Web

Penetration Testing

with

Kali Linux

Very Informative

تست نفوذ وب با کالی لینوکس

نسخه نمایشی

محمد شریعتی مهر . مرداد ۹۵

نام کتاب : تست نفوذ با کالی لینوکس 2

منبع : Web Penetration Testing with Kali Linux

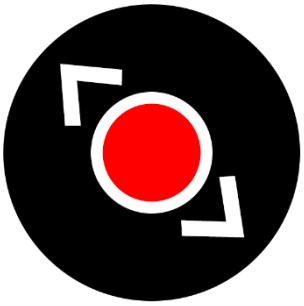
موضوع : امنیت شبکه

سطح آموزشی : متوسط

تاریخ انتشار : مرداد 95

تعداد صفحات : 558

نویسنده و مترجم : محمد شریعتی مهر



آیا این کتاب برای شما ساخته شده است ؟

اگر که در زمینه تست نفوذ و تست نفوذ وب فعالیت می کنید و به مرجعی کامل در زمینه تست نفوذ وب نیاز دارید یا محقق امنیت شبکه هستید و به دنبال جدیدترین راهکارهای تست نفوذ وب هستید , یا توسعه دهنده اپلیکیشن های وب هستید یا در تیم امنیتی یک پروژه اپلیکیشن وب فعالیت می کنید و نیاز دارید تا اپلیکیشن خود را از نظر امنیتی بهینه کنید یا شخصی علاقه مند در زمینه تست نفوذ اپلیکیشن های وب هستید .... این کتاب برای شما طراحی شده است.

مهم ترین مزیت ها و فواید این کتاب برای شما ؟

این کتاب با صرف زمان زیادی ایجاد شده و کلیه آزمایش های موجود به صورت تصویری یک بار مجددا توسط شخص بنده از صفر برای شما انجام شده است.

در بسیاری از بخش ها نواقص آموزشی موجود در کتاب مرجع برطرف شده و مراحل انجام کار با شرح بیشتری نمایش داده می شود که از جنبه آموزشی کار را برای شما بسیار ساده تر خواهد کرد.

هدف اصلی این کتاب آشنایی شما با ابزارهای مختلف تست نفوذ وب در سیستم کالی لینوکس 2 می باشد . کار با ابزارها را یاد می گیرید و قادر خواهید بود در تست های نفوذ خود از آنها به سادگی استفاده کنید.

شما خواهید توانست یک محیط تست محلی برای خود ایجاد کنید و انواع مختلفی از آسیب پذیری های اپلیکیشن های وب را تست کنید. نحوه تست و مراحل به صورت گام به گام به همراه متن و تصاویر گویا گنجانده شده است.

از مهم ترین ویژگی های این کتاب معرفی ابزارهای مختلف کالی لینوکس در هر زمینه و نحوه کار با آنها می باشد.

تمرین ها چطور ؟

داخل کتاب شما آزمایش های زیادی را انجام خواهید داد ولی به منظور یادگیری هر چه بهتر دایما تمرین ها , مطالب و آموزش های جدیدی برای شما طراحی خواهد شد که فقط کاربرانی که کتاب را از طریق سایت سفارش داده اند قادر به دسترسی و مطالعه این محتوا خواهند بود. مهمترین مزیت چنین رویکردی این است که با این روش بروزترین آموزش ها و مفاهیمی که شاید در کتاب گفته نشده آموزش داده خواهد شد. این مطالب جدید را از آدرس زیر مطالعه کنید :

http://netamooz.net/courses/web-hacking-basics/

در این کتاب چه می خوانم ؟

با مفاهیم اولیه مورد نیاز امنیت اپلیکیشن های وب آشنا می شوید * یک محیط تست کامل به منظور تست اپلیکیشن های خود را در رایانه شخصی خود پیاده سازی می کنید * با فاز شناسایی آشنا شده و با ابزارهای زیادی در این زمینه کار می کنید و تست ها را پیاده سازی می کنید * با آسیب پذیری های رایج اپلیکیشن های وب آشنا شده و شروع به تست این آسیب پذیری ها می کنید * با انواع مختلف آسیب پذیری های تزریق آشنا می شوید و شروع به تست نفوذ این آسیب پذیری ها می کنید * با حملات سمت کلاینت آشنا شده و در این زمینه تست می کنید * آسیب پذیری های مبتنی بر SSL معرفی شده و اقدام به تست با ابزارهای موجود در این زمینه می کنیم * با فریم ورک های حمله رایج مانند SET و BEEF به منظور پیاده سازی حملات مهندسی اجتماعی و سمت مشتری کار می کنید * با آسیب پذیری های رایج آژاکس آشنا می شوید * با شیوه ها و ابزارهای مختلف تست فازینگ اپلیکیشن های وب کار می کنید.

فصل یک : مقدمه ای بر تست نفوذ وب

مقدمه ای بر تست نفوذ و تست نفوذ وب

تست امنیتی فعال

هکر کیست؟

متدولوژی های مختلف تست

هک اخلاقی یا Ethical Hacking

تست نفوذ Penetration testing

ارزیابی آسیب پذیری

حسابرسی امنیتی

قوانین تعامل

تست جعبه سیاه : تست جعبه خاکستری

جزئیات تماس مشتری

اطلاعیه های تیم فناوری اطلاعات مشتری

نگهداری داده های حیاتی و حساس

جلسه وضعیت Status meeting

محدودیت های تست نفوذ

نیاز به تست اپلیکیشن های وب

حملات مهندسی اجتماعی

آموزش کارمندان به منظور مقابله با حملات مهندسی اجتماعی

مروری بر اپلیکیشن وب برای آزمونگرهای نفوذ

پروتکل انتقال ابرمتن (HTTP)

هدر درخواست و پاسخ

هدر درخواست

هدر پاسخ

متدهای مهم HTTP برای تست نفوذ

متد GET/POST

متد HEAD

متد TRACE

متدهای PUT و DELETE

متد OPTIONS

ردیابی نشست با استفاده از کوکی ها

کوکی Cookie

جریان کوکی بین سرور و کلاینت

کوکی های ماندگار و غیرماندگار

پارامترهای کوکی

داده های html در پاسخ http

اپلیکیشن وب چندلایه

فصل دو : نصب آزمایشگاه خود با کالی لینوکس

کالی لینوکس

تکامل کالی لینوکس نسخه 2.0

نصب کالی لینوکس

نصب کالی بر روی USB در لینوکس

نصب کالی بر روی USB در ویندوز

نرم افزارهای مجازی سازی و ایمیج های ARM برای کالی لینوکس

انتشار ثابت در مقایسه با انتشار رولینگ

کالی رولینگ چیست ؟

نصب کالی رولینگ در ماشین مجازی Virtual Box

نصب کالی لینوکس بر روی هارد درایو

نصب ماشین مجازی OWASP

پیاده‌سازی متااسپلوییتبل Metasploitable

مجازی سازی کالی لینوکس درمقابل نصب بر روی ماشین فیزیکی

ابزارهای مهم در کالی لینوکس

پروکسی های اپلیکیشن وب

پروکسی برپ Burp Proxy

سفارشی کردن رهگیری کاربر

ویرایش درخواست ها در حین فرایند

Burp Proxy و وبسایت های مبتنی بر SSL

ابزارهای WebScarab و ZAP

ابزار ProxyStrike

اسکنر آسیب پذیری وب

نیکتو Nikto

اسکنر آسیب پذیری Skipfish

کاوشگر وب Dirbuster

اسکنر آسیب پذیری OpenVAS

بکارگیری پایگاه داده

ابزارهای شناسایی سیستم مدیریت محتوا (CMS)

فازرهای اپلیکیشن های وب

استفاده از تور برای تست نفوذ

فصل سه : شناسایی و نمایه سازی وب سرور

شناسایی

شناسایی فعال و شناسایی منفعل

شناسایی : جمع آوری اطلاعات

جزئیات ثبت دامنه

هویز : استخراج اطلاعات دامنه

شناسایی میزبان ها با استفاده از DNS

بروت فورس رکوردهای DNS با استفاده از انمپ

Recon-ng فریم ورک جمع آوری اطلاعات

سرشماری نام دامنه با استفاده از Recon-ng

ماژول های گزارش دهی

اسکن : کاوش هدف

اسکن پورت با استفاده از انمپ

گزینه های مختلف برای اسکن پورت

عبور از فایروال و IPS با انمپ

کشف فایروال با back checksum

شناسایی سیستم عامل با انمپ

ایجاد پروفایل سرور

انگشت نگاری اپلیکیشن

اسکن نسخه Nmap

اسکن نسخه Amp

انگشت نگاری فریم ورک اپلیکیشن وب

هدر HTTP

اسکنر Whatweb

شناسایی میزبان های مجازی

شناسایی لودبالانسرها

لودبالانسرهای مبتنی بر کوکی

دیگر روش های شناسایی لودبالانسرها

اسکن وب سرورها برای آسیب پذیری و پیکربندی های نادرست

شناسایی متدهای HTTP با استفاده از ابزار NMAP

تست وب سرورها با استفاده از ماژول ها اگزیلیاری

خودکارسازی اسکن با پلاگین اسکنر وب WMAP

گزارش گرافیکی با ابزار Skipfish

کاوش اپلیکیشن های وب

کاوشگر برپ Burp Spider

لاگین اپلیکیشن

فصل چهار : آسیب پذیری های اصلی در اپلیکیشن های وب

نشت اطلاعات

مرور شاخه

مرور شاخه ها با ابزار DirBuster

کامنت های HTML

مشکلات احرازهویت

بروت فورس اعتبارنامه ها

ابزار هایدرا

بروت فورس جیمیل و یاهو

پیمایش مسیر

حملات پیمایش مسیر از طریق Burp Proxy

آسیب های مبتنی بر تزریق

حملات تزریق دستور

تزریق اسکیوال

اسکریپت نویسی بین سایتی XSS

انواع آسیب پذیری های XSS

جعل درخواست بین سایتی

آسیب پذیری های مبتنی بر نشست

راههای مختلف سرقت توکن ها

بروت فورس توکن ها

شنود توکن ها و حملات شخص واسط

سرقت توکن ها با حملات XSS

اشتراک توکن نشست بین اپلیکیشن و مرورگر

ابزارهای آنالیز توکن ها

حمله تثبیت نشست

مقابله با حملات تثبیت نشست

آسیب پذیری گنجاندن فایل

درج ریموت فایل

درج فایل محلی

مقابله با حملات درج فایل

آلودگی پارامتر HTTP

تفکیک پاسخ HTTP

فصل پنج : حمله به سرور با استفاده از آسیب های مبتنی بر تزریق

تزریق دستور

شناسایی پارامترها برای تزریق داده ها

تزریق دستور مبتنی برخطا و نابینا

متاکاراکترها برای جداکننده دستور

اسکن تزریق دستور

ایجاد یک فایل کوکی برای احرازهویت

اجرای Wapiti

بکارگیری تزریق دستور با استفاده از متااسپلوییت

شل PHP و متااسپلوییت

بکارگیری شل شوک

معرفی شل شوک

بکارگیری شل شوک با متااسپلوییت

تزریق اسکیوال

عبارات اسکیوال

عملگر یونیون UNION

مثال کوئری اسکیوال

پتانسیل حمله به آسیب تزریق اسکیوال

تزریق اسکیوال نابینا

متدولوژی تست تزریق اسکیوال

اسکن برای وجود تزریق اسکیوال

جمع آوری اطلاعات

بکارگیری خودکار اسکیوال با ابزار اسکیوال مپ

معرفی ابزار تزریق اسکیوال نابینا BBQSQL

معرفی ابزار تزریق مای اسکیوال Sqlsus

ابزار تزریق SQLNinja

فصل شش : بکارگیری کلاینت ها با استفاده از حفره های XSS و CSRF

منشا حملات XSS

معرفی جاوا اسکریپت

مروری بر اسکریپت نویسی بین سایتی

انواع حملات XSS

XSS ماندگار

XSS بازتاب یافته

XSS مبتنی بر DOM

دفاع دربرابر حملات XSS مبتنی بر DOM

حملات XSS با استفاده از متد POST

جاوا اسکریپت و XSS یک ترکیب کشنده

سرقت کوکی ها

کی لاگر

دیفیس وبسایت

اسکن آسیب های XSS برای وبسایت

ابزار ZAP

هدف گذاری و انتخاب وضعیت ها

حالت های عملیاتی ZAP

پالیسی اسکن و حمله

ابزار Xsser

ابزار W3af

پلاگین های W3af

رابط گرافیکی ابزار W3af

حملات CSRF

پیش نیازهای حملات CSRF

متدلوژی حملات CSRF

تکنیک های کاهش حملات CSRF

فصل هفت : حمله بر روی وبسایت های مبتنی بر SSL

لایه سوکت امن

SSL در اپلیکیشن های وب

فرایند رمزنگاری SSL

رمزنگاری متقارن در مقایسه با رمزنگاری نامتقارن

الگوریتم های رمزنگاری نامتقارن

الگوریتم رمزنگاری متقارن

هشینگ برای یکپارچگی پیام

شناسایی پیاده سازی ضعیف SSL

ابزار OpenSSL

ابزار SSLScan

ابزار SSLyze

تست پیکربندی SSL با انمپ

حمله شخص واسط SSL

فصل هشت : بکارگیری کاربران با استفاده از فریم ورک های حمله

حملات مهندسی اجتماعی

جعبه ابزار مهندسی اجتماعی

حمله فیشینگ

SpearPhishing Attack

حامل های حمله وبسایت

حمله جاوا اپلت

حمله برداشت اعتبارنامه ها

حمله Web jacking

اکسپلوییت مرورگر با متااسپلوییت

حمله تغییر برگه

فریم ورک بکارگیری مرورگر BeEF

معرفی بیف

تزریق هوک در بیف

ماژول های شناسایی

ماژول های بکارگیری

ماژول های جمع آوری اطلاعات میزبان

ماژول های دسترسی همیشگی

ماژول های شناسایی شبکه

ماژول های IPEC

بکارگیری آسیب XSS در نرم افزار mutillidae با ابزار بیف

فصل نه : مشکلات امنیتی آژاکس و سرویس های وب

مقدمه ای بر آژاکس

ایجاد بلوک های آژاکس

جریان کاری آژاکس

مشکلات امنیتی آژاکس

افزایش سطح حمله

منطق برنامه نویسی افشا شده اپلیکیشن در سمت کلاینت

کنترل دسترسی نامناسب

چالش های تست نفوذ اپلیکیشن های وب مبتنی بر آژاکس

آنالیز کد سمت مشتری با فایرباگ

پانل Script

پانل Console

پانل شبکه Net

وب سرویس ها

معرفی وب سرویس های SOAP و RESTful

ایمن سازی وب سرویس ها

آسیب پذیری Insecure direct object reference

فصل ده : فازینگ اپلیکیشن های وب

مقدمات فازینگ

انواع تکنیک های فازینگ

فازینگ جهشی Mutation Fuzzing

فازینگ ایجاد Generation Fuzzing

اپلیکیشن های فازینگ

فازینگ پروتکل شبکه

فازینگ فایل

فازینگ رابط کاربری

فازینگ اپلیکیشن وب

فازینگ مرورگر وب

فریم ورک های فازر

گام های فازینگ

تست اپلیکیشن های وب با استفاده از فازینگ

فازینگ ورودی ها در اپلیکیشن وب

درخواست URI

هدرها

فیلدهای فرم

بررسی نتایج فازینگ

فازرهای اپلیکیشن وب در کالی لینوکس

فازینگ با Burp intruder

ابزار PowerFuzzer

بخش هایی از کتاب به صورت تصادفی در ادامه ....

مقدمه ای بر تست نفوذ و تست نفوذ وب

فرمانده ارشد امنیت اطلاعات (CISO) و مدیر ارشد امنیت (CTO) زمان و هزینه های هنگفتی را بر روی اپلیکیشن ها و امنیت کلی فناوری صرف می کنند . این موضوع شاید فواید زیادی هم برای آنها نداشته باشد و در نهایت با امنیت پایین روبرو شوند. گرچه طی سال های اخیر امنیت اطلاعات به یک اصل مهم و با اولویت بالا برای سازمان ها تبدیل شده ولی نفوذهای امنیتی به قدرت خود باقی است. حملات ایجاد شده بر روی اهداف سازمانی یکی از بزرگترین خرده فروشان در ایالات متحده امریکا موجب شده تا اطلاعات بیش از چهل میلیون کارت اعتباری و جزئیات آن افشا شود که در نتیجه منجر به استعفای CISO و CTO شرکت شده .

حمله بر روی شبکه شرکت پلی استیشن سونی حاصل حملات تزریق اسکیوال بوده (یکی از رایج ترین حملات اپلیکیشن های وب) که در نتیجه آن شبکه مربوط بیش از 24 روز از سرویس دهی خارج شد! این حمله موجب لو رفتن اطلاعات شخصی بیش از 77 میلیون حساب کاربری مشتریان شد. در ادامه آن جزئیات شخصی و رکوردهای مالی در بازارهای سیاه به صورت زیرزمینی به فروش رفته و برای فعالیت های مخرب مورد استفاده قرار گرفت.

حملات زیاد دیگری نیز رخ داده که در اخبار گزارش نشده است. هرچند که شاید اپلیکیشن های وب تنها دلیل رخداد این حملات نبوده اند ولی همیشه به عنوان یک نقش یاری دهنده در کمک به هکرها برای سرقت اطلاعات و ارسال بدافزار بوده است.

تنها وب سرور یا وبسایت مسئول این حملات نبوده اند . آسیب پذیری های موجود در مرورگر کاربران نیز نقش مهمی داشته است. یک مثال خوب حمله آرورا (Aurora) بود که در سازمان های بزرگ زیادی مثل گوگل , ادوبی , یاهو و ... انجام شد. مهاجمین یک آسیب پذیری ساعت صفر Heap Spray را در مرورگر اینترنت اکسپلورر بکارگیری کردند تا به سیستم های سازمان و دیوایس های کاربران نهایی دسترسی پیدا کنند . در این مورد خاص آسیب پذیری مرورگر وب یک فاکتور کلیدی به شمار می رفت.

دلیل دیگر آسیب پذیر بودن اپلیکیشن های وب به حملات این است که پالیسی های امنیت فناوری اطلاعات به صورت واکنشی عمل می کنند در صورتیکه باید به صورت فعال عمل کنند . هرچند که امنیت در حال حرکت به سمت نقطه ایده آل خود می باشد ولی هنوز فاصله زیادی با حالت ایده آل مورد نظر دارد. یک کارمند ناراضی یا یک هکر قبل از اجرای حملات یا سرقت اطلاعات , پالیسی های واکنشی شما را مطالعه نمی کند! پس ایجاد مستندات واقعا خیلی موثر و یاری دهنده نیست.

سیستم های تشخیص و جلوگیری از نفوذ و فایروال ها با حملات جدید نمی توانند مقابله کنند! استفاده از دیوایس های شخصی کارکنان درون سازمان BYOD بسیار افزایش یافته و همین موضوع منجر به افزایش سطح حملات شده و موجب بروز مشکلات زیادی برای تیم امنیتی شده است. هرچند این کارمندان سازمان هستند که می مانند و ما بایستی به عنوان تیم امنیتی خود را با آنها سازگار کنیم.

اینترنت شاهد بروز وبسایت ها و اشخاصی (Script Kiddies) شده که هیچ دانشی از علم امنیت ندارند و تنها با ابزارهای ساده ای آشنایی دارند که بعضا آنها را خریداری کرده و شروع به انجام حملات می کنند.

توسعه تعداد بیشمار وبسایت ها و ارایه راهکارهای جدید وب همگی موجب ایجاد مشکلات جدید امنیتی می شوند . چرا که هرچه تکنولوژی گسترده تر شود بایستی به تناسب آن امنیت نیز رشد کند ولی متاسفانه هرگز اینگونه نیست.

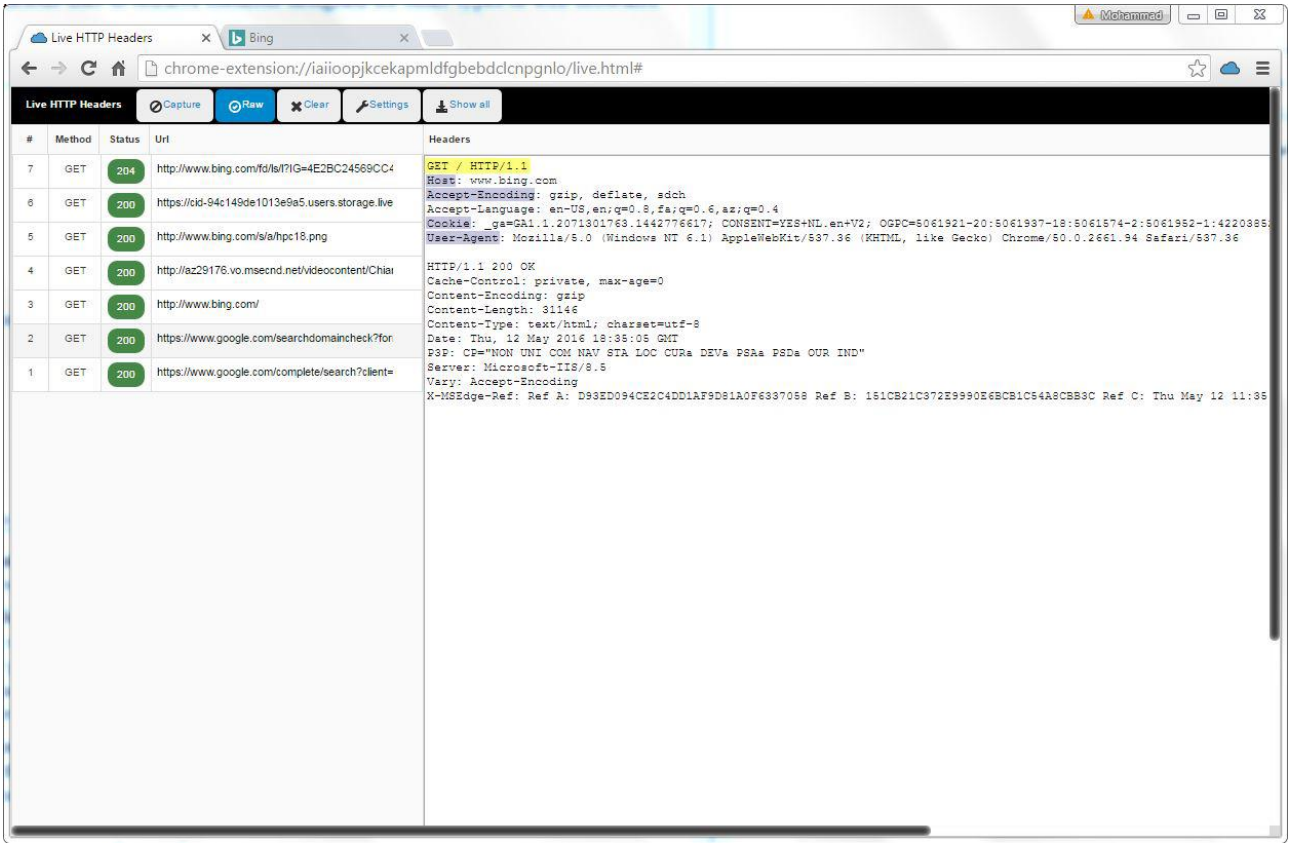
سرمایه گذاری های کم و حتی عدم سرمایه گذاری در بازبینی کد و پیدا کردن باگ ها , عدم درک اهمیت رمزنگاری داده ها بر روی شبکه و ... همگی مشکلات زیادی را بوجود آورده اند .

اگر به دو مورد از رایج ترین انواع حملات اپلیکیشن های وب دقت کنیم , می بینیم که تزریق اسکیوال (SQL Injection) و حملات اسکریپت نویسی بین سایتی (XSS) موجب شده که ورودی کاربران به درستی بکارگرفته نشود. به همین منظور شما بایستی اپلیکیشن های خود را با راهکارهای فعالانه تری تست کنید . در طی فاز تست , می توانید از ورودی های مختلفی که یک هکر ممکن است بکارگیری کند استفاده کنید. این ورودی ها از طریق فرم های ثبت نام یا ورود به سمت سرور ارسال می شوند .

این رویکرد خیلی بهتری است تا اینکه صبر کنید و منتظر مانده تا یک نفر اپلیکیشن شما را بکارگیری کند و به آن نفوذ کند و تازه به فکر ایمن سازی آن باشید. سیستم های جلوگیری از نفوذ و فایروال ها هرگز آنقدر هوشمند نیستند که بتوانند این نوع حملات را مانع شوند. اصلا به این منظور طراحی نشده اند. شما بایستی اپلیکیشن های خود را درست به نحوی تست کنید که هکر این کار را انجام می دهد.

هدر درخواست

تصویر زیر با استفاده از افزونه Live HTTP Headers گرفته شده است . همانطور که در تصویر مشاهده می کنید , درخواست از سمت کلاینت و با استفاده از متد GET به وبسایت www.bing.com فرستاده شده است. خط اول متد استفاده شده را نمایش می دهد . در این مثال ما از متد GET به منظور دسترسی به روت وبسایت که با علامت "/" مشخص شده استفاده می کنیم . نسخه HTTP استفاده شده نیز HTTP/1.1 می باشد.



فیلدهای زیادی مشخص شده است ولی ما درباره موارد مهم گفتگو می کنیم :

میزبان (HOST) : این فیلد در هدر جای دارد و به منظور شناسایی وبسایت از طریق نام میزبان (در صورتیکه از آدرس آیپی اشتراکی استفاده می کنند) کاربرد دارد .

همچنین مرورگر وب کلاینت رشته ای تحت عنوان user-agent را تنظیم می کند که به منظور شناسایی نوع و نسخه مرورگر کاربر , کاربرد دارد.

عامل کاربر (User-Agent) : این فیلد توسط مرورگر به مقادیر پیش فرض تنظیم می گردد ولی توسط کاربر نهایی می تواند جعل شود . این کار معمولا توسط کاربران مخرب به منظور دریافت محتویات از سایت ها (که محتویات مورد نظر را فقط برای مرورگر خاصی در نظر گرفته اند) انجام می شود.

کوکی (Cookie) : این فیلد یک مقدار موقتی اشتراکی بین کاربر و سرور را برای مدیریت نشست ذخیره می کند.

ارجاع (Referer) : این فیلد مهم دیگری است و در صورتیکه از وبسایت یا URL دیگری به سایت مقصد هدایت شده باشید آن را خواهید دید. در واقع این فیلد حاوی آدرس سایت قبلی (سایت ارجاع) یا سایتی با کلیک بر روی لینک از آن به سایت هدف رسیدیم می باشد. هکرها این فیلد را در حملات XSS دستکاری کرده و کاربر را به وبسایت های مخرب هدایت می کنند.

کدگذاری مورد پذیرش (Accept-Encoding) : این فیلد طرح فشرده سازی پشتیبانی شده توسط کلاینت را تعریف می کند . gzip و Deflate رایج ترین این الگوها هستند . فیلدهای زیاد دیگری نیز وجود دارند ولی فیلدهای دیگر کاربرد کمی برای تسترها دارد.

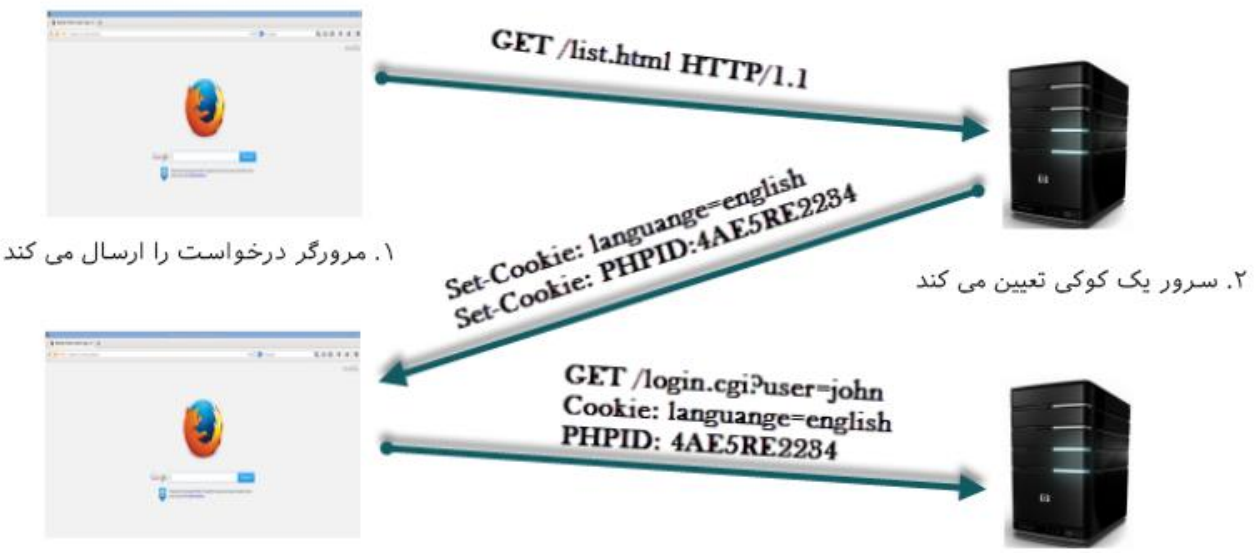
جریان کوکی بین سرور و کلاینت

همانطور که در شکل زیر نمایش داده شده است کوکی همیشه توسط سرور کنترل و تنظیم می شود. مرورگر وب تنها مسئول ارسال آن در سمت سرور می باشد . در تصویر زیر می بینیم که یک درخواست GET به سرور ارسال می شود و اپلیکیشن وب بر روی سرور کوکی را برای شناسایی کاربر و تعیین زبان انتخاب شده توسط وی تعیین می کند :

در مرحله اول کاربر یک درخواست GET به سرور ارسال می کند.

در مرحله دوم سرور بر اساس نوع و محتویات موجود در هدر درخواست نوع زبان و کوکی مربوط به نشست را تعیین می کند.

از این به بعد هر درخواستی که توسط کلاینت به سرور ارسال شود حاوی کوکی تعیین شده می باشد.



۱. مرورگر درخواست را ارسال می کند

۲. سرور یک کوکی تعیین می کند

۳. مرورگر کوکی را در درخواست های بعدی ارسال می کند

نصب آزمایشگاه خود با کالی لینوکس

آماده سازی کلید همه کارهاست . این کار در تست نفوذ از اهمیت بالایی برخوردار است چرا که شما در حین انجام تست نفوذ دارای مدت زمان محدودی به منظور انجام فرآیندهای شناسایی , اسکن , بکارگیری و درنهایت ارایه گزارش به مشتری هستید . هر تست نفوذی که پیاده سازی می کنید در ماهیت و طبیعت خود متفاوت است و نیازمند رویکرد خاصی است. ابزارها در فرآیند تست نفوذ نقش کلیدی ایفا می کنند و به این منظور شما بایستی از قبل جعبه ابزار خود را آماده کرده باشید و علاوه بر این تجربه کافی استفاده از این ابزارها را داشته باشد .

در این فصل به توضیح عناوین زیر می پردازیم :

- مروری بر کالی لینوکس و تغییرات اعمال شده از نسخه قبلی
- راههای مختلف نصب سیستم عامل کالی لینوکس
- مقایسه مجازی سازی با نصب بر روی سخت افزار فیزیکی
- مرور و پیکربندی ابزارهای مهم در کالی لینوکس
- نصب تور و پیکربندی آن

انتشار ثابت در مقایسه با انتشار رولینگ

انتشار رولینگ (Rolling) یا همان غلتان بهتر است یا انتشار ثابت (Fixed) ؟ کدامیک از شیوه های انتشار توزیع لینوکس را ترجیح می دهید ؟

انتشار غلتان یا همان انتشار رولینگ (Rolling Release) یکی از شیوه های انتشار و توزیع لینوکس می باشد که مداوم به روزرسانی می شود. ایده کار این است توسعه دهندگان به نحوی عمل کنند که تا جای ممکن جدیدترین و بروزرسانی ها و پچ های ایجاد شده در اختیار کاربران مصرف کننده قرار گیرد.

راههای زیادی به منظور انجام این کار وجود دارد.

یک شیوه راهی است که Arch Linux انتخاب کرده که به موجب آن بروزرسانی های کوچک ولی مدام در اختیار کاربران قرار گیرد. راه دیگر رویکردی است که به موجب آن یک فایل ایمیج قدیمی با نسخه های جدیدتر جایگزین شده تا تغییرات نرم افزاری در اختیار کاربران قرار گیرد. این رویکرد را Ubuntu Core برگزیده است.

در شرایطی که رولینگ ریلیز روز به روز رایج تر می شود ولی بهتر است بدانید که استفاده از آن چیز جدیدی نیست. یکی از قدیمی ترین توزیع های فعال لینوکس یعنی Gentoo Linux که والد Chrome OS نیز به شمار می رود 15 سال قبل این رویکرد را انتخاب کرد.

مدل انتشار ثابت (Fixed Release) مدلی است که اکثر ما می شناسیم که توسط کمپانی Canonical برای توزیع اوبونتو و توسط کمپانی Red Hat برای توزیع RHEL استفاده می شود. در انتشار ثابت , توزیع های اصلی بر اساس برنامه از قبل تعیین شده منتشر می گردد که به موجب آن پچ های امنیتی و بروزرسانی های کوچک نیز انجام می شود.

هر کدام از این روش ها مزایا و معایب خودشان را دارند. برای مثال در شیوه انتشار رولینگ , باگ های بزرگ ممکن است در یک سیستم تجاری نمایان شود ! از طرف دیگر در انتشار ثابت به منظور انجام بهینه سازی های اساسی بایستی ماهها و حتی سال ها منتظر ماند تا در یک نسخه ثابت عرضه شود.

به نظر شما کدام مدل برای توزیع کالی لینوکس مناسب تر است ؟ آیا انتخاب شیوه انتشار رولینگ توسط کالی رویکرد مناسبی است ؟

Burp Proxy و وبسایت های مبتنی بر SSL

پروکسی Burp در وب سایت های مبتنی بر SSL نیز کار می کند . به منظور رمزگشایی , پروکسی اتصال را رهگیری کرده و خود را به جای وب سرور معرفی کرده و یک گواهینامه که با CA خود امضا شده ایجاد می کند.

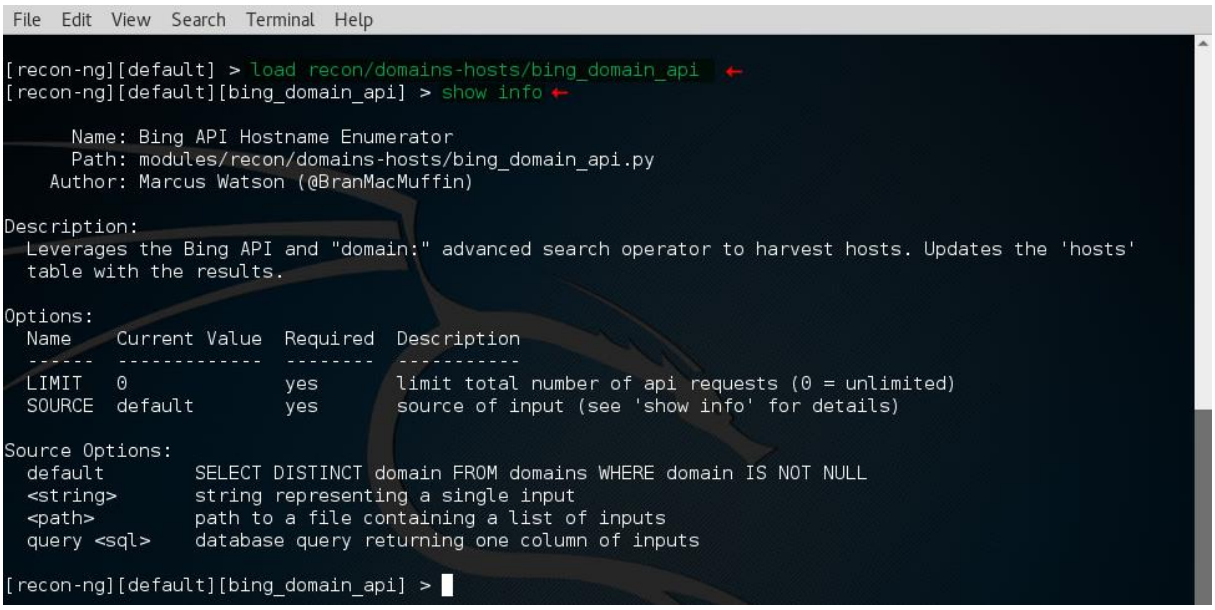
این شروع کار است. پروکسی خود را در مقابل گواهینامه SSL واقعی وبسایت به عنوان کاربر معرفی کرده و درخواست رسیده از وبسایت را با گواهینامه فراهم شده توسط وبسایت رمزنگاری می کند . سپس اتصال از وبسایت در محل پروکسی قطع می شود . پروکسی داده ها را رمزگشایی کرده و این بار آنها را با گواهینامه ایجاد شده توسط خود (در ابتدای کار) رمزنگاری می کند تا در مرورگر کاربر نمایش داده شود . دیاگرام زیر مسیر جریان این فرایند را بسیار ساده تر توضیح می دهد :

سرشماری نام دامنه با استفاده از Recon-ng

جمع آوری اطلاعات درباره زیردامنه های وبسایت هدف به شما کمک خواهد کرد تا محتویات و ویژگی های وبسایت را شناسایی کنید. هر محصول یا سرویس ارایه شده توسط سازمان هدف شما ممکن است زیردامنه اختصاصی خود را داشته باشد. این موضوع به شما کمک کرده تا محتوای گوناگون را به شیوه ای منسجم سازماندهی کنید. با شناسایی زیردامنه های مختلف , خواهید توانست تا یک نقشه سایت و فلوچارت از بخش های مختلفی که سایت هدف را به هم متصل می کنند ایجاد کنید.

سرشماری سطح پایین و سطح بالا دامنه

با استفاده از ماژول سرشماری نام میزبان بینگ می توانید زیردامنه های دیگر سایت اینستاگرام را بدست آورید. به این منظور ابتدا با استفاده از دستور `load` ماژول مورد نظر خود را بارگذاری کنید. سپس دستور `show info` را وارد کرده تا اطلاعات توضیحی ماژول نمایش داده شود.



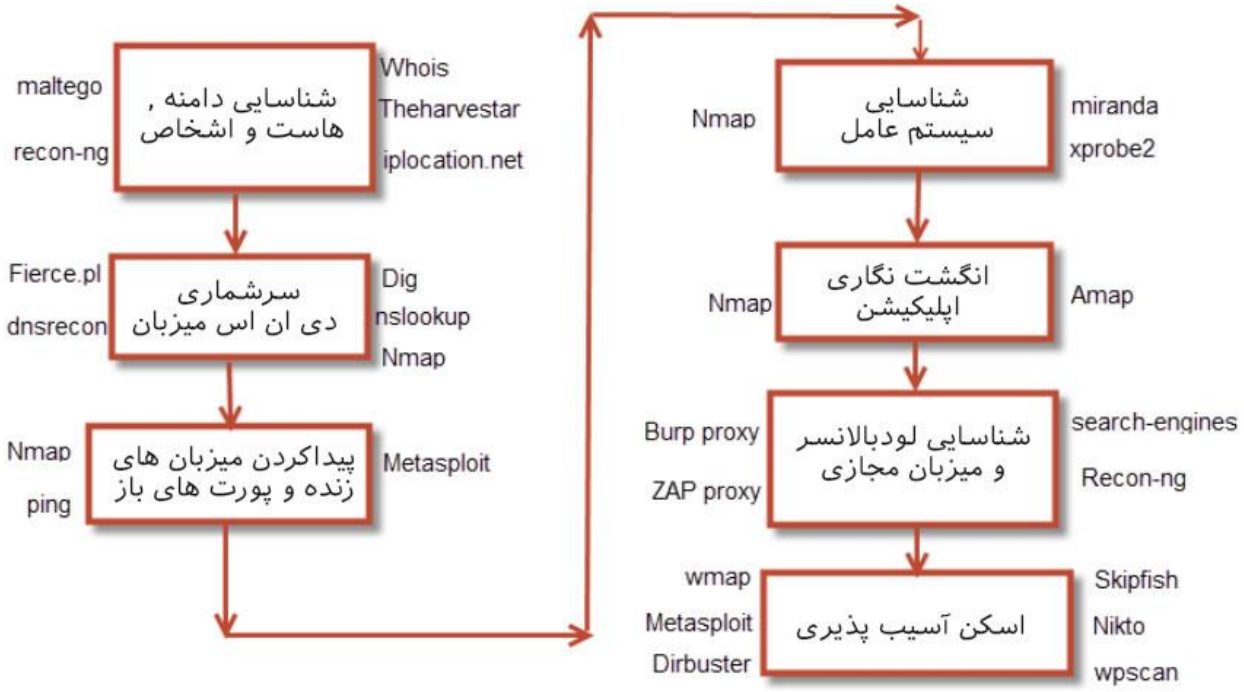
گام بعدی این است که دامنه هدف را در گزینه SOURCE تعیین کنید که ما در اینجا سایت Instagram.com را به عنوان هدف خود اضافه می کنیم.

اسکنر Whatweb

هدف اصلی ابزار Whatweb شناسایی تکنولوژی های مختلف بکار رفته در وبسایت ها می باشد. این ابزار به صورت پیش فرض درون کالی لینوکس و بک باکس موجود است . درون کالی لینوکس کافی است از منو Applications به مسیر زیر رفته تا به این ابزار دسترسی پیدا کنید :

Applications > Web Application Analysis > Web Vulnerability scanners

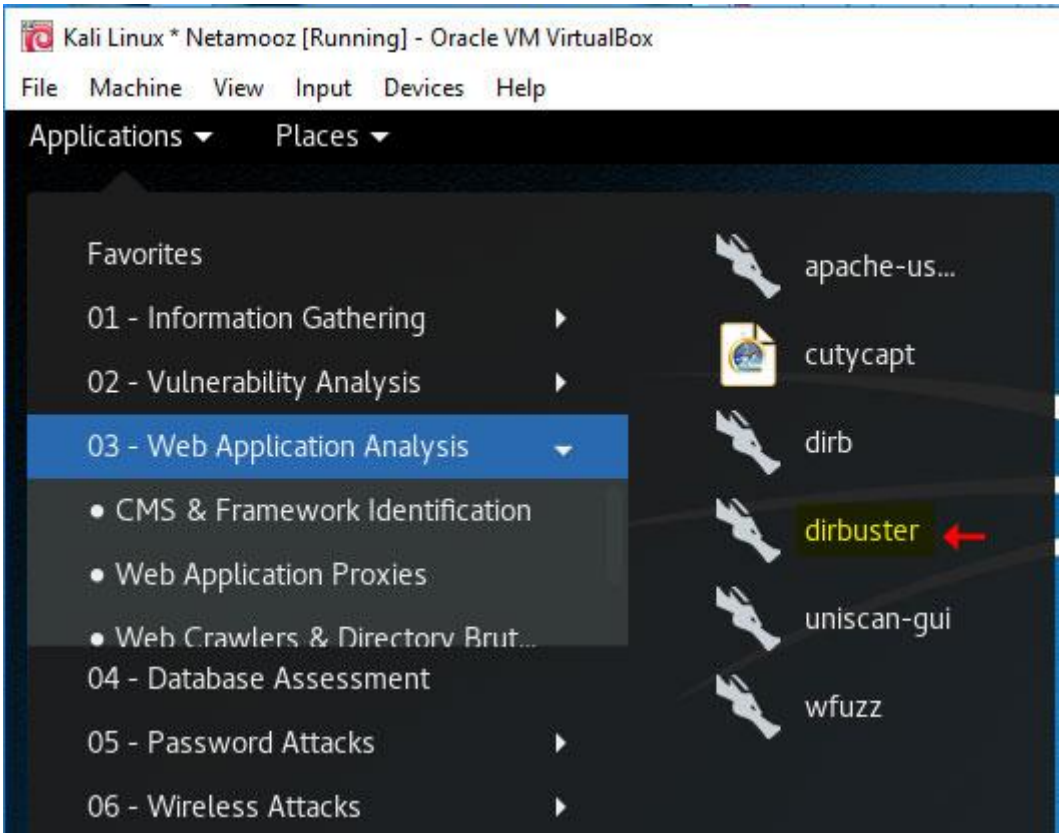
به پایان این فصل رسیدیم . تا اینجای کار فاز شناسایی را با اسکن وب سرور به پایان رساندیم. در تصور زیر برخی از ابزارهای مفید در کالی لینوکس که در این فاز استفاده می شوند را مشاهده می کنید :



مرور شاخه ها با ابزار DirBuster

یکی از ابزارهای رایج به منظور اسکن وب سرورها به منظور امکان وجود نقص مرور شاخه ها ابزار DirBuster می باشد. این ابزار در ابتدا تحت پروژه OWASP منتشر گردید ولی هم اکنون به عنوان افزونه ای برای ابزار WebScarab Proxy سرویس دهی می کند. هرچند درون کالی لینوکس 2 شما هنوز هم می توانید آن را به عنوان یک ابزار مستقل استفاده کنید. به این منظور کافی است تا از منو اصلی کالی لینوکس به مسیر زیر رفته :

Applications > Web Application Analysis > Web crawlers & Directory Bruteforcing



ابزار هایدرا

هایدرا ابزاری قوی و با قابلیت سفارشی سازی بالا می باشد که به صورت پیش فرض درون کالی لینوکس و بک باکس موجود است. با استفاده از ابزار هایدرا می توان انواع مختلف احرازهویت را بروت فورس کرد

ابزار هایدرا قادر به تست پروتکل های مختلفی همچون , POP3 , HTTP , SSHv2 , SMB و RDP می باشد. فرایند کار به این شکل است که شما به ابزار مجموعه ای از نام های کاربری و پسوردهای موجود و یکسری پارمترهای اختصاصی را می دهید و هایدرا بقیه کار را به صورت خودکار انجام می دهد. در کتاب مقدمات تست نفوذ وب به صورت مفصل درباره شیوه انجام حملات بروت

فورس مبتنی بر فرم گفتگو کردیم . در اینجا به اختصار به نحوه پیاده سازی این حملات اشاره می کنیم. ساختار کلی دستور به صورت زیر می باشد :

```
hydra 192.168.1.8 .....
```

هایدرا ابزار بسیار انعطاف پذیری است و دارای گزینه های کاربردی زیادی می باشد . برای انجام موفقیت آمیز یک حمله بروت فورس بنا به نوع حمله به برخی از اطلاعات زیر نیاز داریم :

آدرس میزبان : در اینجا مقدار `192.168.1.8` می باشد ولی هر آدرس سایت دیگری مثلا `netamooz.net` را می توانید بکار ببرید.

متد : در اینجا متد مورد نظر ما `http-form-post` می باشد چرا که هدف ما احرازهویت مبتنی بر فرم می باشد ولی می توان متدهای دیگر را استفاده کرد مثلا برای حملات ایمیل `smtp`

تزریق دستور مبتنی برخطا و نابینا Blind Command Injection

زمانیکه یک دستور را به دنبال پارامتر ورودی ارسال می کنید و خروجی دستور در مرورگر نمایش داده می شود , شناسایی آسیب پذیر بودن اپلیکیشن وب نسبت به تزریق دستور بسیار ساده است. خروجی ممکن است در قالب یک خطا و یا حتی نتایج واقعی دستور اجرا شده بر روی وب سرور باشد. به عنوان یک هکر در ادامه کار شما می توانید بنا به شرایط دستورهای اضافی را برای شل ایجاد و ارسال کنید. زمانی که خروجی حاصل از اجرای دستور در وب سرور ,

درون مرورگر نمایش داده می شود به آن آسیب پذیری مبتنی بر خطا یا تزریق دستور بینا (Non-Blind Command Injection) می باشد.

نوع دیگر تزریق دستور نابینا می باشد (Blind Command Injection) و خروجی حاصل از اجرای دستورها بر روی وب سرور به کاربر درون مرورگر نمایش داده نمی شود و هیچ پیام خطایی بازگشت داده نمی شود.

هکر بایستی از دیگر راهها به منظور تشخیص اجرای موفقیت آمیز دستور خود بر روی وب سرور استفاده کند. زمانی که خروجی دستور به کاربر نمایش داده می شود بنا به شرایط می توانید از دستورهای بش یا خط فرمان ویندوز همچون `dir` , `ls` , `ps` , `tasklist` استفاده کنید. ولی زمانیکه تزریق نابینا انجام می شود بایستی دستورهای خود را با دقت انتخاب کنید. به عنوان یک هکر قانونمند , مطمئن ترین و ایمن ترین راه برای شناسایی وجود ضعف تزریق (در زمانیکه اپلیکیشن به شما خروجی نمی دهد) استفاده از دستور `ping` می باشد.

شل PHP و متااسپلوییت

در اینجا می خواهیم نحوه بکارگیری یک آسیب تزریق دستور در یک برنامه ساخته شده با PHP را با استفاده از ابزار قدرتمند متااسپلوییت نمایش دهیم. به این منظور بایستی گام های زیر انجام شود :

1. ایجاد شل PHP با استفاده از ابزار msfvenom

2. آپلود شل درون وب سروری که دسترسی به آن از سیستم هدف امکان پذیر باشد.

3. نصب یک نشست مترپرتر TCP در متااسپلوییت که منتظر اتصال سیستم هدف بماند

عملگر یونیون UNION

به منظور تست فیلدهای ورودی برای آسیب تزریق اسکیوال , یکی از مفیدترین عبارات اسکیوال عملگر UNION می باشد. گفتیم که از متاکاراکتر ویرگول نقطه می توانید استفاده کنید ولی بیشتر برنامه ها آن را بلاک کرده در نتیجه کوئری شما با شکست مواجه خواهد شد.

تست پیکربندی SSL با انمپ

ابزار انمپ دارای اسکریپتی با نام ssl-enum-ciphers می باشد که توانایی شناسایی سوییت های سایفر پشتیبانی شده توسط سرور را دارد و همچنین این ابزار می تواند اهداف را بر اساس قدرت رمزنگاری را دارد. این اسکریپت چندین

اتصال را با استفاده از TLS 1.2 , SSLv3 و TLS 1.2 را دارد. اسکریپت همچنین در صورت وجود آسیب پذیری POODLE یا CRIME آن را برجسته می

حمله فیشینگ
SpearPhishing Attack

زیرمنو شماره یک با نام Spear-Phishing Attack Vectors به شما اجازه می دهد تا ایمیل های سفارشی را بر روی قربانی های خاص پیاده سازی و اجرا کنید. هدف اصلی این ماژول یکپارچه سازی یک پیلود به صورت یک فایل پیوست درون ایمیل و ارسال آن از طریق ایمیل به قربانی هدف می باشد.

برای شروع زیر منو شماره 1 .....

این تنها یک نسخه نمایشی از کتاب تست نفوذ وب با کالی لینوکس میباشد . نسخه اصلی را می توانید از اینجا دریافت کنید.

http://netamooz.net/product/web-penetration-with-kali-linux/