Cyber Security Study Material

خلاصه‌ای از ویدیو آشنایی با مسیر ورود به دنیای امنیت سایبری

ویدیو: حمید کشفی

- راه های ارتباطی با ایشان:
- توییتر
- یوتیوب
- فهرست منابع معرفی شد: گیت هاب

نویسنده: عرفان

توییتر

تلگرام

Contents فهرست مطالب

پیشگفتار

این مطلب خلاصه‌ای از ویدیو آشنایی با مسیر ورود به دنیای امنیت سایبری هست. این ویدیو، نسخه‌ی ضبط شده از لایو آقای **حمید کشفی**، متخصص و مشاور امنیت سایبری است. ایشون با سابقه‌ی ۲۰ ساله خود در این حوزه، منابع مفید و مورد نیاز رو با ما در اشتراک گذاشتند و از تجربیات خودشون برامون گفتند.

اگر هیچ ایده‌ای از دنیای امنیت کامپیوترها ندارید، یا مطالبی به گوش‌تون خورده،جای درستی اومدید. توصیه میشه حتی اگر این خلاصه رو میخونید، ویدیوی یوتیوب رو هم نگاه کنید(سعی کردم هر بخش رو زمان بندیش رو بنویسم، به کامنت ها مراجعه کنید)

برای ورود حوزه‌ی امنیت سایبری، به دلیل پیچیدگی هایی که وجود داره، شما به یک برنامه‌ی مشخص و دقیق نیاز دارید تا بتونید پله پله پیشرفت کنید و دانش خودتون رو افزایش بدید.

آقای کشفی تاکید کردند مسیر حرفه‌ای ورود به این حوزه، با ترتیبی که توضیح دادند انجام میشه.

من سعی کردم هر نکته‌ی مهمی رو که آقای کشفی داخل ویدیو دربارش توضیح دادند رو اینجا بنویسم.

دقت کنید تمامی متن های آبی رنگ، لینک هستند و شما رو به مطلب اشاره شده منتقل می‌کنند.

ترتیب محتوای این متن خلاصه شده بر اساس ویدیو هست.

امیدوارم مفید واقع بشه و نگاه شما رو به دنیای هک و امنیت باز کنه.

پیشنیازهای کلی و مهارت‌های نرم

فارغ از اینکه توی چه شاخه‌ای از امنیت سایبری قصد دارید فعالیت کنید، لازمه بدونید یاد گرفتن این مطالب ممکنه **الان** به نظر بی فایده باشد و به کار نیاد، ولی در آینده و طولانی مدت، داخل کار (تست نرم افزار، باگ بانتی و ...) به کار میاد.

لزومی نداره همه این نکات رو 0 و 1 قبول کنید و انجام بدید، اما طبق تجربه در بلند مدت، به این نتیجه میرسیم که بهتره این منابع رو کار کنید، تا بعدا پشیمون نشید.
اگر علاقه دارید که وارد امنیت بشید و به نتیجه برسید، باید این موضوع رو درک کنید که تا چندین ماه مطالبی که میخونید هیچ ربطی به امنیت و security ندارن (حداقل ۴ ماه اول)

دو مورد مهم برای شروع فعالیت در امنیت :

۱- دانش زبان انگلیسی (در حد خواندن مقاله و کتاب)
۲- زمان گذاشتن و نظم در مطالعه

- اگر توانایی خواندن یک پاراگراف از کتاب رو ندارید و نمیتونید درصد بالایی از مطلب رو متوجه بشید، توصیه میشه اول زبان انگلیسی‌تون رو تقویت کنید(کلاس برید و تمرین کنید).
خواندن اولین کتاب ممکنه به نظر سخت باشه، اما به مرور و با تمرین نکات و کلماتی که خوندید، زبان تون تقویت میشه و کتاب های بعدی رو راحت تر متوجه می‌شوید.

- از شما انتظار میره که با مطالعه این منابع و کتاب‌ها، مفاهیم رو به خوبی یاد گرفته باشید.
- نکته ای که هست، اینه که شما اگر قصد دارید به هدف تون در این حوزه برسید، باید روزانه به صورت مداوم ۲ تا ۳ ساعت مطالعه مفید داشته باشید. مطالعه مفید یعنی اگر ۶ ساعت کتاب میخونید و پشت کامپیوتر میشینید، باید چکیده اون ۶ ساعت حداقل ۳ ساعت درک مفهوم اون مطلب باشه. در ابتدا این کار رو باید ۳ ماه منظم و مداوم انجام بدید.

*نکته: اگر دانش زبانی تون خوب نیست و نمیتونید به صورت روزانه مطالعه کنید، بهتره وارد این حوزه فعلا نشید و ابتدا روی این دو مهارت تمرین کنید. وقفه انداختن بین مطالعه باعث فرار مفاهیم میشه. *پیوستگی در مطالعه بسیار مهمه*.
این موضوع رو هم در نظر بگیرید، که بهتره از اول کار ساعت های که صرف خوندن و تمرین می‌کنید رو محاسبه کنید تا مسیر پیشرفت خودتون رو ببینید و هفته به هفته خودتون رو تحلیل کنید.

یادداشت برداری

قراره حجم زیادی از دیتا و اطلاعات وارد مغز شما بشه. به همین دلیل نیاز دارید یک روش یا مکانیزم برای یادداشت برداری مطالب داشته باشید.
یادداشت برداری باید بصورت منظم و دقیق باشه، صرفا نوشتن روی یک کاغذ بدون رعایت ترتیب و ساختار بیهوده است. در آینده قراره از این یادداشت ها استفاده کنید.
نرم افزارهای که می‌تونید برای نوت برداری ازشون استفاده کنید زیاد هستند. چندتاشون رو اینجا مینویسم:

- Notion
- Obsidian
- xmind

نرم افزار notion آنلاین هست و قابلیت sync شدن موبایل و کامپیوتر رو داره.
برنامه obsidian این قابلیت رو نداره، ولی برای لینک کردن مطالب و ساده نویسی خیلی به کار میاد.
از هر دو هم میتونید به صورت همزمان استفاده کنید.

نگارش حرفه ای (هم به فارسی و هم انگلیسی) بسیار اهمیت داره. توانایی درست نوشتن و رعایت قوانین نگارشی، هنگام نوشتن گزارش برای شرکت ها به کار میاد. به همین دلیل باید تمرین کنید فنی بنویسید، و تلاش کنید نوت هایی که بر میدارید یک چارچوب منظم داشته باشند و به ترتیب اولویت باشند. مقاله نوشتن هم در آینده می تونه کمک کننده باشه.

مرور کلی هر شاخه

داستان از این قراره که شما در هر زمینه‌ای از امنیت که میخواهید فعالیت کنید، در نهایت به معلومات پایه نیاز پیدا می‌کنید. پس بهتره که همین اول مطالب پایه رو یاد بگیرید.

- OS & Network

شبکه و سیستم عامل شالوده‌ای برای شروع مسیر هستند.
در ابتدا شما باید یک سیستم عامل رو بشناسید و اجزای اون رو بدونید. شما باید بتونید مثل یک مدیر سیستم از آن استفاده کنید.

- Programming & Scripting

برای کار کردن در زمینه‌ی امنیت، باید توانایی خواندن و تحلیل کد رو داشته باشید. برای استفاده از ابزارهایی که قرار هست در آینده به کار بگیرید به این دانش نیاز دارید(بدونید پشت صحنه چه اتفاقی داره میوفته و چه کد و منطقی در جریانه) . دقت کنید برای پیاده سازی برنامه ها و اسکریپت نویسی (scripting) هم لازمه این مهارت رو بدونید. اگر اسکریپت نویسی رو بلد نباشید مثل مکانیکی هستید که جعبه ابزار نداره و وسایلش ناقصه. حتی اگر باگ بانتی (bug bounty) بخواید کار کنید لازمه که این دو مهارت رو بلد باشید.

- Basic Hacking/ Pentest/ Exploitation

هدف از خوندن کتاب ها و منابع این بخش اینه که شما یک نگاه کلی به دنیای هک و زیر شاخه های مختلف داشته باشید. در این مرحله هدف این نیست که شما متخصص بشید، بلکه اینه که خیلی از مطالب قبل رو کاربردشون رو متوجه بشید و با cyber security بیشتر آشنا بشید.

Network and VoIP -

هدف از مطالعه این بخش هم اینه که شما با شاخه های جدیدی از امنیت شبکه های کامپیوتری به صورت تخصصی آشنا بشید(دقیقا مثل بخش قبلی)

Web application security-

در این قسمت به این موضوع می‌پردازیم که چطوری امنیت وب اپلیکیشن ها یعنی چی .
زمانی مطالعه این منابع این بخش مفید هست که شما دید برنامه‌نویسی داشته باشید و با نحوه پیاده سازی سایت ها و اپلیکیشن ها آشنا باشید.

mobile application security-

امنیت برنامه های موبایل بسیار شبیه به وب هست، به همین دلیل این بخش بعد از مطالعه وب قرار می‌گیره.

code auditing-

این بخش مربوط به بررسی باگ ها و آسیب پذیری های امنیتی در هر زبان برنامه‌نویسیه.
طبیعتا پیش نیاز این بخش برنامه‌نویسی است. همینطور به دلیل پیچیدگی بالا نیازمند درک خوبی از برنامه‌نویسی و باگ کلاس های مختلف هست.

Reversing-

یکی از زیر شاخه های پیچیده‌ی امنیت که نیازمند داشتن دانش بسیار خوبی از برنامه‌نویسی و code auditing هست. (در واقع شما با ورود به این زمینه متوجه می‌شید که علاوه بر شاخه های قبلی، باید مطالب جدید تری رو یاد بگیرید)
- به همین ترتیب شما بخواهید وارد زمینه های cryptography ، fuzzing ، malware analysis هم بشید نیاز دارید درک خوبی از برنامه‌نویسی، شبکه، تحلیل سورس کد و باینری داشته باشید.

جزئیات هر کدوم از این زیر شاخه ها رو در ادامه می‌بینید.

سیستم عامل و شبکه

قبل از شروع این فصل، این نکته رو در نظر داشته باشید که حتی اگر شما پیش زمینه ای از شبکه و سیستم عامل دارید، باز هم توصیه می‌شه کتاب ها و منابع این بخش رو مطالعه و تمرین کنید.
این کار باعث میشه شما مطالبی که در اون ضعف دارید رو تقویت کنید و مفاهیم رو با دقت بیشتری درک کنید. (این موضوع شامل برنامه‌نویسی هم میشه)

از شما به عنوان متخصص security انتظار میره، که حداقل دو تا سیستم عامل رو بدونید: لینوکس و ویندوز

" کتاب های این بخش کلفت و قطور هستند، و این موضوع بی دلیل نیست (:
حجم زیاد این کتاب ها به این دلیل است که شما بتونید مطالب رو بصورت عمقی یاد بگیرید و مشکلات امنیتی رو به خوبی فرا بگیرید."
کسی که مطالب پایه رو ندونه، بعدا پیشرفت نمی‌کنه و نتیجه‌ی خوبی نمی‌گیره. اگر قراره که در این زمنیه طولانی مدت فعالیت کنید، لازمه که مباحث پایه و اساسی رو بلد باشید.
افرادی که مباحث پایه مثل برنامه‌نویسی، سیستم عامل و شبکه رو عمیق مطالعه نکردن و صرفا رفع تکلیف کردن، با تفکر بر این که باگ های سطحی رو میتونن گزارش بدن و در قبالش پاداش بگیرن وارد این حوزه میشن. غافل از اینکه دقیقا همین کار رو آدم های دیگه هم انجام میدن.
این افراد همه برای پیدا کردن باگ های عمیق و مفهومی شکست می‌خورند.

بر می‌گردیم به سیستم عامل و شبکه:
دوره Lpic 1 برای لینوکس پیشنهاد میشه (داخل ریپازیتوری گیت هاب که ابتدای این فایل قرار داده شد میتونید لینک دوره رو پیدا کنید).

- از شما انتظار میره که لینوکس رو در حد محتوای این دوره بلد باشید.
- کتاب Linux Bible هم به عنوان کتاب منبع (reference book) پیشنهاد میشه.

برای شروع شبکه کتاب + Network پیشنهاد میشه. این کتاب رو باید خط به خط بخونید و برای درک بهتر، تمرین های آخر هر درس رو حل کنید و خودتون رو محک بزنید.
می‌تونید مطالبی که کمتر مرتبط هستند، با درک خودتون مطالعه نکنید (مثل مباحث فیزیکی و سیم کشی کابل ها)

کتاب های مرتبط با ویندوز / MCSA

- خواندن کتاب های ویندوز، به این دلیل هست که در آینده برای گرفتن دسترسی روی سیستم های ویندوزی و استفاده از آسیب پذیری ها نیاز دارید که ویندوز رو کار کنید.
- می‌تونید ویندوز رو در کنار لینوکس کار کنید. یا به صورت جدا مطالعه کنید.

کتاب + Security

این کتاب آموزش کلی امنیت و بعضی از کلمات کلیدی و سطحی هست. هدف از مطالعه‌ی این کتاب اینه که بفهمیم چه چیزایی داخل دنیای امنیت وجود داره، چه شاخه هایی هست، چه مباحث پایه ای هست . قراره آشنا بشید چه مباحثی برای یاد گرفتن در دنیای امنیت هست(مثل روزنامه باید بخونید)

- ## شروع امنیت از باگ بانتی

باگ بانتی (bug bounty) مسیر مناسبی برای ورود به دنیای امنیت نیست.
اصل و ماهیت باگ بانتی اینه که شرکت ها، برنامه ها و نرم افزار های خودشون رو پس از رد شدن از تست های و فیلتر های امنیتی به صورت عمومی برای دیگر مهندسین امنیتی قرار میدن که باز هم مورد تست قرار بگیره. این موضوع به این معناست که شما علاوه بر اینکه همزمان با تعداد زیادی هکر و مهندس امنیتی دارید رقابت می‌کنید، باید اینقدر دانش بالایی داشته باشید که بتونید باگ های عمیق و حفره های امنیتی پیچیده تر که قبلا داخل تست های اون شرکت پیدا نشده رو کشف کنید.
بنابراین، کسی از باگ بانتی نتیجه می‌گیره که دانش پایه ای قوی داشته باشه و بتونه از اون چکیده دانش استفاده کنه .
اگر شما از طریق باگ بانتی وارد دنیای امنیت سایبری بشید، مثل اینه که از ته یک قیف شروع کنید.
حتی اگر بخواهید مشاوره امنیتی بدید، برای مثال نمی‌تونید به یک برنامه نویس خبره با ۱۵

سال سابقه توضیح بدید که چطوری کد امن بزنه، اگر درک سطحی از مباحث داشته باشید. (مثلا sql injection)
هر چقدر عمیق تر و حرفه ای تر بشید، رقابت کمتر و پیچیده تر خواهد شد. (داستان دوپلیکیت خوردن هم کمتر میشه.)
اگر هدفتون اینه که بهره‌وری مالی خوبی داشته باشید، لازمه که درک عمیق داشته باشید.
اگر درست و حساب شده وارد دنیای امنیت شده باشید، نتیجه‌ی بهتری هم خواهید داشت.
از یک باگ هانتر خوب این انتظار میره که درک خوبی از مباحث پایه داشته باشه.

چرا و چطوری کتاب بخونیم؟

- کتاب همیشه جزو منبع های دست اول است. مابقی منابع اکثرا از کتاب نشات میگیرند. به نسبت وقتی که برای مطالعه یک مبحث از طریق کتاب می‌گذارید، بیشتر از هر روش دیگری نتیجه می‌گیرید.
- ترتیب نوشتار مطالب داخل کتاب، باعث میشه که شما با مباحثی که اصلا اطلاعاتی دربارش ندارید نیز آشنا بشید.
- یکی از نکات مثبت مطالعه از طریق کتاب اینه که شما میتونید هر موضوعی رو که متوجه نشدید از طریق فهرست دنبال کنید و اون مطلب رو چند بار مطالعه کنید. (یکپارچه بودن کتاب کمک میکنه مطالب به صورت ساختار یافته ملکه‌ی ذهن شما بشه)
- هنگام خواندن کتاب، به این موضوع توجه کنید که شما باید محتوای هر فصل رو به خوبی درک کنید و به خاطر بسپارید.
- توجه کنید که نباید زمان تمام کردن یک کتاب خیلی طولانی یا خیلی سریع باشه. زمان مطالعه هر مبحث نیست به حجم محتوای اون متغیر هست. (زمان لازم رو میتونید از طریق دوره های آموزشی که برگزار میشه به دست بیاورید، کافیه تحقیق کنید.)
- انتظار میره که بین ۵۰ تا ۶۰ ساعت کتاب + Network رو تمام کنید.
- اگر می‌بینید نصف کتاب مونده و شما هنوز مطالب رو درک نکردید و تمرینات رو متوجه نشدید، یا مشکل زبان انگلیسی هست یا عدم توانایی هضم مفاهیم.
- کتاب اول شما رو آب بندی میکنه. (از نظر نوت برداری، زبان انگلیسی، خلاصه نویسی و درک و مفهوم)

Programming and Scripting

- این بخش مناسب کسانی است که می‌خواهند یک آشنایی با اسکریپت نویسی پیدا کنند.
-تاپیک های امنیتی که توی برنامه نویسی هست رو این کتاب ها (سه کتاب پایتون داخل گیت هاب) توضیح میدن. ممکنه فکر کنید که کتاب ها قدیمی باشند، اما تمرینات و موضوعاتی که داخل کتاب ها گفته میشه بسیار مفید هستند و دید خوبی به ما میدن. علاوه بر این به ما یاد میدن چطوری معلومات برنامه نویسی در security استفاده میشه.
- توصیه میشه اول یک زبان اسکریپتی (مثل Python یا Go) رو یاد بگیرید. پایتون از این نظر مهمه که زبان رایج برای ابزار نویسی و امنیت هست.
- بعد از فراگیری پایتون، میتونید با توجه به نیاز آینده یک زبان برنامه نویسی دیگه هم یاد بگیرید.
- برنامه نویسی و اسکریپت نویسی با هم تفاوت دارند. اسکریپت نویسی مثل آچار فرانسه است، اما برنامه نویسی فرق میکنه. با یادگیری مفاهیم برنامه نویسی متوجه میشید برنامه هل چطوری پیاده‌سازی میشن و چطوری میشه حفره های امنیتی شون رو کشف کرد.

-کتاب های این بخش، هر کدام با توجه به هدف شما در آینده ارزش خواندن دارند (برای مثال اگه قصد دارید ios کار کنید، می‌تونید کتاب مربوطه رو بخونید).
- زبان برنامه نویسی C، زبان مادر است. توصیه میشه فارغ از هر هدفی که دارید کتاب Effective C رو مطالعه کنید.
- اگر قصد دارید وارد حوزه‌ی web 3 و smart contract ها بشید، کتاب Black hat Rust توصیه میشه.

تحصیلات آکادمیک و امنیت

- دانشگاه رفتن برای فعالیت در حوزه امنیت سایبری لازم نیست، اما دقت کنید مدرک دانشگاهی در حوزه کامپیوتر در آینده به کار میاد و خیلی هم خوبه، اما اینطوری هم نیست که بگیم اگر کسی مدرک مرتبط نداشته باشه یا دانشگاه نرفته باشه نمیتونه وارد امنیت بشه.
- شما می‌تونید تمام مطالبی که طی دوره لیسانس (کامپیوتر) تدریس میشه رو طی ۶ ماه (طبق زمان بندی که در ابتدا گفتم) یاد بگیرید.(دروسی مثل ساختمان داده، سیستم عامل، مبانی شبکه، و غیره)
- از شما انتظار میره که مطالبی که در رشته های کامپیوتر و مهندسی نرم افزار تدریس میشه رو بدونید.
- در همین بخش برنامه‌نویسی، این رپوی گیت هاب رو دنبال کنید: computer-science

---

نکاتی که دانستن آنها مفیده:

- برای رسیدن به سطح جونیور(تازه کار- مبتدی) و مشغول به کار شدن، حداقل ۶ ماه تا ۱ سال کار نیازه.
- از بخش سیستم عامل و شبکه حداقل ۳ کتاب و از بخش برنامه نویسی حداقل ۴ کتاب باید بخونید.
- دقت کنید، در زمینه امنیت سایبری باید هر روز و مادام العمر مطلب جدید بخونید (هوش مصنوعی هم که دیگه کارو یه باره کرد).
- در بخش برنامه نویسی، تا کتاب Effective C کافیه.
- زبان اسکریپتی هر سیستم عامل رو باید بلد باشید. (bash for Linux/ powershell for windows)
- کتاب منبع (reference book) زمانی به درد بخور هست که شما یک مطلب رو مسلط هستید و قصد دارید روی یک موضوع خاص دقیق بشید. (ابتدا باید کلیات مبحث رو کار کنید و بعدا سراغ کتاب رفرنس برید)
- کتاب HTTP: The Definitive Guide بعد از بخش های OS , Networking, Programming میتونید بخونید.

- بعد از اتمام هر فصل کتاب می‌تونید مطالب، کنفرانس ها و مقاله‌های بروز تر اون فصل رو مطالعه کنید و بعد فصل بعدی رو آغاز کنید.
- شاید این موضوع رو باید ابتدای این کتابچه میگفتم، ولی این رو بدونید که علاقه از همه چیز مهمتره، پس از اون اراده و نظم و استمرار روزانه برای مطالعه اهمیت ویژه‌ای داره.
- در وهله اول باید ببینید شما میتونید از پس یک کتاب ساده‌ای مثل + Network بر بیایید یا نه. اگر نمی‌تونید هر روز مقاله های سخت و پیچیده بخونید و خودتون رو بروز نگه دارید، اگر این عشق و علاقه رو ندارید، بهتره وارد این حوزه نشید.
- هوش مصنوعی کار راه بندازه، اما استفاده از اون برای یادگیری مفاهیم به صورت عمیق مناسب نیست، چون شما مطمئن نیستید که آیا جواب درست یا کامل رو می‌گیرید یا نه. باید برای جستجوی جواب خود تحقیق کنید. این جزوی از پروسه‌ی یادگیریه.

Basic Hacking/ Pentest/ Exploitation

-کتاب های این قسمت ممکنه به روز نباشن و عمری ازشون گذشته باشه، اما دید خوبی از موضوعات مختلف و زیر شاخه های حوزه امنیت به شما نشون میده. در این بخش شما می‌تونید یک سطح اولیه و ابتدایی و قابل لمس از زیر شاخه های حوزه های امنیت رو متوجه بشید.

-توصیه میشه چند جلد ازین کتاب ها رو بخونید (حتی اگر از قبل حوزه مورد علاقتون رو پیدا کردید). ممکنه بفهمید که به یک حوزه دیگه علاقه دارید (مثلا بفهمید که به wireless hacking علاقه دارید) .
-تکنیک ها، ابزارها، مجموعه ای از اطلاعات و روش ها. کتاب های این بخش، از زمینه کاری شما در آینده ایده می‌دهد. این کتاب ها رو باید بخونید و مثال هاش رو حل کنید تا بفهمید در آینده چیکاره‌اید.
- سه کتاب اول در این بخش رو حتما بخونید.
در این کتاب ها با مباحث زیر آشنا خواهید شد :
red team, blue team, exploitation, finding bug process using binary, fuzzing, etc

- به سلیقه خودتون و با توجه به علاقتون ۳-۴ تا از کتاب های این بخش رو بخونید. میتونید فهرست هر کتاب رو بخونید و بعد انتخاب کنید که اون کتاب رو بخونید یا نه.

نکته: محتویات رزومه اول شما، ابزار های که شما توسعه دادید و مقاله هایی که داخل گیت هاب یا بلاگ خود نوشتید میتونه باشه. سعی کنید در این مسیر، چیز هایی که یاد گرفتید رو مستند کنید و خودتون رو برند کنید. (مهم نیست که سطح این مقالات یا ابزار ها پایین باشه، مهمه اینه که شما در اون زمینه دانش خوبی داشته باشید)

[یادآوری: دوستان عزیزم، توصیه میکنم این بخش و بخش برنامه نویسی رو از ویدیو هم نگاه کنید(حتی با سرعت بالا هم که شده نگاه کنید). طبیعتا تمام مثال هایی که آقای کشفی در لایو استریم گفتند رو نمیتونم همه رو اینجا بنویسم و از حوصله شما خارج است.]

Network & VoIP

این بخش مربوط به کسانی میشه که کار شبکه و SOC انجام دادند و قصد دارند مشخصا در زمینه Network Security فعالیت کنند.
ممکنه به نظر برسه کتاب های اینجا اکثرا فسیل هستند، اما حواستون باشه بیشتر پروتکل های شبکه هم همونطور کار می‌کنند که ۱۰ یا ۱۵ سال پیش کار می‌کردند!
پس همچنان خیلی ازین کتاب ها ارزش خوندن و مطالعه دارند.

-کلا کسانی که علاقه دارند در امنیت شبکه کار کنند، این بخش رو حتما نگاه کنند.

<< یه قهوه ای بخورید که بریم قسمت شیرین ماجرا (; >>

Web Application Security

شما با هر پیش زمینه ای و هر مهارتی که دارید، اگر تصمیم دارید که امنیت وب کار کنید، حتما و حتماااا باید کتاب **Web application hackers handbook** رو جلد تا جلد (به قول آقای کشفی) بخونید.

- چرا این کتاب رو بخونیم؟ چون مثل خیلی از کتاب های قبلی ایده و قالب برای کار کردن در وب اپلیکیشن رو به شما میده. علاوه بر این به شما یاد میده چطوری یک گزارش بنویسید، و اصلا پروسه تست نفوذ یک برنامه چطوریه.
- این کتاب قدم به قدم و با جزئیات، این حوزه رو براتون توضیح میده
- بعد از مطالعه هر فصل، به دنبال مقالات و مطالب به روز اون مطلب که خوندید بگردید.
- تمرینات این کتاب و portswigger academy حتما جدی بگیرید و در دنیای واقعی اون باگ یا مشکل امنیتی رو دنبال کنید و یاد بگیرید.

کتاب های بعدی رو میتونید بر حسب علاقه و نیاز مطالعه کنید.
اگر علاقتون در امنیت وب سمت کلاینت و مرورگر هست کتاب Browser Hackers Handbook پیشنهاد میشه.

کتاب JavaScript for Hackers دید عمیقی به شما میده راجع به جاوا اسکریپت و به شما در پیدا کردن باگ ها و مشکلات امنیتی سمت کلاینت کمک می‌کنه (اینو بدونید که کتاب سنگینیه اما ارزش خوندن داره).

*نکته:

شما باید:

- به اندازه یک database administrator از دیتابیس بدونید
- به اندازه یک برنامه نویس متوسط برنامه نویس بلد باشید
- به اندازه یک windows administrator از ویندوز بلد باشید
- به اندازه یک لینوکس ادمین ، تنظیمات و راه اندازی سیستم ها رو بدونید
- به اندازه یک متخصص شبکه که کارش راه اندازی روتر و سوئیچ هست به روتینگ پروتکل ها و غیره آشنا باشید (و ...)

مجموع همه‌ی اینها، از شما یک مشاور تست نفوذ و مهندس امنیت عمومی می‌سازه.
تنها در صورتی که قصد دارید در یک زیر شاخه به صورت تخصصی فعالیت کنید و عمیق بشید، می‌تونید بعضی از این زمینه ها رو رد کنید(در این مورد کار سخت تری در پیش دارید) .

-اگر اینها رو سطحی کار کرده باشید، مشاوره ها و گزارش های شما برای کشف مشکلات امنیتی هم سطحی خواهد بود.
-سختی و پیچیدگی جزو جدانشدنی از امنیت سایبری است.

Mobile Application Security

خیلی از مشکلات امنیتی که در امنیت برنامه های موبایل هست، ذات و ماهیت شون مثل وب اپلیکیشنه. این دوتا عملا مثل هم هستند. بنابراین توصیه میشه که قبلش وب کار کرده باشید.

کتاب Mobile Application Hackers Handbook برای شروع پیشنهاد میشه، بعد از اون می‌تونید بین اندروید و ios یکی رو بر اساس علاقه انتخاب کنید.

کتاب FRIDA Handbook : به شدت واجب و لازمه. برای تست موبایل اپلیکیشن، به صورت عمیق و کشف قابلیت ها و ویژگی ها اون برنامه، از فریم ورک FRIDA استفاده میشه. استفاده از این برنامه از نون شب برای امنیت کار موبایل واجب تره(بعد از کتاب اول بخونید)

سرنخ تمام مطالبی و زیر شاخه های که گفته شد رو میتونید طی دو تا سه سال یاد بگیرید (و متوجه بشید که در کدوم زمینه دوست دارید متخصص بشید) .
اما برای فعالیت در یک زمینه مثل code audit (به صورت تخصصی) باید ۲ تا ۳ سال مطالعه داشته باشید و خودتون رو به روز نگه دارید.

Code Auditing

اول از همه بگم این بخش طولانیه و مهمه، توصیه میکنم از داخل ویدیو ببینید تا بهتر متوجه داستان بشید.
لینک این قسمت (دقیق شما رو میبره سر موضوع) :
https://www.youtube.com/live/M6-ELr9FRNY?si=HBm 8kW pooNAM-L&t=14827

- اگر بخوام خیلی خیلی خلاصه از این قسمت براتون بگم، اینه که توی security برنامه نویسی دانش بسیار مهمیه که باید یاد بگیرید.
- مهارت شما در خواندن کد و کشف آسیب پذیری، از این نظر مفید ست که دیگه وابسته به CVE ها و تکنیک های عمومی که در سطح وب ریخته نیستید.
- اگر دانش source code auditing رو داشته باشید (و تجربه خوندن سورس کد) پلتفرم یا فریم ورک ها رو داشته باشید دیگه سمت مشکلات امنیتی سطح پایین رو نخواهید رفت.
- کتاب اول این بخش رو باید به عنوان کتاب مرجع استفاده کنید. کتاب دوم سبک تر و برای شروع راحت تره.
- کار شما به عنوان source code auditor اینه که حداقل ۱ یا ۲ زبان برنامه نویسی رو به سبک audit (تحلیل حرفه ای کد) بلد باشید.
- این بخش زمان بره و پیچیدگی های خاص خودش رو داره.

بیشتر ازین اگه دوست دارید بدونید، حتما ویدیو رو ببینید که بنظرم خیلی جذابه (مخصوصا آخرش که آقای کشفی توضیح میده چطوری با دانش تحلیل سورس کد و استفاده از دوتا ابزار مهم در این زمینه تونسته طی ۲ ماه ۱۵۰ تا باگ RCE از پلاگین های متن باز wordpress کشف کنه :)

Reverse Engineering

مهندسی معکوس یا reverse engineering، به تنهایی در امنیت کاربردی نداره. زمانی کاربرد داره که شما اون رو با شاخه های دیگه ترکیب کنید. مثلا با وب اپلیکیشن، code auditing ، فازینگ ترکیبش کنید.
در شبکه مهندسی معکوس رو می‌تونید با روتر و سوئیچ ترکیب زمانی برای کشف مشکل امنیتی در firmware.
مهندسی معکوس و فازینگ (fuzzing) زمانی ترکیب می‌شوند، که برای مثال زمانی که فازر (fuzzer) یک باگ یا آسیب پذیری پیدا میکنه، شما اون کد باینری (binary) رو مهندسی معکوس کنید و بفهمید مشکل امنیتی از کجا نشات می‌گیره و چطور پیدا شده.

- مهندسی معکوس پیش نیاز زیاد داره(شاخه های قبل که گفتیم)، ولی به طور مشخص لازم هست که شما زبان ماشین (Assembly) رو هم باهاش آشنا باشید. اگر ۱۰ یا ۱۵ سال پیش قصد داشتید مهندسی معکوس رو یاد بگیرید، بدون شک الزام بود که شما زبان اسمبلی رو مسلط باشید. اما امروزه اگر زبان ماشین رو به صورت ساده می‌خواهید استفاده کنید، با استفاده از ابزارهای پیشرفته ای که وجود داره (مثل Ghidra , IDA Pro, etc) اولویت یادگیری زبان ماشین کمتر شده.(همچنان لازمه)
- کار این ابزار ها، decompile کردن زبان های برنامه نویسی مختلف هست و به در مهندسی معکوس کمک می‌کنه. ترکیب این ابزار ها و پلاگین ها هوش مصنوعی بسیار مفیده در این زمینه پیشرفت خوبی داشته.
- اگر علاقتون سمت موبایل اپلیکیشن هست، وقتتون رو بگذارید روی ARM Assembly Internals and Reverse Engineering
- قبل از اینکه سراغ ابزار ها برید، شما باید یک از این دو کتاب قدیمی و فسیل رو بخونید. کلیت کار عوض نشده:

1. Reversing: Secrets of Reverse Engineering
2. Reverse Engineering for Beginners

بعد از مطالعه یکی از این دو منبع و آشنایی با زبان اسمبلی، می‌تونید سراغ ابزار ها برید. (لینک منابع برای یادگیری ابزار ها داخل گیت هاب آقای کشفی)
مهندسی معکوس در وب اپلیکیشن برای تحلیل کد های بکند و API هایی که با زبان های Go یا Rust نوشته شدن به کار میاد. برای تست روی این سبک اپلیکیشن ها به مهندسی معکوس نیاز دارید. (حتی در موبایل اپلیکیشن اهمیت مهندسی معکوس بیشتر میشه)

Malware & Forensic

در بدافزار ها فقط شما با باینری سروکار دارید. برای تحلیل malware ها و بررسی‌شون، reverse engineering رو باید بدونید. (تماما با کد های باینری باید سروکله بزنید)

آینده‌ی دنیای امنیت سایبری و دیدگاه آقای کشفی

توصیه میکنم این قسمت از ویدیو رو تماشا کنید:
https://www.youtube.com/live/M6-ELr9FRNY?si=R23wszfrc_ddMIZJ&t=18896

خلاصه: آقای کشفی در حوزه های مختلفی از امنیت سایبری فعالیت کردند و در هر کدام چندین سال به صورت جدی و اختصاصی زمان گذاشتند و مطالعه کردند. اینجا براتون مینویسم:

- reverse engineering
- wireless security
- RFID
- network security
- web application security
- source code auditing (5-6 years)
- mobile application security

دقت کنید که مطالعه ایشون در این زمینه ها از روی علاقه شخصی بوده و هست.

- در حال حاضر، دنیا داره به سمت Web App و Cloud Security میره. مشخصا داشتن تخصص در این دو زمینه آینده‌ی کاری شما (چه از نظر معلومات فنی چه از نظر نیاز بازار) وابسته به این دو زمینه خواهد بود.
- مورد دوم اینکه شما با یادگیری system exploitation ، fuzzing ، binary exploitation همیشه " نون‌تون توی روغنه " . برای مثال شما با یادگیری exploitation و memory corruption می‌تونید تخصص خودتون رو ببرید سمت شاخه های خاص (مثلا مرورگر ها، امنیت موبایل، نرم افزار های سیستمی).
- از زمان خلقت و به وجود آمدن امنیت سایبری، داستان های مثل Buffer overflow و حمله های سیستمی وجود داشته تا به امروز. نه زبان برنامه نویسی امن، نه هوش مصنوعی و نه تدابیر امنیتی در نرم افزار ها در سیستم عامل ها، نمیتونن امنیت سیستم ها
- رو به طور کامل برقرار کنند. (در این مورد می‌تونید بیشتر تحقیق کنید، نکات جالبی داره)

- cloud security آینده‌ی خیلی خوبی داره.
- اینترنت اشیا (IoT) و Embedded Devices به طور خاص با توجه به آینده‌ی تکنولوژی و استفاده از کامپیوتر ها در قسمت های مختلف زندگی انسان کاربرد و آینده داره.
- عمیق شدن در امنیت وب اپلیکیشن و کار کردن در یک زبان و فریم ورک به صورت تخصصی نقش مهمی داره.
- بصورت کلی، آشنا بودن و دانش عمومی امنیت الان دیگه بی فایده است. شرکت ها به دنبال نیرویی هستند که علاوه بر دانش general security ، در یک یا دو زمینه به صورت تخصصی مهارت داشته باشه. (به عنوان یک نیروی حرفه ای یا senior ، باید حداقل یکی از این زیر شاخه ها رو به صورت تخصصی و عمیق کار کرده باشید)

Fuzzing

داستان فازینگ چیه؟

- فازینگ به صورت خلاصه، به معنای پرت کردن یک سری ورودی های تصادفی (random) و غیر منتظره به input های یک نرم افزار تا موقعی که به خطا بخوره (crash کنه) و رفتار غیر منتظره نشون بده

شما حتی در این شاخه هم به reverse engineering نیاز پیدا می‌کنید، زمانی که یک باینری رو فاز می‌کنید و کرش کرد، با استفاده از اون crash dump متوجه می‌شید که کدام قسمت از آن نرم افزار و باینری آسیب پذیر است و باعث مشکل شده. (درک خوبی از برنامه نویسی ، code audit و مهندسی معکوس باید داشته باشید)

بصورت کلی هر شاخه ای از امنیت رو برید، می‌بینید که reverse engineering و code auditing برا خلاف اینکه مباحث پیشرفته ای هستند، همه جا به کار می‌روند.

کتاب اول در زمینه فازینگ (Fuzzing: Brute Force Vulnerability Discovery) :

کتاب قدیمی هست، اما توضیح کلی از فازینگ و مکانیزم ها برای ما میگه. فصل های مختلف این کتاب دید جامع و خوبی به ما میده. این کتاب مقدمه‌ای هست برای خوندن مقالات جدید. (نقشه راه خوبی برای فازینگ هست)

- دو منبع بعدی هم برای شروع فازینگ مناسب هستند.
- دو منبع پایین هم بسیار مفید و سبک هستند برای شروع در شاخه‌ی فازینگ:

- The Fuzzing Book (free web content)
- Fuzzing Against the Machine

" زمانی که به عنوان یک senior از آب و گل درومدید و خواستید بر اساس دانش خودتون مشکلات امنیتی جدید رو کشف کنید و تحقیق و research کنید، بلد بودن فازینگ بخش جداناپذیری از کار شما میشه. "

"اگر میخواهید در زمینه smart contract ها فعالیت کنید، باز هم به فازینگ نیاز دارید. "

" آدم های خفنی که دنبال می‌کنید که باگ های خفن و 0day رو کشف می‌کنند، همه از ترکیب fuzzing + reverse engineering استفاده می‌کنند. "

مخلص کلام، فازینگ خیلی مهمه. برید یاد بگیرید :)

Cryptography

رمزنگاری یا cryptography، پیش نیاز نیست بلکه یک نیاز موازی هست.
در هر شاخه‌ای از امنیت سایبری، رمزنگاری بخش جدانشدنی از معماری برنامه هاست.

بخش قابل توجهی از باگ های جالب سیستم ها مثل ویندوز، لینوکس و نرم افزار های وب اپلیکیشن، از مشکلات مربوط به رمزنگاری ریشه می‌گیرند.

- اگر قصد دارید به صورت حرفه‌ای در این زمینه فعالیت کنید، این رو بدونید که با ریاضیات سروکار دارید.
- دانستن جزئیات متوسط از رمزنگاری، به شما کمک میکنه آسیب پذیری های جالب تری رو پیدا کنید. (زمانی که مهندسی معکوس و فازینگ هم کار می‌کنید، دونستن رمزنگاری الزامیه)
- هنگام مطالعه منابع این کتاب، اگر قصد دارید می‌تونید از قسمت ریاضیات رد بشید.
- مباحث خیلی سطحی از رمزنگاری رو در پیش نیاز ها یاد می‌گیرید، اما برای توسعه دانش خودتون می‌تونید کتاب ها و یا دوره های آموزشی به درد بخور رو مطالعه کنید.
- حتی اگر وب کار می‌کنید، توصیه میشه که یک گریزی به رمزنگاری بزنید و مطالب پایه رو خوب یاد بگیرید.

Hardware Security

برای کسانی که با embedded system آشنا هستند، با برنامه نویسی آشنا هستند، با reversing کمی آشنا هستند و باگ کلاس های مختلف آشنا هستند، حالا می‌خواهند این معلومات رو ترکیب کنند و یاد بگیرند چطوری یک سخت افزار رو تست کنند و مشکلات امنیتی شون رو کشف کنند.

- کلیت ماجرا اینه که شما یک سخت افزار رو تحلیل امنیتی می‌کنید، و تست می‌کنید چه راه های ورودی و تکنیک های برای کشف آسیب پذیری وجود داره.
- مهمترین و قشنگ ترین کتاب این بخش که برای شروع مناسب و آسان است:
  The Hardware Hacking Handbook
- کتاب Practical IoT Hacking هم برای شروع مناسبه

این دو کتاب به روز و مناسب برای یادگیری 0 تا 100 هک سخت افزار هستند.

مثال Hardware Hacking :

- چطوری از یک مودم ISP دسترسی shell بگیریم
- از دستگاه پوز بانکی تست security بگیریم
- بصورت پیشرفته تر: تست سخت افزاری یک ابزار کنترل صنعتی شرکت گازی یا یک ترمینال برق
- تست سخت افزار گوشی و سوء استفاده از مشکل امنیتی آن به کمک نرم افزار

Cloud Security

همه دنیا داره میره سمت cloud و فضای ابری. اکثر شرکت ها و بیزنس ها (چه شرکت های استارتاپی کوچک و چه کمپانی های بزرگ) ، برنامه ها و اپلیکیشن هاشون روی فضای ابری host میشن. یک بخشی از شبکه یا سیستم ها و سرور های مشتریان شما و کسانی که درخواست مشاوره امنیتی دارند روی cloud ذخیره میشه.
به طبع یک سری مشکلات امنیتی و باگ کلاس ها مخصوص خودش رو داره.

- کتاب ها و منابع این بخش به شما آموزش میده چطوری با پلتفرم ها و سیستم های بستر cloud سر و کله بزنید. (به خصوص برای کسانی که وب کار می‌کنند کتاب آخر توصیه میشه)
- حتی در حد یک AWS administrator باید با مشکلات امنیتی این سیستم ها آشنا باشید.

سخن پایانی

- همونطور که خودتون متوجه شدید، کار کردن در زمینه cyber security دشواری زیاد داره. مطالعه خیلی خیلی زیاد لازم داره، پشتکار و وقت گذاشتن زیاد نیاز داره.

- اگر به عنوان یک تازه کار که ۶ ماه تا ۱ سال وقت گذاشتید و به خروجی نگرفتید، دلسرد نشید و خودتون رو با کسایی که از شما جلوتر هستند و تجربه‌ی زیادی دارند مقایسه نکنید، چون اون افراد برای مثال در ۱۵ سال هر روز، مستمر و پیوسته مطالعه کردند و زمان گذاشتند و نتیجخ فعالیت ها و تست کردن های متعدد کاری‌شون طی سالیان میشه اینکه از یک اپلیکیشن توی ۱۵ دقیقه آسیب پذیری پیدا می‌کنند .
- به خودتون سخت نگیرید، صبور باشید و به مطالعه کردن ادامه بدید.
- برای یادگیری مباحثی که هنوز پیش نیاز هاش رو بلد نیستید حرص نداشته باشید. (اگر هنوز در ابتدای مسیر هستید، به دنبال نقشه راه های cloud security یا fuzzing نباشید)

موفق باشید 3>