات و استفاده از مکانیسم‌های امنیتی مناسب به‌گونه‌ای که مورد سوء استفاده قرار نگیرد برای افراد مفید خواهد بود.

کلمات کلیدی: شنود شبکه، نفوذ به شبکه، هک، ابزارهای نفوذ، تهدیدات سایبری، حملات رمز عبور، Wireshark، Cain and Abel.

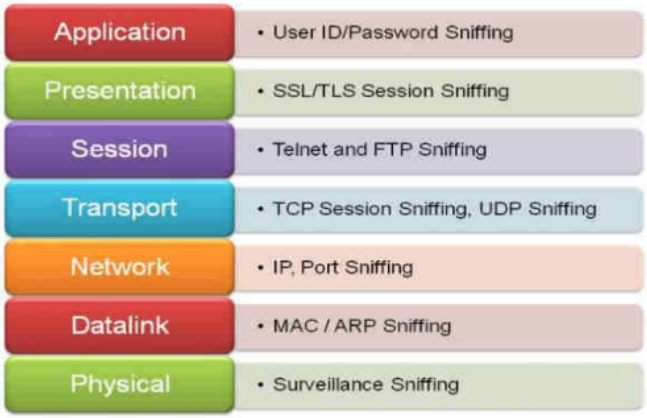
۱ مقدمه

یک شبکه، از مجموعه‌ای از گره‌ها مانند هاب‌ها، پل‌ها، سوئیچ‌ها، رهیاب‌ها[۱]، فایروال‌ها، شکل‌دهنده‌های بسته[۲] تشکیل شده است. هاب‌ها به اتصال دو دستگاه کمک می‌نمایند. پل‌ها و سوئیچ‌ها در لایه ۲ ISO-OSI (ارتباط بین سیستم‌های باز) عمل می‌کنند. رهیاب‌ها نقش تحویل بسته‌ها را از مبدأ به مقصد انجام می‌دهند. فایروال‌ها با فیلترکردن ترافیک بین فرستنده و گیرنده از شبکه‌ها محافظت می‌کنند. بستر شبکه به‌صورت

[1]Router

[۲]packet shapers: شکل‌دهی ترافیک که به شکل‌دهی بسته نیز معروف است، یک روش مدیریت ازدحام است که انتقال داده‌های شبکه را با به تاخیر انداختن جریان بسته‌های کمتر مهم یا کمتر دلخواه تنظیم می‌کند.

۷*۲۴ در حال استفاده است و در معرض انواع مختلفی از حملات مانند ARP[۳] و DDOS[۴] (انکار سرویس توزیع‌شده) است. ازاین‌رو نظارت بر عملکرد آن نقش حیاتی در حفظ شبکه ایفا می‌کند. ابزارهایی مانند Wireshark و Cain and Abel در این مقاله مورد تجزیه‌وتحلیل قرار می‌گیرند. ترافیک شبکه توسط Wireshark قابل‌ردیابی و تفسیر است و با ابزار Cain and Abel حملاتی مانند آشکارسازی رمز عبور و مسمومیت ARP را می‌توان تجزیه‌وتحلیل کرد. اقدامات پیشگیرانه بر اساس خروجی ابزارهای نظارتی مانند Wireshark و سایر ابزارهای نظارتی انجام می‌شود. شنود شبکه به‌صورت کلی شامل گرفتن، رمزگشایی، بازرسی و تفسیر اطلاعات داخل یک بسته شبکه باهدف سرقت اطلاعات است.



شکل ۱: شنود در لایه‌های مختلف OSI [۱]

معمولاً شناسه‌های کاربران، رمزهای عبور، جزئیات شبکه، اطلاعات کارت‌های اعتباری نمونه اطلاعات مهمی هستند که در شبکه مورد تبادل قرار می‌گیرند. شنود به‌طورکلی به‌عنوان یک نوع حمله «غیرفعال» نامیده می‌شود که در آن مهاجمان می‌توانند در شبکه به‌صورت مسکوت از اطلاعات مهم سوءاستفاده کنند [۱].

۲ ادبیات موضوعی

ابزارهای متعددی در حال حاضر به‌منظور شنود، اسکن و آنالیز شبکه مورداستفاده قرار می‌گیرند که در این مقاله نمونه‌هایی از آنها را قید کرده‌ایم [۲، ۳].

[۳] پروتکل ارتباطی«Address Resolution Protocol» یا به‌اختصار پروتکل ARP، برای یافتن آدرس MAC سیستم‌های شبکه است.

[۴] حملات DDoS یا حمله محروم‌سازی از سرویس، یکی از رایج‌ترین و قدرتمندترین حملات سایبری به شمار می‌رود که سرورها و سرویس‌های آنلاین را مورد هدف قرار می‌دهد.

جدول ۱: ویژگی‌های ابزارهای نفوذ به شبکه [۲]

SNO	TOOLS	FEATURES
1	ENDACE	Deep Packet Analyzer
2	Wireshark	Network Protocol Analyzer
3	Tcpdump [2]	Network Sniffer
4	Dsniff	Passive sniffs the network
5	Etherpeek	Protocol Analyzer
6	Sniffit [3]	Network Analyzer
7	Etherflood [4]	White hat hacking purpose
8	ETHERCAP	Packet sniffer
9	Insider	Network Scanner
10	Pof [5]	Identify the Operating system
11	NetworkMiner	Forensic Analyzer
12	Ettercap	Sniffs dynamic connections
13	KISMET	Passive sniffer
14	Cain and Abel	Cracking passwords
15	NetStumbler [6]	Active sniffer
16	Ntop	Determines network status
17	Ngrep	Packet sniffer
18	EtherApe [7]	Network traffic monitor
19	KisMAC	Network discovery tool
20	Aircrack-ng	Detection of network packets
21	SUITE	Creates encrypted packets

۳ بهترین ابزارهای شنود شبکه

۱.۳ Wireshark

Wireshark یک تحلیل‌گر بسته است و برای عیب‌یابی، تجزیه‌وتحلیل شبکه استفاده می‌شود. این پروژه که در ابتدا Ethereal نام داشت، در می 2006 به دلیل مشکلات مربوط به علامت تجاری به Wireshark تغییر نام داد. Wireshark یک رابط کاربری تعاملی است که از pcap برای ضبط بسته‌ها استفاده می‌نماید. بر روی سیستم‌های عامل مختلف نظیر unix و solaris و در مایکروسافت ویندوز اجرا می‌شود. ابزاری است که کاربران می‌توانند از منوی "Capture" آن برای ضبط تصاویر استفاده‌کننده. می‌تواند بسته‌ها را ضبط کرده و انتخاب‌های مختلفی را برای برآوردن تنظیمات و شرایط تحلیل‌گران ارائه دهد [۴].

Wireshark همچنین ویژگی‌های بسیاری را ارائه می‌دهد. از ethernet، IEEE 802.11، PPP و Loopback پشتیبانی می‌کند. Wireshark شامل یک رابط کاربری تعاملی و همچنین یک نسخه خط فرمان است. Wireshark داده‌های ترافیکی با کد رنگی را برای نشان‌دادن پروتکل مورداستفاده برای انتقال نمایش می‌دهد. این ابزار همچنین شامل گزینه‌های مختلف فیلتر است که داده‌های نمایش‌داده‌شده را محدود می‌کند. مهاجم می‌تواند از این ابزار در ترکیب با Cain and Abel برای انجام Session hijacking استفاده نماید [۵].

علاوه بر این Wireshark با ضبط و تحلیل بسته‌های داده‌ای که از طریق رابط شبکه عبور می‌کنند، عمل می‌نماید و به کاربر اجازه می‌دهد تا ترافیک را به طور زنده، ضبط یا فایل‌های پیگیری بسته‌های قبلی را تجزیه‌وتحلیل نماید. این نرم‌افزار از محدوده وسیعی از پروتکل‌ها از جمله HTTP، TCP، UDP، DNS، FTP و بسیاری دیگر پشتیبانی می‌کند و با قابلیت پشتیبانی از ترافیک رمزگذاری شده مانند SSL/TLS، Wireshark درک بهتری از ارتباطات امن را ارائه می‌دهد.

با تجزیه و تحلیل ترافیک شبکه، می‌توان از توانایی‌های Wireshark برای بهبود کارایی شبکه استفاده کرد. با شناسایی الگوها و روندهای ترافیک، متخصصان می‌توانند شبکه را بهینه‌سازی و عملکرد بهتری را فراهم نمایند.

Wireshark قادر به تجزیه‌وتحلیل بسته‌های VoIP (Voice over Internet Protocol) است. این ویژگی، امکان بررسی و مانیتورینگ ارتباطات تلفنی اینترنتی فراهم می‌سازد. همچنین Wireshark قادر به مشاهده پیام‌های DNS (Domain Name System) است. این قابلیت به شما اجازه می‌دهد تا درخواست‌های DNS مورد ارسال و دریافت را بررسی نمایید و به تجزیه‌وتحلیل مسائل احتمالی مرتبط با آن بپردازید.

برای شناسایی ترافیک شبکه، ابزار Wireshark باید بر روی سیستم شما نصب شود تا بسته‌ها را ضبط کند. در ابتدای اجرای برنامه باید کارت شبکه را انتخاب و سپس شروع به ضبط ترافیک کرد.

■ ویژگی‌های پیشرفته Wireshark

- تحلیل پروتکل:

Wireshark می‌تواند طیف وسیعی از پروتکل‌های شبکه، از جمله TCP/IP، UDP، ICMP، HTTP، FTP، DNS، و بسیاری دیگر را تشریح کند که این امکان را می‌دهد که جزئیات هر بسته، مانند آدرس IP مبدأ و مقصد، شماره port و داده‌های بارگذاری را مشاهده کنید.

- فیلتر کردن:

Wireshark این امکان را می‌دهد که بسته‌هایی که در پنجره اصلی نمایش داده می‌شوند را فیلتر کنید. این می‌تواند برای محدودکردن ترافیکی که به تجزیه‌وتحلیل آن علاقه دارید مفید باشد. به‌عنوان‌مثال، می‌توانید بر اساس آدرس IP، شماره port، پروتکل یا کلمه کلیدی فیلتر کنید.

- کدگذاری رنگ:

Wireshark از کدگذاری رنگی برای برجسته‌کردن انواع مختلف ترافیک استفاده می‌کند. این می‌تواند به شما کمک کند تا به‌سرعت انواع بسته‌های موردعلاقه خود را شناسایی کنید. به‌عنوان‌مثال، بسته‌های TCP معمولاً با رنگ سبز، بسته‌های UDP به رنگ آبی و بسته‌های ICMP به رنگ صورتی نمایش داده می‌شوند.

- اطلاعات تخصصی:

Wireshark اطلاعات تخصصی بسیاری از بسته‌هایی را که می‌گیرد ارائه می‌دهد. این اطلاعات می‌تواند به شما کمک کند تا معنای بسته را بفهمید و مشکلاتی را که ممکن است دارید عیب‌یابی کنید.

- آمار:

Wireshark می‌تواند آماری در مورد ترافیک شبکه‌ای که می‌گیرد جمع‌آوری کند. از این آمار می‌توان برای شناسایی روندها و الگوهای ترافیک استفاده کرد.

- گراف‌ها:

Wireshark می‌تواند نمودارهایی از ترافیک شبکه‌ای را که می‌گیرد ایجاد کند. از این نمودارها می‌توان برای تجسم ترافیک و شناسایی مشکلات احتمالی استفاده کرد.

علاوه بر این ویژگی‌های پیشرفته، Wireshark تعدادی ویژگی دیگر نیز دارد که می‌تواند برای عیب‌یابی مشکلات شبکه مفید باشد، مانند توانایی دنبال‌کردن جریان‌های TCP، واکاوی بسته‌های VoIP و تجزیه‌وتحلیل ترافیک شبکه بی‌سیم.

■ نمونه‌هایی از نحوه استفاده از ویژگی‌های پیشرفته Wireshark:

- برای عیب‌یابی اتصال کند شبکه:

می‌توانید از Wireshark برای ضبط ترافیک شبکه استفاده کنید و سپس آن را برای علائم تراکم، از دست‌دادن بسته‌ها یا سایر مشکلات تجزیه‌وتحلیل کنید.

- برای بررسی یک نقض امنیتی:

می‌توانید از Wireshark برای ضبط ترافیک شبکه و سپس تجزیه‌وتحلیل آن برای فعالیت‌های مخرب، مانند آلودگی‌های بدافزار یا تلاش‌های دسترسی غیرمجاز استفاده کنید.

- برای بهینه سازی عملکرد شبکه:

می‌توانید از Wireshark برای ضبط ترافیک شبکه و سپس تجزیه‌وتحلیل آن برای شناسایی تنگناها و سایر مناطقی که شبکه می‌تواند بهبود یابد استفاده کنید.

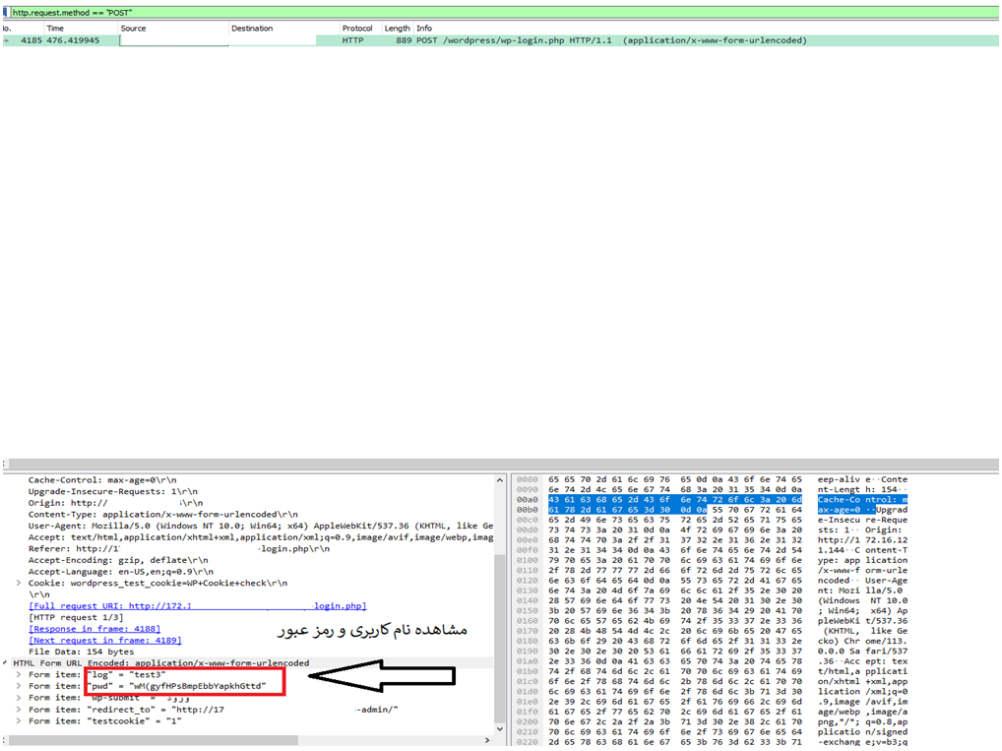
- برای توسعه پروتکل‌های شبکه جدید:

می‌توانید از Wireshark برای ضبط و تجزیه‌وتحلیل ترافیک ایجاد شده توسط پروتکل جدید خود استفاده کنید تا مطمئن شوید که مطابق انتظار کار می‌کند.

Wireshark یک ابزار قدرتمند است که می‌تواند برای اهداف مختلف استفاده شود. با یادگیری نحوه استفاده از ویژگی‌های پیشرفته آن، می‌توان درک عمیق‌تری از ترافیک شبکه به دست آورد و مشکلات شبکه را به طور مؤثرتری عیب‌یابی کرد.

۱.۱.۳ شنود شبکه با Wireshark

برای مشاهده رمز عبور در Wireshark، http را در فیلتر تایپ کرده و روی Apply کلیک کنید. این کار تمام بسته‌های http را فیلتر می‌کند. اگر روی فیلتر انجام شده روی پروتکل http، مجدد فیلتر متد post را اعمال کنید، در جزئیات ترافیک، نام کاربری و رمز عبور وارد شده برای آی پی مقصد به‌وضوح قابل‌مشاهده است. http.request.method == ”POST”



شکل ۲: مشاهده نام کاربری و رمز عبور از ترافیک ضبط شده

۲.۱.۳ جایگزین‌های Wireshark

ما ۷ جایگزین برای Wireshark فهرست کرده‌ایم که دارای ویژگی‌های مشابهی مانند Wireshark از جمله ساختاری، رایگان و منبع‌باز بودن هستند [۶، ۷].

جدول ۲: جایگزین‌های منبع باز Wireshark [۷]

ابزار	توضیحات ابزار
tcpdump	tcpdump از کتابخانه libpcap برای گرفتن بسته‌ها استفاده می‌کند.
Microsoft Network Monitor	Microsoft Network Monitor یک تحلیلگر بسته برای ضبط، مشاهده و تجزیه‌وتحلیل داده‌های شبکه و رمزگشایی پروتکل‌های شبکه که در حال حاضر توسعه آن متوقف شده است.
Intercepter-NG	Intercepter-NG یک ابزار شبکه چندمنظوره برای انواع مختلف بازیابی اطلاعات جالب از جریان شبکه و انجام انواع مختلف MiTM است.
apptalk.ninja	apptalk.ninja یک نرم‌افزار نظارت بر اپلیکیشن موبایل است.
netcat	Netcat (nc) یک ابزار شبکه کامپیوتری برای خواندن و نوشتن از طریق اتصالات شبکه با استفاده از TCP یا UDP است. Netcat به شکل یک پشتیبان قابل‌اعتماد طراحی شده است.
Ettercap	Ettercap یک مجموعه جامع برای حملات مرد میانی است.
Nethogs	Nethogs یک نرم‌افزار نظارت بر پهنای باند است.

https://appmus.com/alternatives-to/wireshark

۲.۳ Cain and Abel

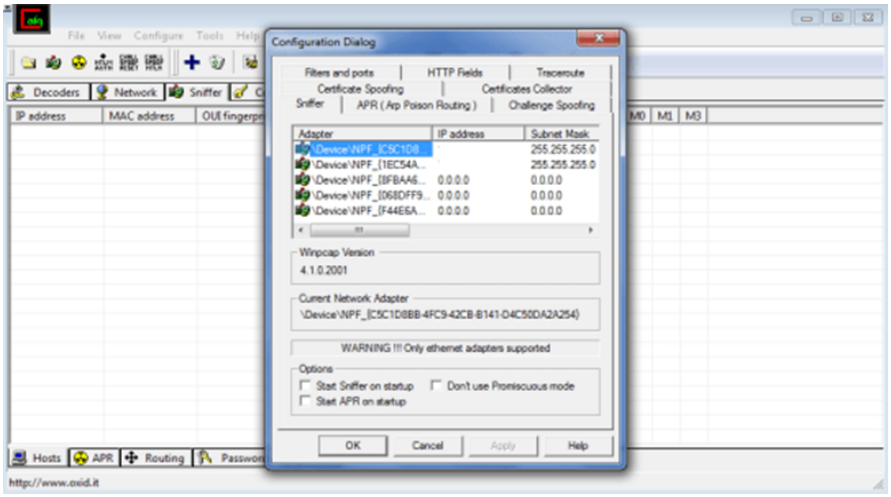
Cain and Abel یک ابزار بازیابی رمز عبور برای سیستم‌عامل‌های مایکروسافت است که اجازه بازیابی آسان با استراق سمع شبکه، آشکارسازی رمزهای عبور با استفاده از Dictionary، Brute-Force و حملات Cryptanalysis، ضبط مکالمات VoIP، رمزگشایی رمزهای عبور درهم، بازیابی کلیدهای شبکه بی‌سیم، کشف رمزهای عبور ذخیره شده و تجزیه‌وتحلیل پروتکل‌های مسیریابی را فراهم می‌کند. برنامه قابلیت exploit آسیب‌پذیری نرم‌افزاری را ندارد؛ ولی برخی از جنبه‌های امنیتی / ضعف موجود در پروتکل‌ها، استانداردها، روش‌های احراز هویت و حافظه پنهان را پوشش می‌دهد [۳، ۶، ۸]. همچنین می‌تواند پروتکل‌های رمزگذاری شده مانند SSH-1 و HTTPS را تجزیه‌وتحلیل کند و شامل فیلترهایی برای گرفتن اعتبار از سازوکارهای کنترلی مختلف است [۵].

۱.۲.۳ شنود شبکه با Cain and Abel

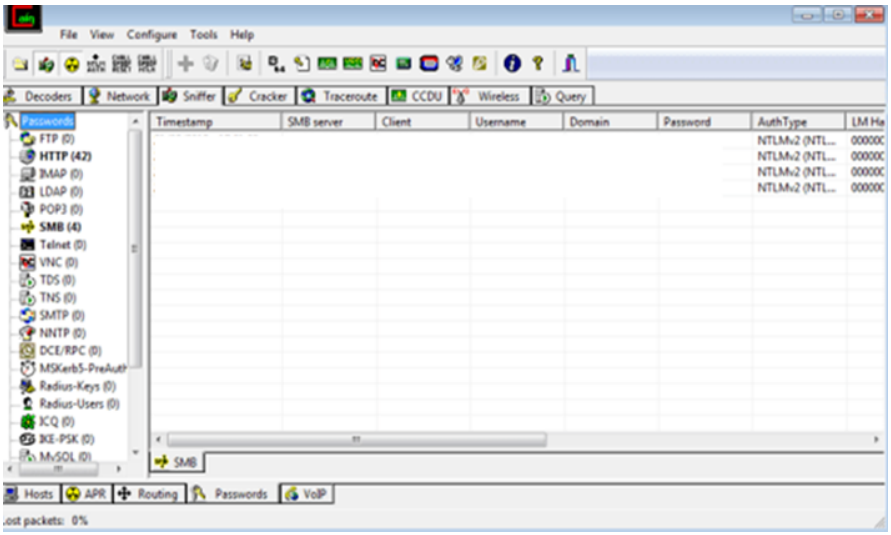
برای آشکارسازی پسوردهای رمزنگاری شده از حمله دیکشنری و brute-force معمولاً از این ابزار استفاده می‌شود و همچنین سایر حملاتی مانند DNS و ARP نیز از طریق آن قابل‌انجام است.

برای شنود رمزهای عبور در حال تبادل روی شبکه، ابتدا نرم‌افزار Cain and Abel را اجرا نموده، سپس در منوی بالایی نرم‌افزار گزینه Configure را انتخاب کرده و در مرحله بعد آداپتور شبکه مناسب را برای

شنود پسوردها به‌صورت متن ساده انتخاب می‌نماییم.



شکل ۳: نحوه تنظیمات در Cain and Abel



شکل ۴: آشکارسازی رمز عبور در Cain and Abel

۲.۲.۳ جایگزین‌های Cain and Abel

در جدول ۳، نه جایگزین برای ابزار Cain and Abel، معرفی شده است.

جدول ۳: جایگزین‌های منبع‌باز Cain and Abel

ابزار	توضیحات ابزار
Wireshark	Wireshark یک ابزار ردیابی شبکه منبع‌باز برای تجزیه‌وتحلیل ترافیک شبکه است.
Ophcrack	Ophcrack یک برنامه منبع‌باز رایگان (دارای مجوز GPL)[۵] است که رمزهای عبور ورود به سیستم ویندوز را با استفاده از هش‌های LM از طریق جداول رنگین‌کمان[۶] می‌شکند.
Reaver	reaver برای بازیابی رمزهای عبور WPA/WPA2 است و یک حمله brute force علیه پین‌های ثبت‌کننده الگوریتم محافظت شده Wifi (WPS) اجرا می‌کند.
Ettercap	Ettercap یک مجموعه جامع برای حملات مرد میانی است.
Kon-Boot (تجاری)	Kon-Boot برنامه‌ای است که فرایند احراز هویت سیستم‌عامل‌های مبتنی بر ویندوز را دور می‌زند.
Aircrack-ng	Aircrack-ng یک مجموعه نرم‌افزار شبکه است که از آشکارساز، ردیاب بسته، رمزگشای WEP و WPA/WPA2-PSK و ابزار تجزیه‌وتحلیل برای شبکه‌های محلی بی‌سیم 802.11 تشکیل شده است.
Offline NT Password and Registry Editor	chntpw یک ابزار نرم‌افزاری برای بازنشانی یا خالی‌کردن رمزهای عبور محلی است که توسط Windows NT، 2000، XP، Vista، 7، 8 و 8.1 استفاده می‌شود.
John the Ripper	John the Ripper یک ابزار نرم‌افزاری رایگان برای شکستن رمز عبور است.
Intercepter-NG	Intercepter-NG یک ابزار شبکه چندمنظوره برای انواع مختلف حملات مرد میانی یا MiTM است.

https://appmus.com/alternatives-to/cain-and-abel

۴ مقایسه کاربردی Wireshark و Cain and Abel

در جدول ۴ مقایسه کاربردی Wireshark و Cain and Abel ارائه شده است.

[۵] GPL یا General Public License که گاهی به آن GNU GPL نیز گفته می‌شود، رایج‌ترین مجوز نرم‌افزار رایگان است. این کار توسط ریچارد استالمن از بنیاد نرم‌افزار آزاد برای پروژه گنو نوشته شده است. این مجوز اجازه می‌دهد تا نرم‌افزار آزادانه مورداستفاده، اصلاح و توزیع مجدد قرار گیرد.

[۶] rainbow tables: جدول رنگین‌کمان یک جدول از پیش محاسبه شده برای ذخیره خروجی‌های یک تابع هش رمزنگاری است که معمولاً برای شکستن هش رمز عبور است.

جدول ۴: مقایسه کاربردی Wireshark و Cain and Abel

ویژگی‌ها	Wireshark	Cain and Abel
تولیدکننده	تیم Wireshark	توسط Massimiliano montro
رابط میانی	GUI and CLI	GUI
لایسنس نرم‌افزار	Freeware	GNU
سیستم‌عامل	لینوکس و ویندوز	فقط پلتفرم ویندوز
ویژگی اصلی	ابزار عالی آنالیز شبکه	
آسیب‌پذیری نرم‌افزار	قابلیت exploit آنها را دارد.	قابلیت exploit آنها را ندارد.
TCP/IP Stream	قابلیت بازیابی آن را دارد.	قابلیت بازیابی آن را ندارد.
تحلیل ترافیک	آنالیز جزئی ترافیک شبکه	قابلیت آنالیز جزئی را ندارد و صرفاً تعداد پکت‌های اخذ شده یا شنود شده را نشان می‌دهد.
پشتیبانی پروتکل‌های شبکه	طیف گسترده	محدود
سهولت کاربری	متوسط	آسان
پشتیبانی سیستم‌عامل اندروید	دارد	دارد
تحلیل جزئیات اطلاعات بسته	دارد	دارد
نظارت بر عملکرد شبکه	دارد	دارد
مشاهده فعالیت‌های در لحظه شبکه	دارد	ندارد
نظارت بر عملکرد برنامه‌های کاربردی	دارد	ندارد
نظارت بر عملکرد CPU و RAM	دارد	ندارد
نظارت بر عملکرد پروتکل HTTP	دارد	ندارد
دورزدن، بازیابی و شکستن رمز عبور	ندارد	دارد

۵ محدودیت‌ها و معایب Wireshark و Cain and Abel

۱.۵ معایب Wireshark

هرچند Wireshark یک ابزار قدرتمند است، اما استفاده از آن نیازمند دانش و تجربه است. همچنین تحلیل ترافیک شبکه ممکن است پیچیده و زمان‌بر باشد و نیازمند تخصص و آگاهی در زمینه پروتکل‌ها و مفاهیم شبکه است.

همچنین باید به محدودیت‌ها در استفاده از Wireshark توجه داشت. به‌عنوان یک ابزار بررسی ترافیک، Wireshark نمی‌تواند به طور کامل اطلاعات رمزنگاری شده را نمایش دهد و نیازمند دسترسی به کلیدها و رمزهای مربوطه است.

۲.۵ معایب Cain and Abel

- Cain and Abel می‌تواند موجب کندی ارتباطات شود. این امر به طور بالقوه می‌تواند حمله را آشکار

کند و کاربر را مشکوک نماید. در آزمایش‌ها، حدود ۳۰ درصد تفاوت بین یک اتصال معمولی و یک اتصال مسموم ARP پیدا کردیم، اما نتایج ممکن است برای سایرین متفاوت باشد. سرعت اضافه شده به دلیل گره اضافی است که بسته‌ها باید از آن عبور نمایند.

- به طور پیش‌فرض نمی‌تواند رمزهای عبور بسیاری از وبگاه‌ها را شناسایی کند. مگر اینکه وبگاهی از یک فیلد رمز عبور مانند "pass" یا "pw" استفاده کند، Cain و Abel آن را با پیکربندی پیش‌فرض تشخیص نخواهند داد. برای اجرا به دسترسی سطح مدیر نیاز دارد. این ابزار با برخی از ابزارهای کرک مانند Ophcrack که برای کرک کردن هش‌ها به هیچ حساب کاربری نیاز ندارند، تفاوت دارد.
- جعل ARP نیاز به دسترسی به شبکه دارد. هیچ کاری با ARP انجام نمی‌شود مگر اینکه کاربر به‌درستی به شبکه متصل باشد [۱۰].

۶ نتیجه‌گیری

ابزارهای متعددی برای شنود و آنالیز ترافیک شبکه مورداستفاده قرار می‌گیرند که ازاین‌بین دو نمونه از بهترین ابزارها مورد بررسی و مقایسه قرار گرفتند. ترافیک شنود شده در آزمایشگاه مورد تحلیل قرار گرفت و نتایج آن ارائه گردید.

- Wireshark ابزار بهتر برای آنالیز شبکه و رصد ترافیک شبکه برای مدیران
- Cain and Abel ابزار ساده‌تر برای آشکارسازی رمز عبور ها

Wireshark به‌عنوان یک تحلیل‌گر پروتکل شبکه منبع‌باز قدرتمند، در ضبط بسته‌های بلادرنگ، تجزیه‌وتحلیل عمیق پروتکل و طیف گسترده‌ای از پلتفرم‌های پشتیبانی شده خود برجسته است. پشتیبانی گسترده، مستندات جامع و رابط کاربرپسند، آن را به انتخابی ارجح برای مدیران شبکه و متخصصان امنیتی که به دنبال بینش دقیق شبکه هستند، تبدیل کرده است. به نظر می‌رسد برای آنالیز ترافیک شبکه ابزار Wireshark مناسب‌تر و جامع‌تر باشد درعین‌حال برای شنود رمز عبور که یکی مهم‌ترین علاقه‌مندی هکرها است، Cain and Abel ابزار مناسبی است. اگر به دنبال یک تحلیلگر بسته ساده و با کاربری آسان هستید، Cain and Abel انتخاب خوبی است. همچنین اگر بتوانید رمزهای عبور را بشکنید یا رمزهای عبور ذخیره شده را از مرورگرها بازیابی کنید، انتخاب خوبی است.

بااین‌حال، مهم است که توجه داشته باشید که Cain and Abel به‌اندازه Wireshark به طور فعال توسعه‌نیافته است و ممکن است از آخرین پروتکل‌های شبکه پشتیبانی نکند.

در کارهای آتی به مطالعه سایر ابزارها و ارائه شواهد شبکه‌ای آنالیز و نفوذ به شبکه در دست اقدام توسط این تیم است.

سپاس‌گزاری

از زحمات جناب آقای دکتر آراسته راد، استاد راهنمای گرامی و سرپرست محترم پژوهشگاه کمال قدردانی را داریم.

مراجع

[1] V. Singh، M. Kumar and L. Raj، "Efficient Method for Preventing Password Sniffing Using MD5 Algorithm"، International Journal of Advanced Engineering Research and Science (IJAERS)، Vol-3، Issue-3، March- 2016، ISSN: 2349-6495.

[2] M. Fathima K M and N. Santhiyakumari، "A Survey On Network Packet Inspection And ARP Poisoning Using Wireshark And Ettercap"، Proceedings of the International Conference on Artificial Intelligence and Smart Systems (ICAIS-2021)، IEEE Xplore Part Number: CFP21OAB-ART; ISBN: 978-1-7281-9537-7

[3] A. Avritzer, R. G. Cole and E. J. Weyuker، "Monitoring for Security Intrusion using Performance Signatures"، WOSP/SIPEW'10، January 28–30، 2010، San Jose، California، USA. Copyright 2010 ACM 978-1-60558-563-5/10/01

[4] S. Dilip Sarve, S. Mahadik, "Comparative Study on Packet Sniffing Tools", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 2, Issue 1, July 2022, Copyright to IJARSCT DOI:10.48175/IJARSCT-5697403

[5] Z. Balogh, S. Koprda and J. Francisti, "LAN security analysis and design", IEEE 12th International Conference on Application of Information and Communication Technologies, October 2018 DOI:10.1109/ICAICT.2018.8746912

[6] N. Kaur and J. Singh، "ETHICAL HACKING IN WINDOWS ENVIRONMENT"، IJESRT INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES and RESEARCH TECHNOLOGY، ISSN: 2277-9655، DOI: 10.5281/zenodo.46485، February 2016.

[7] https://appmus.com/vs/wireshark-vs-cain-and-abel

[8] http://www.wireshark.org/

[9] http://www.oxid.it/cain.html

[10] http://www.cs.toronto.edu/~arnold/427/15s/csc427/tools/CainAndAbel/index.html