بهمن ماه1402	گزارش عملکرد ماهانه	
نام : علی	جمع کل ساعت کارکرد این ماه : **44:00 ساعت**	

لیست پروژه های فعال :

عنوان پروژه	شرح خدمات
کار بر روی آسیب‌پذیری SQL Injection سامانه simania.co.il - تهیه گزارش از سامانه‌های پروژه SQL Injection	- تهیه گزارش در مورد سامانه‌های مذکور - کار بر روی آسیب‌پذیری sql injection در سامانه simania.co.il با تمرکز بر ابزار sqlmap
Mass Scan for Modems in Israel	- جستجوبرای مودم‌های در دسترس در محدوده رژیم و تلاش برای تغییر آدرس DNS Server بر روی آن

توضیحات : 26-30 (دی) و 7-9-11 (بهمن) - از مرخصی استفاده شد.

ریز عملکرد روزانه

تاریخ	پروژه	توضیحات	ساعت
1402/10/25	sefrou.co.il	تکمیل گزارش ماهانه و گزارش ورود و خروج - بر روی سامانه sefrou.co.il یک ماژول به نام wp-postrating وجود دارد که دارای آسیب‌پذیری sql injection می‌باشد. برای cve-2011-4646 یه مقدار جستجو کردم که POC وجود دارد یا خیر، که پیدا نکردم - فایل‌های سیستم رو تماماً روی nextcloud بارگذاری کردم	7:00
1402/10/26	-	مرخصی	00:00
1402/10/27	bonimonline.co.il	پر کردن یک فایل اکسل مورد درخواست مدیریت در رابطه با کارهای انجام گرفته بر روی تارگت‌های پروژه SQL Injection - گزارش‌نویسی سامانه bonimonline.co.il از تارگت‌های پروژه SQL Injection	4:00
1402/10/30	-	دانشگاه	00:00
1402/11/01	simania.co.il	مطالعه سند جدید ساختار Planka و Next Cloud و تغییر دادن این دو محیط - اسکن مجدد سامانه simania.co.il با ابزار Acunetix - مرور داکیومنت‌های Sqlmap - اسکن سامانه simania.co.il با استفاده از ابزار Sqlmap - شروع استخراج لیست دیتابیس‌های سامانه - استفاده از Tor به جهت جلوگیری از بلاک شدن - مطالعه بیشتر در خصوص تکنیک‌های جلوگیری از بلاک شدن و ابزارهای مخصوص این کار	7:00
1402/11/02	simania.co.il	ادامه روند استخراج لیست دیتابیس‌ها از سامانه simania.co.il - کوئری‌های مورد استفاده Time-Based بوده و به همین جهت این پروسه بسیار زمان بر شده است - با وجود استفاده از Tor همچنان گاهی IP بلاک می‌شود - جلسه با مدیریت	5:00
1402/11/03	Modem Mass Attack	امروز تسک فورس با هدف اسکن به صورت mass برای یافتن هر نوع مودم در محدوده رژیم و کشف آسیب‌پذیری بر روی آن‌ها و تغییر آدرس DNS Server در تنظیمات مودم‌ها - با کمک مدیر فنی با ابزار Censys لیستی از دیوایس‌های برند GoAhead را پیدا کردیم - سپس یکی از آی پی ها را به عنوان تست باز کردم - نام کاربری و رمزعبور پیش فرض روی آن تنظیم شده بود - درخواست لاگین را ضبط کردم - سپس با ابزار Burp suite و اکستنشن Intruder ابتدا از میان آی پی هایی که پیدا کرده بودیم مواردی که نام کاربری و رمزعبور آن‌ها پیش فرض admin است را پیدا کردم - بعد از آن درخواست تغییر آدرس DNS Server را در Intruder قرار دادم - در این میان متوجه شدم باگ بزرگتری در این سری از دیوایس ها وجود دارد و آن این است که اگر در یکی از آن ها لاگین کنیم، با شناسه نشست بدست آمده میتوان به مابقی مودم هایی که نام کاربری و رمزعبورشان با دیوایس اول یکی بوده با استفاده از همان شناسه نشست درخواست ارسال کنیم. تحلیل این موضوع این است که فرآیند چون فرآیند احراز هویت به صورت تصادفی است و هر بار یک شناسه نشست ارائه میدهد نمیتوان نتیجه گرفت که تابع فراخوانی شده همواره یک مقدار ثابت را برای یک جفت نام کاربری و رمزعبور بر میگرداند، بلکه میتوان نتیجه گرفت که احتمالا در جایی این دیوایس ها به یکدیگر متصل بوده و برای همین با شناسه نشست یکی از دیوایس ها میتوان وارد مابقی دیوایس ها با همان جفت نام کاربری و رمزعبور نیز شد - لذا بطور مستقیم شناسه نشست را وارد درخواست کرده و با ابزار Intruder آدرس DNS Server حدود 580 عدد از این دیوایس‌ها را تغییر دادم.	7:00
1402/11/04	Modem Mass Attack	امروز در مورد ابزار Censys بیشتر مطالعه کردم - درمورد معادله CPE داکیومنت های MITRE و NVD را مطالعه کردم - سعی کردم بتوانم کوئری پیدا کنم که مودم‌های TP-Link را برگرداند - به صورت دست و پا شکسته تعدادی را پیدا کردم اما آسیب‌پذیری روی آن‌ها پیدا نکردم - برخی Router بودند - از گیت هاب چند لیست پسورد برای Brute-Force روی مودم‌ها جمع‌آوری کردم	5:00
1402/11/07	-	مرخصی - دانشگاه	00:00
1402/11/08	setter.co.il	نوشتن گزارش سامانه setter.co.il و بارگذاری در پلانکا	3:00
1402/11/09	-	مرخصی - کسالت	00:00

1402/11/10	shmuel.goder.co.il shukrumla.co.il	نوشتن گزارش سامانه shmuel.goder.co.il - نوشتن گزارش سامانه shukramla.co.il	4:00
1402/11/11	-	مرخصی - دانشگاه	00:00
1402/10/14	shulirand.co.il	نوشتن گزارش سامانه shulirand	2:00