حمله لغت نامه ای[1] در ورد پرس:

تحلیل امنیتی و جرم یابی قانونی

چکیده

تحقیق جرم‌یابی قانونی موثر یک حمله امنیتی به یک نرم افزار کاربردی تحت وب به سهولت جرم‌یابی حقوقی سیستم نرم‌افزار تحت وب، ابزار جرم‌یابی حقوقی پشتیبان و مهارت‌های مامور تحقیق جرم‌یابی وابسته است. آمادگی نرم افزار کاربردی جرم یابی قانونی مجموعه شواهد رابا لاگینگ قادر کننده و حفاظت از شواهد برای آن دسته از فایلهای لاگی که از طریق روشهایی مانند تنظیمات دسترسی به منظور حفظ یکپارچگی است، ترکیب می کند. هم چنین، مامور تحقیق جرم شناسی بایستی درک خوبی از کارکرد نرم افزار تحت وب، معماری سامانه وب و مسائل امنیتی نرم افزار تحت وب داشته باشد.

این مقاله در مورد حمله لغت نامه ای در برابر ورد پرس (نرم افزار تحت وب) که توسط شخصی به نام پیتر کوییل (Peter Quill) که یک شخصیت ساختگی است، پژوهش می کند. حمله لغت‌نامه ای می‌تواند پسورد 7 کاراکتری استفاده شده در حساب کاربری اشخاص را با موفقیت حدس بزند. مجموعه‌ای از روش‌ها و ابزار به‌طور اساسی بررسی شدند تا مشخص شود که آیا این روش‌ها بنا به شرایط این پژوهش قابل اجرا هستند یا نه. روش‌ها اغلب شامل بازگرداندن فایل‌های ورودی از وب، سرویس دهنده نرم افزار کاربردی، سرور پایگاه داده و خود سرویس دهنده نرم افزار کاربردی است. در حالی‌که، ابزارها با جمع آوری، تحلیل و ارائه فایل داده ورودی سرو کار دارند.

[1] حمله لغت‌نامه‌ای، در تحلیل رمز و امنیت شبکه‌های رایانه‌ای، روشی برای شکستن یک رمز و یا مکانیزمی برای احراز هویت است، این حمله با تلاش برای تشخیص کلید رمز گشایی یک متن یا رمز عبور به وسیله جستجوی همه احتمالات ممکن در یک لغت‌نامه صورت می‌گیرد.

کلمات کلیدی: جرم شناسی وب، حمله لغت نامه ای، ورد پرس.

1. مقدمه

حمله‌های شکستن (کرکینگ) رمز عبور می‌تواند از طریق روش‌های مختلفی مانند حمله‌های لغت‌نامه ای، حمله‌های جستجوی فراگیر و جدول رنگین‌کمانی انجام شود. همه آنها عموما اشکالی از حمله‌های حدس رمز عبور هستند که در آن مرتکب جرم تلاش می‌کند تا با استفاده از مجموعه ای از کلمات استخراج شده از اطلاعات شخصی کاربر یا مجموعه لغت نامه های موجود استفاده شده مانند Jhone the Ripper و Cain و Abel [16] در نرم افزار کرکینگ[۲] رمز عبور در سیستم نفوذ نماید. یکی از مهم‌ترین عوامل شرکت کننده درکارآیی این نرم‌افزارها استفاده رمز عبوری ضعیف در حساب‌های کاربری آن‌لاین کاربرهاست. تحلیلی[15] که در یونان برای ارزیابی قدرت رمز عبورها اجرا شد، نشان می‌دهد طول میانگین کاراکتر استفاده شده فقط 7 تا است که در مقایسه با پسوردهای 16 کاراکتری توصیه شده نسبتا ضعیف عمل می‌کنند. بنابراین، هنوز حالت‌های مختلفی از سرقت اعتبارنامه ورودی وجود دارد و این روش‌ها در حال رشد هستند[2].

تحقیق جرم شناسی یک در تعیین شواهد فعالیت‌های غیرمجاز و مجرمانه یک فرایند بسیار مهم است[13]. در حوزه نرم‌افزارهای تحت وب، بسته به چارچوب نرم افزارهای کاربردی (وب)، پلت‌فرم[۳]، پایگاه داده و وب سرور، راه‌های متعددی می‌تواند برای تحقیق جرم‌شناسی می تواند وجود داشته باشد. این تحقیق به جرم شناسی نرم افزارهای تحت وب برای نمونه حمله‌های کرکینگ پسورد که وردپرس را هدف قرار می‌دهند، می‌پردازد. ابزارها و روش‌های جرم شناسی موجود استخراج شده از منابع همراه با قابلیت بکارگیری آنها در پژوهش مورد مطالعه به‌طور اساسی تحلیل شده اند. به‌علاوه این تحقیق، اطلاعاتی درمورد چگونگی بکارگیری نرم افزار جرم شناسی آماده بکار در ورد پرس و چگونگی اجرای تحقیق روی حمله‌های برنامه‌های تحت وب را نشان می‌دهد.

[2] هکر با استفاده از ابزارهای مخصوص در تلاش برای یافتن مقدار اولیه یک عبارت رمزگذاری شده و یا پیدا کردن یک مقدار حساس مثلاً رمز عبوری است که حتی عبارت رمزگذاری شده آن را هم در دست ندارد.

[3] پلتفرم در واقع بستری است که برنامه های نرم افزاری نوشته شده برای یک وسیله در آن قابل اجرا و استفاده است.

مقاله به شکل زیر تعریف شده است، بخش اول مروری برمنابع موجود دارد تا زمینه‌ای برای مفاهیمی همچون انواع حمله‌ها، رده بندی آنها و نیازها برای جرم شناسی برنامه‌های تحت وب، فراهم کند. بخش دوم به تفصیل تنظیمات آزمایشی و نتایج را بیان می‌کند. بخش بعدی روش‌هایی که می‌توانند برای تحقیقات جرم شناسی مربوط به آزمایش استفاده شوند و از چند عمل متقابل که برای کم کردن اثر حمله‌های اجرا شده در پژوهش، نتیجه شده‌اند را مورد بررسی قرار می‌دهد. سپس بخش بحث و بررسی است که به دنبال آن بخش نتایج مطرح می شود.

2. سوابق و کارهای مربوطه.

A. کلمه عبور کاربر.

عاملی که در کارآیی حمله های کرکینگ رمز عبور آنلاین مشارکت دارد، رمز عبورهای انتخابی کاربران است که به آسانی قابل پیشگویی هستند. تحلیل انجام شده [15] که روی 19000 رمز عبور واقعی بدست آمده از پایگاه‌های داده مختلف بطور کلی نشان می‌دهد که مشخصه اصلی پسوردهای انتخابی چنین پسوردهایی، طول میانگین برابر یا کمتر از 7 کاراکتر بوده و اغلب از کاراکترهای حرفی-عددی استفاده شده است. استفاده از یک پسورد تکراری در سایت‌های مختلف می تواند وسیله نفوذ کسانی باشد که مرتکب جرم پیشگویی رمز عبورها می‌شوند [1]. یک نظر سنجی نشان می‌دهد که 43-51 درصد کاربران پسورد یکسانی را برای حساب‌های کاربر خود در سایت‌های مختلف انتخاب می‌کنند. بنابراین ضروری است که کاربران پسوردهای مختلفی را برای هر حساب کاربری در وب سایت‌های مختلف انتخاب نمایند.

مطالعات دیگر بر اهمیت بالا بردن قدرت رمز عبور تاکید می‌کند که منجر به رمز عبوری بسیار پیچیده برای مهاجمان شکننده رمز عبورها می شود. رمز عبور از نوع گرامر مستقل از متن (CFG) حداقل 8 کاراکتر دارد و نمونه‌هایی از آن عبارتند از "123fatherabc"، "hyhycyhyh" و "[a*b]-[a-b]". همچنین، هنوز یک پژوهش واقعی برای سنجش قدرت رمز عبورهای (CFG) انجام نشده است. مشابه با داشتن رمز عبوری که بتوان آن را آسان به خاطر آورد، [3] روشی را پیشنهاد می‌شود که پسوردها برای بسیاری از حساب‌های کاربری که از تابع درهم

تقویت شده مخفی (cryptographic) استفاده می کنند، محاسبه می‌شود. قدرت این روش به این است که کاربر تنها بایستی یک رمز عبور ساده را از طریق افزونه مرورگر به خاطر آورد. این افزونه پسورد اصلی را پذیرفته و درهم‌سازی تکراری را برای ورودی پسورد واقعی اعمال می‌کند. همچنین توسط [5] که شبیه سازی را که از قانون هفت رمز عبور استفاده کرده و می تواند توسط مجری به سیستم اعمال شوند، بر قدرت رمز عبور تاکید می شود. آزمایشی برای تحلیل کرکینگ اجرا شده است که از الگوریتم Weir برای 12000 رمز عبور که روش‌های مختلفی برای رمز عبور بندی اعمال شده است، استفاده می‌کند. نتایج بدست آمده تصدیق نمود که 16 راه‌کار پایه، که پسوردهایی با حداقل ترکیبی از 16 کاراکتر است، ارجح‌ترین حالت است. سیاست‌های رمز عبور برای انتخاب رمز عبور، در بسیاری از وب‌سایتهای مشهور شامل دسته بندی‌های اجتماعی، وب‌لاگ، ایمیل، خرید و مالی بر یک مبنا قرار گرفته است. شباهت‌هایی بین وب‌سایت‌های اجتماعی، وب‌لاگ و ایمیل وجود دارد که در آن حداقل 6 تا 8 کاراکتر در سیاست رمز عبور اعمال می‌شود.

روشی دیگر برای ساختن پسورد استفاده از رمز عبورهای یادیار است[6]. یک نظر سنجی شروع به تولید رمز عبورهای یادیار توسط کاربرها نمود و سپس این رمز عبورها با رمز عبورهای کنترلی مقایسه شدند. یک نمونه از رمز عبور یادیار عبارت است از ”SWMtM$$!!“ است که مبتنی بر عبارت ”Show Me the Money!“ است که برگرفته از فیلم Jerry Maguirre است در حالی‌که یک رمز عبور کنترلی ”atreyu09“ است از شخصیت آتری یو فیلم ”Atreyu of the Never Ending Story II“ است. نتایج نشان می‌دهد 11 درصد از کلمات عبور کنترلی در مقایسه با تنها 4٪ از 144 رمز عبور حفظی شکسته شده اند. بنابراین پشنهاد می‌شود از ساخت رمز عبورهای حفظی در اینترنت اجتناب کنید زیرا عبارت‌های شناخته شده تری هستند.

B. به‌دست آوردن کلمات عبور.

روش‌های غیرقانونی زیادی مانند وب سایت های به دست آوردن رمز عبور عبور با طعمه fishing[4] و حملات آنلاین کرکینگ رمز عبور عبور، برای به دست آوردن کلمات عبور وجود دارد. تحقیقات قبلی [12] اشاره می‌کند رمز عبورهای عبور می توانند توسط مدیر رمز عبور جستجو و در یک مرورگر جمع‌آوری شوند. مثالی از این دست عبارت از هدایت شدن کاربر به یک سایت جعلی ورود کاربری بعد از وصل شدن به یک روتر وای‌فای (شبکه بی‌سیم) غیرمجاز، می باشد. صفحه غیر مجاز عین صفحه اصلی ورود پیکر بندی شده است بنابراین مدیر رمز عبور در دستگاه به صورت خودکار نام عبور و رمز عبور کاربری را در فیلدهای مربوطه را پر می‌کند.

به عبارت دیگر حملات احراز هویت توسط مرتکبین جرم، بسته به اطلاعاتی که از آنها در دست است به چهار دسته تقسیم می‌شوند[3]:

1. مهاجمان با نام کاربری دزدیده شده.
2. مهاجمان با نام کاربری و رمز عبور عبور دزدیده شده.
3. مهماجمان با پول دزدیده شده کاربران توسط ماشینی که امنیت آن در معرض خطر است.
4. مهاجمانی با پول و رمز عبور وب سایت دزدیده شده.

این مقاله روی نوع اول تحقیق می‌کند که نیاز است تا در آن رمز عبور از طریق روش‌های مختلفی حدس زده شود. همچنین مهاجمان می‌توانند رمز عبور عبور را به 4 طریق کشف کنند.

1. جمع‌اوری اطلاعات لازم و کافی در مورد کاربران که می‌تواند به کشف رمز عبور عبور آنها کمک کند.
2. بوسیله اجرای مهندسی اجتماعی و ترغیب کاربرها به آشکارسازی نام کاربری و رمز عبور عبور.
3. سرقت رمز عبور کاربری توسط شولدر سرفینگ (نگاه کردن پسورد به هنگام تایپ از روی دست اشخاص) و نرم افزار جاسوسی.
4. استفاده از ابزار کرک کردن رمز عبور.

[4] Password Harvesting Fishing: به دست آوردن کلمه عبور با طعمه

در یکی از نشریات، حملات کرکینگ آنلاین رمز عبور می تواند به دو دسته حمله فراگیر[5] و حمله لغت نامه ای طبقه بندی شود [16]. بعلاوه، [5] عواملی که کارآیی حدس رمز عبور را تحت تاثیر قرار می‌دهند، مانند مقاومت رمز عبور در برابر حدس زده شدن و نحوه عملکرد حملات حدس رمز عبور، را شماره گذاری می‌کند.

C.حملات بروت فورس(Brute Force).

این حمله تمامی ترکیبات ممکن تولید شده توسط کاراکترها را استفاده می‌کند [16-14]. بعنوان مثال یک حمله بروت فورس با 6 کاراکتر الفبایی از aaaaaa شروع کرده سپس آن را به aaaaab توسعه می دهد سپس aaaaac، aaaaad و تا zzzzzz ادامه می‌دهد. این افزایش ها و توسعه ها بسته به شکل حملات مهاجم تغییر می‌کند. همچنین مجموعه ای از کارکترها می‌توانند برای حمله بروت فورس مورد استفاده قرار گیرند مانند عددی، حروف کوچک، حروف کوچک با عدد و ترکیب الفبا. در برخی موارد این حمله بسیار موثرتر است زیرا حمله لغت نامه‌ای لیستی از کلماتی که تنها شامل بخشی از کل کلمات هستند را در بر می‌گیرد[16].

D. حملات لغت نامه ای.

در اجرای یک حمله لغت نامه ای، مرتکب شونده جرم، با مراجعه به لغت نامه لیستی از کلمات را که انتظار می رود رمز عبور هدف باشند را استفاده می‌کند. برخی قوانین می‌توانند به کلمات ورودی اعمال شوند، مانند شرع کلمه با حرف بزرگ، پیشوندهای عددی، جایگزینی کاراکتر a با @. کارآیی حمله‌های لغت نامه ای وابسته به کلمات محدودی است که رمز عبور شامل آن است و قوانینی که برای ساخت آن ترکیب و استفاده شده است. یک دیکشنری وسیع می تواند شانس پیشگویی رمز عبور هدف بالاتری را داشته باشد اما به زمان بیشتری را برای پردازش نیاز دارد.

[5].brute force

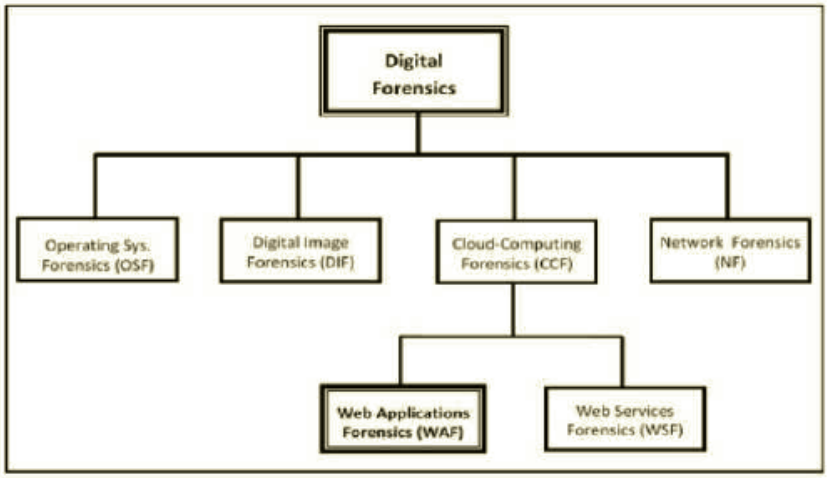
E. جرم‌یابی قانونی دیجیتال.

هدف جرم‌یابی کامپیوتری استفاده از ابزار و روش‌های متعدد برای جمع آوری شواهد از کامپیوترهایی است که با جرم در ارتباط هستند. عمردیجیتالی شدن افزایش یافته و جرم‌های سایبری که انجام می‌شوند صرفا محدود به کامپیوترها نیستند، بلکه در تمام وسایل الکتریکی به پدیده‌ای فراگیر تبدیل شده اند. مدل پیشنهادی[9] برای جرم‌یابی دیجیتال شامل 9 مولفه است، شناسایی با ذکر نام، آماده سازی، استراتژی دستیابی، محافظت، جمع آوری، سنجش، تحلیل، ارائه و بازگرداندن شواهد. این مدل یک ساختار استاندارد برای توسعه جرم‌یابی است که همچنین می تواند توسط ماموران قضایی برای ارتباط دادن اشخاص غیرفنی با تکنولوزی استفاده شود. همچنین، مولفان اظهار می‌کنند که این مدل بسیار جامع بوده و هیچ راه ساده‌ای برای سنجش کارآیی روش آنها نیست.

F. رده بندی جرم‌یابی قانونی رایانه‌ای.

حملات حدس رمز عبور عبور در وب‌سایت‌ها با استفاده از جرم‌یابی قانونی برنامه های کاربردی تحت وب (WAF)، می تواند ردیابی شود. این روش روی ردیابی معکوس و بازگشت به ریشه ارتکاب جرم که از اثر انگشت به‌جا مانده از مهاجم متمرکز است. جرم‌یابی قانونی برنامه‌های کاربردی تحت وب، وابسته به ماهیت مورد از طریق هر دو سمت-سرور و سمت-کاربر اجرا شود. بعلاوه، این روش بسیار متکی به فایل‌های ورورد به‌دست آمده از منابع مختلف نظیر مرورگرهای وب، وب سرورها و پایگاه داده هستند[7]. جرم یابی قانونی برنامه‌های کاربردی تحت وب با دیگر زمینه های تحقیقات جرم‌یابی همان‌گونه که در شکل (1) نشان داده است، ارتباط دارند. بعنوان یک مثال، جرم‌یابی قانونی سرورهای تحت وب (WSF) می‌توانند همگام با جرم‌یابی قانونی شبکه کارکند، زیرا سطح تجهیزات ورودی شبکه می تواند مانند روترهای پروتکل اینترنت (IP)، سیستم تشخیص نفوذ و دیوارهای آتش (Firewalls) مورد سنجش قرار گیرد. رده‌بندی ارائه شده [7] که در آن جرم‌یابی قانونی برنامه‌های کاربردی تحت وب (WAF) و جرم‌یابی قانونی سرویس‌های تحت وب (WSF) می‌توانند تحت عنوان، جرم‌یابی قانونی رایانش ابری (CCF) طبقه بندی

شوند. علاوه بر آن، سیستم‌های عملیاتی جرم‌یابی قانونی، جرم‌یابی قانونی عکس دیجیتالی، جرم‌یابی قانونی رایانش ابری، جرم‌یابی قانونی شبکه در زیر دسته جرم‌یابی قانونی دیجیتالی قرار می‌گیرند.



شکل (1): دسته بندی جرم‌یابی قانونی دیجیتال[7].

به عبارت دیگر، جرم‌یابی قانونی تحت سرویس وب متفاوت از جرم‌یابی قانونی نرم‌افزارهای کاربردی تحت وب است زیرا بیشتر روی حملات امنیتی در سرویس‌های وب توجه دارد.

G. جرم‌یابی قانونی نرم‌افزارهای کاربردی تحت وب.

هدف اصلی جرم‌یابی قانونی نرم‌افزارهای کاربردی تحت وب ردگیری حمله امنیتی در یک نرم‌افزار کاربردی تحت وب است که به مرتکب شونده‌ای که جرم سایبری را انجام داده است، بازمی‌گردد [7]. اگرچه، نکته مهمی که بایستی مورد توجه قرار گیرد این است که شانس بالاتری وجود دارد که سیستم در معرض خطر بایستی آماده باقی مانده و روشن بمانند، زیرا یک وب سایت پویا (زنده) باکاربرانی فعال است که مدام به سیستم دسترسی دارند. اگرچه، این امر وابسته به ماهیت کسب و کار و نمونه‌ای است که تصمیم می‌گیرد، آیا زمانی برای تعطیلی سیستم برای تحقیق در مورد آن تصمیم‌گیری لازم است یا نه[17].

به‌علاوه، یک سیستم برنامه‌های کاربردی تحت وب متداول شامل چهار مولفه است که عبارتند از وب سرور، سرور برنامه‌های کاربردی، سرور پایگاه داده و خود برنامه کاربردی تحت وب. سرور وب درخواست‌ها را پردازش کرده و از

طریق HTTP صفحات وب را در در مرورگر کاربر ذخیره می‌کند، در حال‌که سرور برنامه‌های کاربردی تحت وب جایی است که برنامه‌های کاربردی تحت وب وجود داشته و توابع صفحات وبی که با کسب و کار منطقی مرتبط است را پردازش می‌کند و همچنین برای خاندن و نوشتن اطلاعات، به سرور پایگاه داده دسترسی دارد. این چهار مولفه می توانند به چهار سرور فیزیکی جداگانه ایزوله شوند، و یا می توانند با هم در یک ماشین به شکل موازی قرار گیرند [17].

H. نیازمندی‌ها.

با توجه به [7]، یک سیستم برنامه‌های کاربردی تحت وب با داشتن قابلیت جمع‌آوری و حفاظت از شواهد آماده جرم‌یابی قانونی شوند. برای جمع‌آوری شواهد، وروردی ها بایستی فعال شده و بصورت مناسبی در سرورهای پیکربندی شوند. حفاظت از شواهد نیازمند این است که یکپارچگی ورودی‌ها بایستی با تنظیم دستورات مناسب روی فایل‌های ورودی حفظ شوند و خارج از دسترسی مرتکبین جرم نگه‌داری شوند. یک جرم‌یاب قانونی به مهارت‌های لازم برای انجام این جرم‌یابی مجهز باشد. درک کامل و کافی‌از معماری برنامه‌های کاربردی تحت وب، جریان برنامه، توابع و مولفه‌های سرور نیز برای جرم‌یاب قانونی اهمیت دارد. تنوع برنامه‌های کاربردی تحت وب بر اساس نوع معماری بکار رفته همراه با مهارت‌های بالا برای جرم‌یابی قانونی ضروری هستند. این آزمایش شامل یک برنامه وردپرس در بالای یک بسته LAMP[6] است که جرم‌یاب را ملزم می‌کند تا در مورد سرورهای لینوکس، آپاچی، PHP و غیره آگاهی داشته باشد.

I. روش بررسی.

روش بررسی ابراز شده در [7] بیان می‌کند که:

[6] . Linux, Apache , MySQL-Server, PHP

a) برنامه کاربردی تحت وب بایستی همیشه در طی تحقیقات جرم‌یابی قانونی از هر نوع دستکاری و خرابی داداه محافظت شود. این امر شامل سرورها یعنی جایی‌که برنامه‌های کاربردی تحت وب اجرا می‌شوند، نیز هست.

b) جرم‌یاب قانونی بایستی تمام فایل‌های لازم برای تحقیقات جرم‌یابی قانونی کشف نماید. این فایل‌ها می‌توانند ورودی سرور، متون جانبی سرور که به برنامه‌های کاربردی تحت وب مرتبطند، فایل‌های پیکر بندی سرور، ورودی‌های برنامه کاربردی شخص سوم نصب شده و ورودی‌های سیستم اجرایی، باشند.

c) داده جمع‌آوری شده بایستی بوسیله ابزارهای جرم‌یابی قانونی بازسازی جزئیات حمله سایبری، تحلیل گردد.

d) بعد از اینکه نتیجه با موفقیت بازسازی شد، مامور تحقیق می‌تواند یافته‌ها را خلاصه نماید و یک گزارش از تمام داده‌ها و فایل‌های استخراج شده از برنامه کاربردی تحت وب ارائه نماید.

3. آزمایش.

A. آغاز آزمایش.

حمله در یک محیط مجزا که از یک سرور محلی برای میزبانی برنامه کاربردی تحت وب هدف استفاده می کند، انجام می‌شود. بسته LAMP که روی سرور اجرا می شود شامل Ubuntu Linux 15.04(x64)، Apache HTTP Server 2.4.12، MY SQL 5.6.24 و PHP5.5.24 است. سرور وب توسط توسط پلتفرم آزمایشی نفوذ کننده Kali Linux (x64) هدف گر فته شد. آدرس‌های آی پی در محدوده شخصی IPv4 یعنی به ترتیب 192.168.1.6 و 192.168.1.10 برای سرور وب و سیستم آزمایشی نفوذ بوده است.

B. برنامه کاردبردی وردپرس.

وردپرس یک سیستم مدیریت محتوای متن باز (CMS) بوده که عمدتا برای ساخت وب‌سایت‌ها و وبلاگ‌ها استفاده می‌شود. داده‌های آماری نشان می دهند که 4.5٪ وب‌سایت‌ها عموما از وردپرس استفاده می‌کنند[4] و این موضوع

در علت انتخاب ورد پرس برای نشان دادن طرز کار نقش دارد. وردپرس 4.2.2 روی سرور به نشانی http://127.0.0.1/wordpress نصب شد.

C. شخصیت.

برای اهداف این آزمایش، یک شخص به اسم Peter Quill خلق شد. وی 32 سال دارد و بعنوان یک مشاور IT کار می‌کند. وی دوست دارد به هنگام رانندگی موسیقی گوش دهد، مخصوصا رده راک متعلق به 1960-70. پیتر تصمیم دارد تا وبلاگ شخصی خود را بصورت آنلاین ا در وردپرس راه‌اندازی نمود زیرا وی می‌خواهد نظریات خود را در مورد آهنگ‌های محبوبش شرح دهد.

D. رمز عبورهای عبور.

مجموعه‌های مختلف رمز عبور برای داشتن نتایج مقایسه ای مبتنی بر موفقیت و زمان پردازش حمله لغت نامه‌ای استفاده شده است. این رمز عبورها بر اساس توصیه های منابع مربوطه انتخاب شده اند. در ارتباط با شخصیت رمز عبور عبور با توجه به آهنگ Jackson 5، "IWant You Back" انتخاب شده است.

E. حمله لغت‌نامه‌ای.

یک لغت نامه با استفاده از سه لغت نامه مرسوم و بسیار رایج ریپر (10934 بایت) و کین و آبل جمعا (1069968 بایت) ایجاد شد [11]. این حمله که از نرم‌افزار کاربردی WPScan روی Kali Linux استفاده می‌کند که صرفا برای نفوذ به وردپرس طراحی شده است. نفوذ با بازیابی نام‌های کاربری و اطلاعات مربوط به آسیب‌پذیری وردپرس به منظور کرکینگ پسورد آغاز شد. نام کاربری هدف از طریق نام شخصیت یعنی پیتر کوییل شناسایی شد. که بوسیله تابع شمارش WPScan فراهم شد. سپس این نام کاربری برای کرکینگ پسورد با فایل لیست نام لغت نامه استفاده شد.

F. ورورد به سیستم.

سرور آپاچی ،به صورت پیش‌فرض، کلیه درخواست دسترسی و ورود را در یک فایل متنی access logs.txt تولید شده ذخیره می‌کند، که می تواند حملات را ردیابی نماید. پارامترهای مختلف درخواست‌های دسترسی می‌توانند برای ردیابی مفید باشند، مانند آدرس آی پی منبع، time stamp[7]، روش درخواست HTTP و نشانی وب درخواستی URL. بعد از اجرای حمله لغت نامه‌ای، فایل اجازه دسترسی کنترل می‌شود. بعلاوه، یک افزونه[8] وردپرس که افزونه WP Security Audit Log، نامیده می‌شود، در نرم‌افزار کاربردی وردپرس نصب شده است تا اطلاعات مربوط به تلاش‌ها برای دسترسی به سیستم و همچنین نام‌های کاربری که مورد استفاده قرار گرفته را، تهیه نماید. همچنین، این افزونه می‌تواند جزئیات مربوط به فعالیت یک کاربر خاص را در وردپرس را جمع‌آوری نماید.

G. نتایج.

حمله با شناسایی نام کاربری هدف قبل از اینکه کرکینگ پسورد انجام شود، آغاز شد این روند با استفاده از دستور wpscan که در شکل (2) نشان داده است، آغاز شد.

```
root@kali:~#                                    wpscan
```

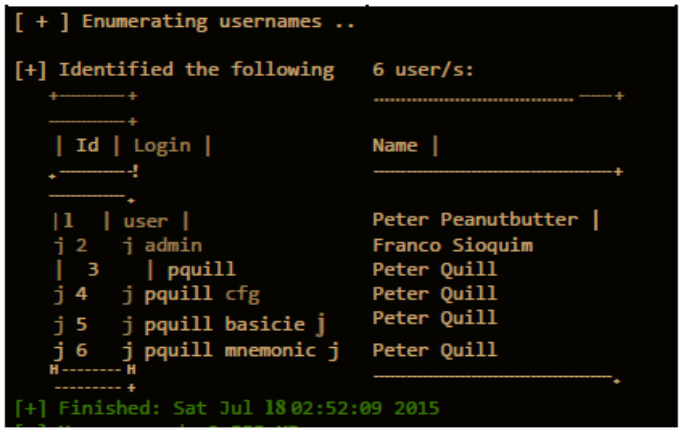
شکل (2): دستور wpscan.

بطور مشابه شکل (3) لیست تمام اسامی کاربری آماده در نرم‌افزار کاربردی وردپرس نشان می‌دهد، که شامل مدیر حساب کاربری نیز هست. نام‌های کاربری زیر ستون ورود به سیستم قرار گرفته‌اند که در آن Pquiil کاربری با رمز عبور پیش‌فرض است که در جدول (1) قابل مشاهده است و نام‌های کاربری باقی مانده Peter Quill از پسورد pquill نوع معمول پیروی می‌کنند. علاوه بر آن، ستون ID، شناسه کاربری کاربران واقعی است که توسط وردپرس استفاده شده است.

---

[8]. منظور از Timestamp عددی است که معادل با تعداد ثانیه هایی است که از ساعت 12 شب روز یکم ژانویه سال 1970 تا کنون سپری شده است و متد time در زبان PHP این زمان سپری شده را در اختیار ما قرار می دهد.

[8] . پلاگین ها ابزارهای جانبی هستند که شرکت سازنده نرم افزار به کاربران داده تا اونها هم بتونند در زمینه بهبود و گسترش دادن کار برنامه فعالیت داشته باشند.



شکل(3): دستور WPscan برای نشان دادن تمام نام‌های کاربری در وب سایت ورد پرس.

PUBLICATIONS

Password	Type
jackson	Default [1]
123jackson45	CFG [14]
iwantyouj ackson5	basic16 [5]
IWtYBk!!	mnemonic [6]

جدول 1: رمز عبورهای استخراج شده از روش‌های پیشنهاد شده توسط انتشارات مربوطه .

یک مثال دستوری در شکل (4) برای اجرای حمله لغت نامه‌ای برعلیه کاربر pquiil که از لغت نامه Jhone th Ripper استفاده می کند، به کار رفته است. با دانستن نام کاربری مورد استفاده توسط شخصیت، حمله‌های باقی مانده از استفاده از دو دیکشنری روی انواع مختلف رمز عبور برای کرکینگ رمز عبور استفاده می کنند که نتایج در جدول (2) نشان داده شده است.

شکل (4): دستور WPScan برای حمله لغت نامه‌ای که لیست کلمات Jhone the Ripper را استفاده می کند را نشان می‌دهد.

Dictionary	Username	Time	Status
JTR	Pquill	00:01:45	Success
JTR	pquill cfg	00:04:10	Fail
JTR	pquill basic16	00:04:10	Fail
JTR	pquill mnemonic	00:04:11	Fail
CAA	Pquill	03:18:41	Success
CAA	pquill cfg	06:38:55	Fail
CAA	pquill basic16	06:39:00	Fail
CAA	pquill mnemonic	06:39:16	Fail

جدول (2): نتایج استفاده از حمله لغت نامه ای که از Thone The Ripper(JTR) و Cain And Abel (CAA) استفاده می‌کند.

این جدول نشان می‌دهد که تمام رمز عبورهای الفبایی پیش‌فرض Jackson هستند می توانند با هر دو دیکشنری کرک شوند. به عبارت دیگر، حمله‌های لغت‌نامه ای در کرک انواع دیگر رمز عبورها که روش‌های قویتر کردن رمز عبور به آنها اعمال شده است، موفق عمل نمی‌کند.

هر دو فایل های دسترسی ورود به سیستم آپاچی و ورد پرس به دست آمده از افزونه‌ها بعد از اجرای حمله لغت نامه‌ای بررسی شده‌اند. شکل (5) نشان می‌دهد که دسترسی ورود به سیستم آپاچی چندین درخواست post[9] به فایل "hp"wp-login.p فرستاد. پارامترهایی که در ورود به سیستم نقش دارند عبارتند از، آدرس IP مشتری، timestamps سرور، درخواست HTTP، کد وضعیت و اندازه جواب به مشتری. تمامی ورود به سیستم بدست آمده از افزونه وردپرسی WP Security Audit Log[10] در شکل (5)، اطلاعات دیگری نظیر نام کاربری و وضعیت ورود به سیستم که در ورود به سیستم آپاچی وجود ندارند را نشان می‌دهد.

[9] دستور post اطلاعات ارسالی را جهت پردازش به یک منبع مشخص شده میفرستد

[10] یکی از قوی ترین پلاگین های امنیتی وردپرس می باشد که تمامی فعالیت ها را به طور کامل ثبت می کند. با استفاده از این افزونه می توان فعالیت کاربران را برسی کرد.

4. تحقیق و بررسی جرم‌یابی قانونی.

این بخش روش‌هایی که می توانند برای تحقیقات جرم‌یابی قانونی آزمایش بکار روند را بررسی کرده و به فایل‌های ورود به سیستم توجه دارد. در تحلیل فایل‌های ورود به سیستم الگوهای زیر می توانند معیاری برای فعالیت مشکوک باشند:

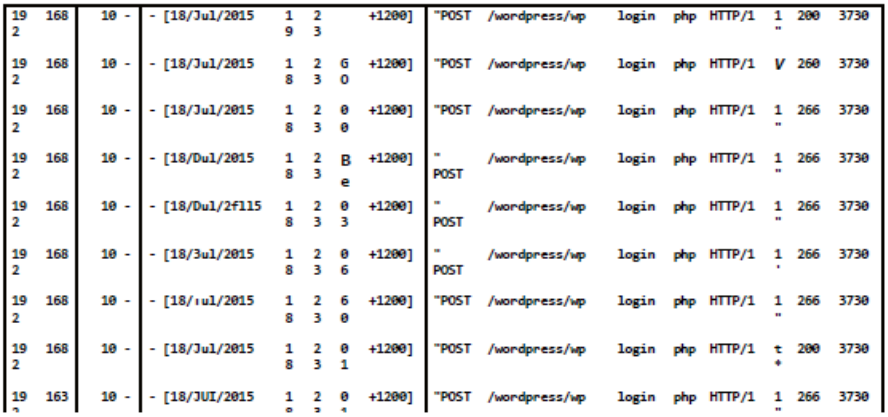
- درخواست‌های HTTP نسبتا طولانی.
- فایل‌هایی که خارج از شاخه فهرست وب سرور قرار گرفته‌اند.
- فایل‌هایی که خارج از فهرست برنامه‌های کاربردی تحت وب و پایگاه داده قرار گرفته‌اند.
- استفاده غیرعادی از روش‌های HTTP مانند HEAD، PUT و PROPFIND.

A. وب سرور.

a) ورورد به سیستم آپاچی.

برای لاگ‌های[11] آپاچی، پیکر بندی می تواند به نشانی http.conf قابل دسترسی باشد. که می‌تواند برای تغییر محل و قالب‌بندی فایل‌های لاگ پیش‌فرض استفاده شود. بطور مشابه می تواند به محل واقعی لاگ‌ها اشاره کند. سه نوع لاگ وجود دارند که می توانند برای جرم یابی قانونی، بازیابی شوند که عبارتند از لاگ‌های خطا، لاگ‌های ماژول، لاگ‌های دستیابی. لاگ های خطا تمام پیام‌های خطا در سرور آپاچی را بایگانی می‌کند. لاگ‌های ماژول بایگانی‌هایی هستند که بطور اختصاصی مربوط به ماژول‌های نصب شده در سرور آپاچی هستند. به عبارتی دیگر، لاگ‌های دستیابی در شکل (5) شامل درخواست HTTP هستند که به سرور انتقال می‌یابند، و این امر به این معناست که حملات بروت فورس و لغت‌نامه‌ای به هنگام استفاده از آن می توانند ردیابی شوند. شکل (5) دنباله ای از درخواست‌های چندگانه POST در یک فایل دستیابی وردپرس نشان می‌دهد.

[11] لاگ ها حاوی اطلاعات بسیار حساس و حیاتی از همه رویداد های مربوط به برنامه های کاربردی، سرویس ها و سیستم عامل می باشند



شکل (5) : لاگ های دستیابی آپاچی بعد از حمله لغت نامه‌ای.

این درخواست ها دارای وقفه ای بسیار کوتاه هستند که نشانگر ویژگی مشکوک آنها است [17].

B. سرور برنامه‌های کاربردی.

سرورهای برنامه‌های کاربردی می توانند شامل مکانیسم لاگینگ[12]که وقایعی مانند، خطاهای نرم‌افزار کاربردی، مشکل بالا آمدن؛ استثناهای کنترل نشده و پیام‌های نرم افزار کاربردی را ثبت می کند، باشند.

a) لاگ‌های PHP.

برنامه کاربردی PHP شامل لاگ‌های خطا است که می‌توانند به صورت پیش‌فرض‌در فهرست لاگ خطای var/log/httpd/php ذخیره شوند. همچنین، می تواند توسط فایل php.ini پیکربندی شود که که در /etc/php.ini/ قرار دارند[10]. پیام‌های آسیب‌های PHP و خطاها می‌توانند در لاگ خطا ثبت و نگهداری شوند. این لاگ‌ها همچنین توسط مدیر سیستم برای نظارت بر برنامه کاربردی سرور زمانی PHP اجرا می شود، ولی خطا در background رخ می‌دهد، مورد استفاده قرار می‌گیرد. یک لاگ مفید دیگر لاگ سیستم است. لاگ‌های

[12] در علوم کامپیوتر به فرایندی که رویداد های اتفاق افتاده یا پیغام های ارسال شده بین کاربران در سیستم را ثبت می کند فرایند Logging و به فایلی که این اطلاعات در ان ثبت می شود Log File می گوئیم.

سیستمی که شامل لاگینگ محدود شده به یک ناحیه هستند که برای یک برنامه کاربردی خاص بکارمی‌روند. این فایل‌های ترکیب شده در لاگ سیستم می‌توانند err.log، warning.log، info.log و debug.log باشند.

C. سرور پایگاه داده.

پایگاه داده عموما دارای لاگینگ محدود بوده و بعضا حتی هیچ لاگینگی به صورت پیش‌فرض فعال در آن وجود ندارد، که خود یک عامل محدود کننده برای تحقیقات جرم‌یابی قانونی است. اگرچه قابلیت‌های لاگینگ Data specific و Table logging که از راه‌انداز پایگاه داده استفاده می کنند به سرور قابل اعمال است.

a) MYSQL

MYSQL پنج نوع لاگ را ذخیره می‌کند که شامل لاگ خطا، General Query[13]log، rely log[14] و binary log[15] و slow Query log[16] است. وظیفه لاگ خطا مواجه شدن با مشکلاتی است که درحین شروع، اجرا و متوقف شدن عملیات در پایگاه داده MYSQL است. Generalquery Log شامل برقراری ارتباز موفق مشتری و گزارش SQL صادره از مشتری است. به عبارت دیگر Binary log ثبت گزارشات به روز شده داده را به عهده دارد و Rely log تغییرات صورت گرفته در داده رسیده از سرور پاسخگو را ثبت می کند. نهایتا، slow query log برای مامور تحقیق جرم یابی قانونی مثمر ثمر است زیرا شامل جستجوهایی است که برای اجرا به زمان بیشتری نیاز دارند بنابراین می تواند به فعالیت‌های مشکوک مربوط باشد.

---

[13] این لاگ بربرقرارشدن صحیح اتصالات و دستوارت کلاینت ها نظارت می کند.

[14] تغییرات داده که از replication master server دریافت می شود.

[15] رویدادهایی که تغییرات دیتابیس را تشریح می کند مانند عملیات ایجاد جدول یا تغییرات روی داده های جداول (همچنین برای replication استفاده می شود).

[16] اطلاعات query هایی که زمان اجرایی بیش از یک مدت زمان تعیین شده دارند.

D. برنامه کاربردی تحت وب.

لاگ‌های برنامه‌های کاربردی تحت وب می توانند شامل اطلاعات بسیار مهمی برای برای جرم یاب قانونی باشند، مانند داده دقیق در باره منطق تجاری. جرم یاب قانونی بایستی معاونت از طرف توسعه دهنگان وب و مدیر وب را که دارای اطلاعات در مورد نرم افزار کاربردی تحت وب هستند را مورد بررسی قرار دهد. اطلاعاتی که می توانند بازیابی شوند مکان و فرمت لاگ‌های نرم افزار کاربردی تحت وب، پیامهای رو لاگ‌ها که می‌توانند بعنوان فعالیت مشکوک تلقی شوند و با چه طولی این لاگ‌ها ذخیره شده اند، می‌باشند[17].

a) لاگ‌های وردپرس.

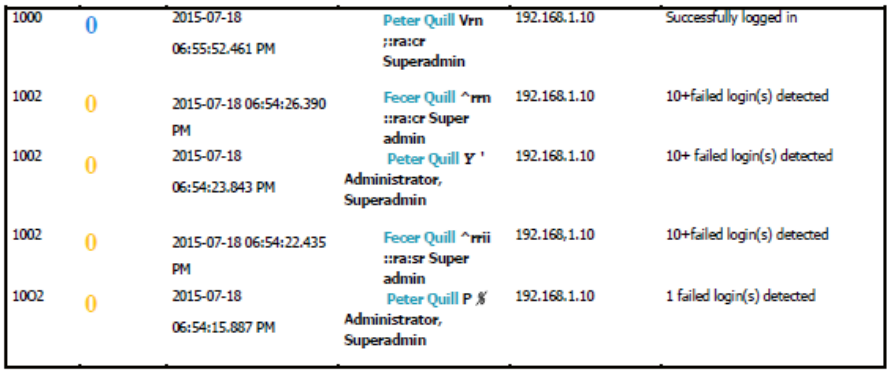
برنامه کاربردی تحت وب وردپرس می تواند دارای لاگ‌های Debug[17] باشد وقتی WP DEBUG روی حالت درست تنظیم می‌شود. و وقتی فعال شد، تمامی خطاها در فایل لاگ Debug، داخل فهرست wp-content/ ذخیره می شوند. این فایل برای جرم‌یاب قانونی بسیار مفید است زیرا می تواند تمامی خطای notice در پس زمینه تولید شده توسط درخواست AJAX[۱۸] و corn job[۱۹] را نشان دهد[18]. به‌علاوه افزونه های وردپرس که قابلیت‌های لاگینگ را ارئه می‌کنند برای بازیابی اتفاقاتی که در برنامه کاربردی تحت وب رخ داده، بکار روند. شکل (6) مثال از اتفاقات ورود به سیستم را به هنگام استفاده از افزونه وردپرس ثبت کرده است.

---

[17] هر ماژول برای برای ثبت لا´ها از چند سطح استفاده می شود، Debug سطحی که بیشترین اطلاعات را در Logfile فراهم می کند.

[18] Ajax تکنیکی برای ایجاد صفحات وب سریع و پویا می‌باشدAjax . به صفحات وب این امکان را میدهد که به صورت غیر همزمان و تنها با تبادل اطلاعات اندکی با سرور، بخشی از صفحه را به روز رسانی کنند

[19] Cron یک سرویس زمانبندی است که وظیفه اجرای روتین‌های خاصی را در زمان مشخص بر عهده دارد. Cron این امکان را ایجاد می کند که کارهای روتین و روزمره را به صورت اتوماتیک به انجام برسانیم. کارهایی که باید با زمانبندی انجام شوند در فایلی با نام CronTab ذخیره می شوند.



1000	0	2015-07-18 06:55:52.461 PM	Peter Quill Vrn ::ra:cr Superadmin	192.168.1.10	Successfully logged in
1002	0	2015-07-18 06:54:26.390 PM	Fecer Quill ^rrn ::ra:cr Super admin	192.168.1.10	10+failed login(s) detected
1002	0	2015-07-18 06:54:23.843 PM	Peter Quill Y ' Administrator, Superadmin	192.168.1.10	10+ failed login(s) detected
1002	0	2015-07-18 06:54:22.435 PM	Fecer Quill ^rrii ::ra:sr Super admin	192.168,1.10	10+failed login(s) detected
1002	0	2015-07-18 06:54:15.887 PM	Peter Quill P % Administrator, Superadmin	192.168.1.10	1 failed login(s) detected

شکل (6): Audit Log وردپرس بعد از حمله لغت نامه‌ای.

5. اقدام متقابل.

اقدامات متقابل زیر برای کاستن از تاثیر حمله لغت‌نامه‌ای در وردپرس که شرح داده شد به‌کار می‌رود. در برخی موارد این اقدامات متقابل قابل اعمال به به انواع دیگر از برنامه‌های کاربردی تحت وب هستند.

A. سیستم قفل گذاری (LOCKOUT).

روش‌های متعددی برای محافظت رمز عبور وب سایت‌ها در مقابل حملات کرکینگ وجود دارد. یک سیستم قفل‌گذاری اجازه می‌دهد تا تعداد ثابتی از خطای وارد کردن پسورد اشتباه ، قبل از قفل شدن موقت یا همیشگی سیستم وجود داشته باشد.

مهاجم تنها شانس وارد کردن تعداد محدودی حدس را قبل از اینکه سیستم درخواست ورود وی را رد کند، دارد. به‌علاوه تعدادی افزونه مانند (word fence، Bult proof security، All in one WP security and Firewalls)[20] وجود دارند که ورد پرس را با قابلیت محافظت امنیتی بیشتر مجهز می‌کنند. برخی افزونه به کاربرقانونی اجازه می دهند که از بیشترین تعداد تکرار عملیات کاربر برای ورود اشتباه را برای خود تنظیم نمایند.

[20] افزونه هایی برای افزایش امنیت شبکه.

B. احراز هویت چند عاملی.

احراز هویت چند عاملی مشخصه دیگری است که همچنین توسط افزونه Word Fence و iThemes Security ارائه شده است (سابقا WPSecurity بهتر بود). Word Fence کاربران وردپرس را قادر می‌سازد تا تا به احراز هویت دو مرحله‌ای از طریق سرویس پیام کوتاه دسترسی داشته باشند. این اقدام متقابل در برابر حملات لغت نامه‌ای و بروت فورس به شدت موثر است زیرا زیرا کاربر علاوه بر نیاز به نام کاربری و رمز عبور ورود به مولفه دیگری برای تصدیق هویت نیازمند است که به شکل کدی است که تنها در وسیله الکترونیکی کاربر مربوطه قابل دیدن است و اط طریق سرویس پیام کوتاه فرستاده می‌شود.

C. انتخاب رمز عبوری قوی.

قوی سازی رمز عبور سریع‌ترین اقدام متقابل در برابر حملات کرک رمز عبور است. این روش تنها به به خود کاربر و دانش وی در مورد دستیابی به یک رمز عبور بسیار مشکل برای شکستن آن است. برخی روش‌های که در برابر حملات لغت نامه‌ای ذکر شد عبارتند از روش CFG، انتخاب رمز عبور 16 کاراکتری و رمز عبورهای حفظی. همان‌گونه که قبلا نشان داده شد، این روش‌ها موثرند زیرا این رمز عبورهای قوی در دو لغت نامه استفاده شده، موجود نیستند. بعلاوه، استفاده از روش رمز عبور طولانی توصیه می‌شود مانند روش انتخاب رمز عبور 16 کاراکتری. این روش نه تنها پیچیدگی رمز عبور را در برابر حملات کرک پسورد افزایش می‌دهد بلکه نیاز به لت نامه‌ای دارد که حداقل تعداد کاراکتر آن 16 تا باشد که پروسه زمان اجرای حمله را تا حدی طولانی تر می سازد.

6. بحث و بررسی.

حمله‌های لغت‌نامه ای آسیب پذیری وردپرس تازه نصب شده را نشان می‌دهد. نام کاربری به راحتی می تواند توسط نرم افزار کاربردی WPScan شمرده شده و کشف گردد. بعلاوه، نام شخصی و شهرت در میان اطلاعاتی است که توسط مرتکب جرم در حمله برای کرک رمز عبور پیچیده‌تر مورد استفاده قرار می‌گیرد. لغت‌نامه‌های Jhone The

Ripper و Cain & Abel ، برای شکست رمز عبور انواع مختلف رمز عبورهای مانند رمز عبورهای مبتنی بر روش‌های قوی‌تر کردن پسورد، مورد استفاده قرار گرفت. نتیج نشان داد که هر دو لغت‌نامه در شکستن رمز عبورهای قویتر شده شکست خوردند، گرچه آنها قادرند تا رمز عبور پیش‌فرضی که از رشته حروف کوچک استفاده می‌کند را تشخیص دهند "Jackson".

لغت‌نامه‌های مشهور دیگری نیز وجود دارند که لیست کلمات بزرگتری هستند و برخی قابلیت این را دارندکه روی سبک خاصی از کلمات تمرکز کنند [11]. عاملی که بایستی به آن توجه شود عامل زمان است، زمان لازم است تا حمله انجام شود. یک لغت نامه بزرگتر همان‌گونه که قبلا نشان داده شد زمان بیشتری برای تحلیل و حمله نیاز دارد، مثلا در مورد دیکشنری Cain & Abel 7 ساعت طول کشید تا حمله تکمیل شود درحالی‌که در Jhone The Ripper 4 دقیقه تا تکمیل عملیات زمان لازم بود. لغت‌نامه‌های مشهور در مورد هدف‌هایی که مرتکب جرم هیچ اطلاعاتی در مورد کاربر ندارد مفید است. اگرچه اگر معلومات قبلی در مورد کاربر موجود باشد، برخی روش‌ها به دیکشنری قابل اعمال هستند و یا استفاده از لیست کلماتی که از دسته بندی موسیقی تولید شده باشد را می توان استفاده نمود. حمله بروت فورس شناسایی عبارت "I WANT YOU BACK" و "Jackson5" را در لیست کلمات با رمز عبور مبتنی بر حداقل 6 کاراکتر و مبنی بر سیاست انتخاب رمز عبور وردپرس، را انجام داد.

آزمایش همچنین چگونگی ردیابی حمله را با آنالیز لاگ‌های دستیابی آپاچی و لاگ‌های WP Security Audit Log شرح می‌دهد. لاگ‌های دستیابی آپاچی نشان میدهند که درخواست‌های POST در مسیر worpress/wp-login.php وجود دارند که بعنوان فعالیت مشکوک ورود به سیستم اهمیت دارند. بایستی توجه شود که شرایط درخواست‌های پی در پی با وقفه بسیار کوچک کمتر از ثانیه یک وضعیت غیرعادی است. عامل دیگری که تشخیص چگونگی دسترسی غیرعادی تاثیر دارد این است که این درخواست‌ها از یک IP صادر می‌شوند. علاوه بر لاگ‌های دستیابی آپاچی، دیگر اطلاعات لازم برای توضیح حمله از نصب افزونه وردپرس برای تولید لاگ‌های احراز هویت، بازیابی می‌شود. تحقیق نشان می‌دهد که تلاش‌های ناموفق برای دستیابی اکانت Peter Quill را هدف قرار داده بودند و در یک چارچوب زمانی مشابه درخواست‌های پی در پی ورود به سیستم در لاگ‌های دستیابی آپاچی رخ داد.

7. نتایج

احراز هویت وب‌سایت نسبت به انواع حمله های حدس رمز عبور مانند حمله لغت‌نامه‌ای و بروت فوس در معرض خطر است. یک حمله برای توضیح بیشتر اینکه چگونه یک حمله لغت‌نامه‌ای انجام شد تا به احراز هویت وب‌سایت ورد پرس نفوذ کند، شبیه سازی شد. مهاجم نیاز دارد تا به نام کاربری قبل از حدس رمز عبور ورود دسترسی پیدا کند. همچنین کسب اطلاعات شخصی‌می تواند برای یک حدس رمز عبور موثر، مفید باشد. حمله لغت‌نامه‌ای نشان داده شده شکستن رمز عبوری که از حروف کوچک الفبا تنها با 7 کاراکتر استفاده می‌کند با استفاده از لغت‌نامه‌های مشهور که بصورت آنلاین موجودند، به راحتی قابل شکست و ردیابی است. به عبارت دیگر اعمال روش‌های قویتر کردن رمز عبورهای که با مرور تحقیقات قبلی پیشنهاد داده شده بود، به‌طور موثری از از حملات کاست. همچنین استفاده از رمز عبورهایی با تعداد کاراکتر بالا آن را به رمز عبوری بسیار مشکل و زمان بر برای کرک تبدیل می‌کند. همچنین اقدامات متقابلی وجود دارد که به وردپرس قابل اعمال هستند مانندLOCKOUT کردن سیستم، احراز هویت چند عاملی (چند مرحله‌ای)، انتخاب رمز عبور قوی و اجتناب از استفاده نام واقعی. این اقدامات متقابل براحتی در افزونه‌های وردپرس مانند WordFence قابل دستیابی هستند. همچنین لاگ‌های دستیابی می‌توانند در اجرا عملیات جرم‌یابی قانونی موثر باشند زیرا شامل اطلاعات مفیدی مانند timestamp، آدرس IP منبع حمله، نام کاربری هدف و تعداد تلاش‌ها برای دستیابی به هدف. مقایسه کارآیی برای هر روش قویتر کردن رمز عبور در این مقاله برجسته نشده و مورد بررسی قرار نگرفته است که می‌تواند پایه ای برای کارهای آینده باشد. بعلاوه این گزارش تنها یک حمله ساده لغت نامه‌ای را بدون اینکه هیچ قانون خاصی به آن اعمال شده باشد، شبیه سازی نمود. یک تحقیق اضافی می‌تواند با تلاش برای حمله با لغت‌نامه‌های پیچیده تر و لیست لغت وسیع‌تر انجام شود. بعلاوه حمله بروت فورس که از یک عبارت معلوم مختص شخصیت استفاده می‌کند نیز می‌تواند شبیه سازی شود.

برای داشتن تحقیق جرم‌یابی قانونی کارآمد در حالت حمله لغت‌نامه ای علیه نرم‌افزار کاربردی تحت وب وردپرس، فایل‌های لاگ روی سرور بایستی به طرز مناسبی پیکر بندی شده و محافظت شوند. مامور تحقیق جرم‌یابی قانونی بایستی مهارت کافی برای اجرای تحقیق و همچنین در مورد معماری، منطق کسب و کار نرم‌افزار کاربردی تحت وب

آگاهی کافی داشته باشد. جرم‌یابی قانونی تحت وب بیشتر به بازگرداندن و تحلیل لاگ‌های به دست آمده از وب سرور، سرور نرم افزار کاربردی، سرور پایگاه داده و نرم افزار کاربردی وردپرس توجه دارد.

REFERENCES

[1] A. Das, J. Bonneau, M. Caesar, N. Borisov and X. Wang, 'The Tangled Web of Password Reuse', *Symposium on Network and Distributed System Security (NDSS)*, 2014.

[2] D. Gillman, Y. Lin, B. Maggs and R. K. Sitaraman, 'Protecting Websites from Attack with Secure Delivery Networks', *Computer*, vol. 48, no. 4, pp. 26 - 34, 2015.

[3] J. A. Halderman, B. Waters and E. W. Felten, 'A convenient method for securely managing passwords', *In Proceedings of the 14th international conference on World Wide Web*, pp. 471-479, 2005.

[4] K. K, '[Infographic] WordPress 4.1 Gets Roughly 1 Million Downloads Every Two Days + Other Mesmerizing WordPress Stats', 2015. [Online]. Available: http://www.codeinwp.com/blog/mesmerizing-wordpress-stats/.

[5] P. G. Kelley, S. Komandur, . M. L. Mazurek, . R. Shay, . T. V. L. Bauer, N. Christin, L. F. Cranor and J. Lope, 'Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms', in *Security and Privacy (SP), 2012 IEEE Symposium on*, San Francisco, CA, 2012.

[6] C. Kuo, S. Romanosky and L. F. Cranor, 'Human selection of mnemonic phrase-based passwords', *In Proceedings of the second symposium on Usable privacy and security*, pp. 67-78, 2006.

[7] A. Lazzez and T. Slimani, 'Forensics Investigation of Web Application Security Attacks', *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 7, no. 3, p. 10, 2015.

[8] MySQL, '5.2 MySQL Server Logs', 2015. [Online]. Available: https://dev.mysql.com/doc/refman/5.0/en/server-logs.html.

[9] M. Reith, C. Carr and G. Gunsch, 'An examination of digital forensic models', *International Journal of Digital Evidence*, vol. 1, no. 3, p. 1–12, 2002.

[10] I. Sanosyan, 'Getting the Most Out of Your PHP Log Files: A Practical Guide', 2015. [Online]. Available: http://www.toptal.com/php/getting-the-most-out-of-your-log-files-a-practical-guide.

[11] Skullsecurity, 'Passwords', 2015. [Online]. Available: https://wiki.skullsecurity.org/Passwords.

[12] D. Silver, S. Jana, D. Boneh, E. Chen and C. Jackson, 'Password Managers: Attacks and Defenses', *In Proceedings of the 23rd Usenix Security Symposium*, 2014.

[13] M. Taylor, J. Haggerty, D. Gresty and D. Lamb, 'Forensics investigation challenges in cloud computing environments', *Network Security*, vol. 2011, no. 3, p. 4–10, 2011.

[14] S. Vaithyasubramanian and A. Christy, 'An Anaysis of CFG Password Against Brute Force Attack for Web Applications', *Contemporary Engineeri*, vol. 8, no. 9, pp. 367 - 374, 2015.

[15] A. G. Voyiatzis, C. A. Fidas, D. N. Serpanos and N. M. Avouris, 'An Empirical Study on the Web Password Strength in Greece', in *Informatics (PCI), 2011 15th Panhellenic Conference on*, Kastonia, 2011.