

۲۰۵۶۸۵۹

مجموعه کتاب‌های مرکز عملیات امنیت

روز دوم

نگاهی به معماری و مانیتورینگ

امنیت شبکه

برگرفته از مفاهیم شارژ SANS

مؤلفان:

سید سعید حسینی

مریم مکاریان خراسانی



**NAGHOOS
PUBLICATION**

سرشناسه	حسینی، سید سعید، ۱۳۶۰-
عنوان و نام پدیدآور	نگاهی به معماری و مانیتورینگ امنیت شبکه برگرفته از مفاهیم شرکت SANS / مولفان سید سعید حسینی، مریم مکاریان خراسانی
مشخصات نشر	تهران: ناقوس، ۱۳۹۸.
مشخصات ظاهری	۱۹۰ص: مصور.
فروست	مجموعه کتابهای مرکز عملیات امنیت؛ روز دوم.
شابک	978-600-473-215-4
وضعیت فهرست نویسی	فیا
موضوع	کامپیوترها - ایمنی اطلاعات
موضوع	Computer security-- Management
موضوع	شبکه های کامپیوتری - تدابیر ایمنی
موضوع	Computer networks--Security measures
موضوع	حفاظت داده ها
موضوع	Data protection
شناسه افرا	مکاریان خراسانی، مریم و ۱۳۷۱-
رده بندی گره	QA ۷۶/۹
رده بندی دیو	۰۰۵/۸
شماره کتابشناسی ملی	۵۸۲۴۸۵۵



**NAGHOOS
PUBLICATION**

برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoos.com.ir

انتشارات ناقوس

نام کتاب	مرکز عملیات امنیت، مکاریان خراسانی به معماری و مانیتورینگ امنیت شبکه برگرفته از مفاهیم شرکت SANS
ناشر	انتشارات ناقوس
مولفین	سید سعید حسینی، مریم مکاریان خراسانی
ناظر چاپ	یاسمن تجملی محدث
چاپ اول	۱۳۹۸
تیراژ	۱۰۰۰جلد
چاپ و صحافی	برجسته
قیمت	۴۰۰۰۰۰ ریال
شابک	۹۷۸-۶۰۰-۴۷۳-۲۱۵-۴
ISBN	978-600-473-215-4

این کتاب برای سرمایه گذار محفوظ است. کتاب را به قسمتی از این اثر به صورت حروف پیکتو چاپ مجدد، چاپ افست، پیکتو، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

انتشارات ناقوس

بلوار کشاورز- خیابان آذر- کوچه پارسی- پلاک ۱۰

تلفن و فاکس: ۶۶۳۷۸۹۵۸-۶۶۳۷۸۹۵۷

فهرست مطالب

مقدمه

۳

فصل اول: معماری امنیتی شبکه

- سناریو ۱: حمله برنامه کاربردی وب ۱۰
نکات کلیدی سناریو ۱ ۱۳
سناریو ۲: Pivot + Client-Side + Watering hole ۱۵
نکات کلیدی سناریو ۲ ۱۹

فصل دوم: روترها، سوئیچ‌ها و FWSM

- روترها ۲۳
تشخیص مبتنی بر روترها : IPFIX / NetFlow ۲۳
داده‌های IPFIX/NetFlow ۲۴
پروتکل TCP ۲۵
پروتکل UDP ۲۷
پروتکل ICMP ۲۷
پرو فایل داده‌های خروجی ۳۰
ارتباطات خروجی غیر طبیعی ۳۰
ارتباطات خارجی با حجم زیاد ۳۱
مقصد های غیر منتظره ۳۲
تصویر سازی ترافیک خروجی ۳۲
نقش کلیدی روترها ۳۳
روتر در سناریوی ۱ (برنامه کاربردی وب) : پیشگیری ۳۳
روترها در سناریوی ۱ (برنامه کاربردی وب) : تشخیص ۳۳
روترها در سناریوی ۲ (کاربران): پیشگیری ۳۴
روترها در سناریوی ۲ (کاربران): تشخیص ۳۴
سوئیچ‌ها ۳۵
IPFIX/NetFlow ۳۵
(VACLs) VLAN ACLs ۳۵
FW Service Module / Internal SI Firewalls ۳۶
Pivot و Switch/FWSM/Internal SI Firewall ۳۷

فصل سوم: فایروال‌های Stateful Inspection

- درک Stateful ۴۱
- پروتکل TCP - پاسنگویی ۴۲
- پروتکل UDP - پاسنگویی ۴۲
- مسدود سازی ترافیک ورودی به صورت پیش فرض ۴۳
- فیلترهای اضافی ترافیک ورودی لایه ۳ ۴۴
- مسدود سازی ترافیک خروجی به صورت پیش فرض ۴۶
- فیلتر کردن خروجی لایه ۳ ۴۷
- فیلتر کردن خروجی لایه ۴ ۴۷
- فایروال SI و سناریو یک (Web App): پیشگیری ۴۷
- فایروال SI و سناریو یک (Web App): تشخیص ۴۸
- فایروال SI و سناریو دو (Client): پیشگیری ۴۸
- فایروال SI و سناریو دو (Client): تشخیص ۴۹

فصل چهارم: فایروال برنامه کاربردی وب

- قابلیت‌های فایروال برنامه کاربردی وب ۵۳
- تشخیص و پیشگیری فایروال‌های برنامه کاربردی وب ۵۴
- فایروال‌های برنامه کاربردی وب و سناریو ۱ (برنامه کاربردی وب): پیشگیری ۵۴
- فایروال برنامه کاربردی وب و سناریو ۱ (برنامه کاربردی وب): تشخیص ۵۴
- فایروال برنامه کاربردی وب و سناریو ۲ (کاربر): تشخیص و پیشگیری ۵۵

فصل پنجم: NIPSs & NIDSs

- سیستم‌های پیشگیری از نفوذ شبکه ۵۹
- از NIPS به NGFW ۵۹
- سیستم پیشگیری از نفوذ شبکه و تشخیص در سناریوهای ۱ و ۲ ۶۰
- سیستم پیشگیری از نفوذ شبکه و سناریو ۱ (برنامه کاربردی وب): پیشگیری ۶۰
- سیستم پیشگیری از نفوذ شبکه و سناریو ۲ (کاربر): پیشگیری ۶۰
- سیستم‌های تشخیص نفوذ شبکه ۶۰
- قرارگیری سیستم تشخیص نفوذ داخل محیط ۶۱
- پی‌کربندی سیستم تشخیص نفوذ ۶۱
- سیستم تشخیص نفوذ شبکه و پیشگیری ۶۲

۶۳	سیستم تشخیص نفوذ شبکه و سناریو ۱ (برنامه کاربردی وب): تشخیص
۶۳	سیستم تشخیص نفوذ شبکه و سناریو ۲ (کاربر): تشخیص
۶۴	NIDS و NSM
۶۴	اساس طراحی NIDS
۶۵	تطبیق امضا
۶۵	رفتار پروتکل
۶۵	تشخیص ناهنجاری

فصل ششم: فایروال‌های نسل بعدی

۶۹	فایروالینگ لایه ۷
۶۹	تفاوت SI و NGFW
۷۰	بازرسی برنامه‌های کاربردی
۷۰	OpenAppId
۷۰	سناریویی دیگر در مورد تفاوت SI و NGFW
۷۰	دید کافی نسبت به کاربر
۷۱	تفاوت NGFW و UTM
۷۱	NGFW و سناریو ۱ (برنامه کاربردی وب)
۷۱	NGFW و سناریو ۲ (کاربر): پیشگیری
۷۲	NGFW و سناریو ۲ (کاربر): تشخیص

فصل هفتم: دستگاه Detonate بدافزار

۷۵	قابلیت‌های دستگاه Detonation بدافزار
۷۶	Detonation بدافزار در سناریو ۲ (کاربر): پیشگیری / تشخیص
۷۶	پلتفرم‌های تحلیل بدافزارها به صورت پویا
۷۶	معرفی چند پلتفرم تحلیل پویای بدافزار

فصل هشتم: Forward Proxy

۸۸	تنظیم پراکسی کاربران
۸۹	WPAD
۹۱	Web Content Filters
۹۱	MIME/Content-Type
۹۲	Blacklisting

- ۹۲ فوروارد پراکسی در سناریو ۲ (کاربر): پیشگیری
- ۹۳ فوروارد پراکسی در سناریو ۲ (کاربر): تشخیص

فصل نهم: SIEM/SIM/SEM

- ۹۷ ابزاری با چندین نام
- ۹۸ مشکل و وضع کنونی SIEM
- ۹۸ اظهارات Hewlett Packard درباره افراد و کارمندان
- ۹۹ اظهارات Hewlett Packard درباره فرآیندها
- ۹۹ ۱۰ استراتژی مرکز عملیات امنیت سایبری MITRE
- ۱۰۲ انطباق و SIEM تاکتیک
- ۱۰۳ هدف یک SIEM
- ۱۰۴ طرح ریزی یک SIEM
- ۱۰۴ استراتژی‌های جمع‌آوری داده
- ۱۰۶ داده‌هایی که باید جمع‌آوری و تحلیل شوند
- ۱۰۷ داده‌های گرم و داده‌های سرد
- ۱۰۸ اجزای SIEM
- ۱۰۹ SIEM و پیشگیری
- ۱۰۹ SIEM و تشخیص

فصل دهم: دستگاه‌های صدای بسته

- ۱۱۳ Packet Data
- ۱۱۳ ضبط کامل بسته‌ها
- ۱۱۴ ابزارهای ضبط کامل بسته‌ها
- ۱۱۴ قابلیت‌های تشخیص
- ۱۱۵ ضبط بسته‌ها و پیشگیری

فصل یازدهم: دستگاه‌های فریب دشمن

- ۱۱۹ هانی پات و هانی نت
- ۱۲۰ دلایل استفاده از یک هانی پات
- ۱۲۰ انواع هانی پات
- ۱۲۲ هانی پات‌های سنتی
- ۱۲۲ هانی پات‌های High-interaction

۱۲۲	هانی پات‌های Low-interaction
۱۲۳	هانی پات‌های Medium-interaction
۱۲۳	هانی پات‌های داخلی
۱۲۴	هانی کلاینت
۱۲۵	هانی توکن
۱۲۶	معرفی چند هانی پات منبع باز

فصل دوازدهم: هوش تهدید

۱۳۱	هوش تهدید
۱۳۲	هوش تهدید استراتژیک و تاکتیکی
۱۳۳	TTP
۱۳۳	IOC
۱۳۶	IOA
۱۳۷	تفاوت IOA ها با IOC ها
۱۳۸	تفاوت TTP ها و شاخصه‌ها
۱۳۸	مروری بر Cyber Kill Chain
۱۳۹	شناسایی شاخصه‌ها
۱۳۹	چرخه تشخیص و پاسخگویی
۱۴۰	(DWL) Dirty Word List
۱۴۰	منابع هوش تهدید
۱۴۱	استانداردهای هوش تهدید
۱۴۳	مدل بلوغ هوش تهدید

فصل سیزدهم: NSM

۱۵۷	نظارت بر امنیت شبکه (NSM) چیست؟
۱۵۷	نظارت مستمر امنیتی (CSM) چیست؟
۱۵۷	تفاوت بین نظارت بر امنیت شبکه (NSM) و نظارت مستمر امنیتی (CSM)
۱۵۸	سیر تکامل NSM و تفاوت با NIDS
۱۵۸	چرا «تشخیص» را با «پیشگیری» جایگزین نکنیم؟
۱۵۹	علت استفاده از NSM
۱۵۹	منابع داده‌ای NSM
۱۶۰	داده‌های بسته‌های شبکه

۱۶۰	داده های استخراج شده
۱۶۰	داده های رشته ای
۱۶۱	داده های جریان
۱۶۱	داده های تراکنش
۱۶۱	داده های آماری
۱۶۱	داده های هشدار
۱۶۲	داده های برجسب گذاری شده
۱۶۲	داده های همبستگی
۱۶۲	جعبه ابزار NSM
۱۶۷	مسائل کاربردی در پیاده سازی NSM
۱۶۷	سنسورها و سرورهای NSM
۱۶۷	چگونه sniff انجام شود
۱۶۸	کجاها sniff شوند
۱۶۸	Umbrella Sensor
۱۶۹	جایگذاری سنسورها
۱۷۰	NTP
۱۷۰	متدولوژی تجزیه و تحلیل
۱۷۰	شرلوک هولمز و نتیجه گیری
۱۷۰	متدولوژی تجزیه و تحلیل NSM
۱۷۲	تشکیل یک تیم شکار
۱۷۳	دستورالعمل های تیم شکار

منابع و مأخذ

۱۷۷	منابع و مأخذ
-----	--------------

مقدمه

تقریباً هر شرکت در حال حاضر حداقل دارای برخی از تجهیزات امنیتی دفاعی سایبری مانند فایروال، پیشگیری از نفوذ، فیلتر ایمیل و آنتی ویروس می باشد. اینها اصول درستی هستند، اما آیا این تجهیزات برای محافظت از شرکت شما واقعا کافی هستند؟

در مجموعه کتابهای مرکز عملیات امنیت، جنبه های مختلفی از امنیت اطلاعاتی را به صورت عمیق بررسی خواهیم کرد. موضوعات اصلی مورد بررسی، موارد زیر خواهند بود:

- معماری امنیتی¹
- مراکز عملیات امنیت²
- نظارت بر امنیت شبکه³
- نظارت مستمر امنیتی⁴

سازمان شما با پیاده سازی مواردی که در این مجموعه کتابها بررسی می شوند، می تواند سریعاً به موفقیت دست پیدا کند، اما امنیت اطلاعات توجه دائمی می طلبد. کتاب روز اول با بررسی وضعیت فعلی امور مربوط به امنیت اطلاعات شروع می شود. سپس به بررسی تهدیدهای محیط فعلی و معماری امنیتی سنتی و مرسوم می پردازد.

معماری فعلی در چه مواردی با موفقیت عمل می کند؟

کدام راه حل های سنتی و مرسوم نمی توانند پاسخی چالش های فعلی باشند؟

با بررسی پاسخ های پرسش های بالا به کاستی های معماری فعلی پی خواهیم برد و با تغییراتی که برای برطرف کردن آنها الزامی است آشنا خواهیم شد.

یکی از چالش هایی که با آن مواجه هستیم تغییرات مداوم و چشم انداز⁵ تهدیدات است. اگرچه یک معماری امنیتی قوی شبکه و کاربر نهایی⁶ در جلوگیری از رخنه⁷، تسهیل به راه حل های استاندارد، موفق تر عمل می کند، ولی آنها هم شکست می خورد. قبل از اینکه سعی کنیم چیزی را بهبود ببخشیم، نیاز داریم که بدانیم چطور آسیب می بیند. باید ابتدا نقاط قوت و ضعف معماری های سنتی و رایج را بررسی کرده، قابلیت های موجود برای مانیتورینگ را تشخیص داده و نقطه هدف مورد نیاز سازمان را تعریف کنیم. جنبه دیگر ارزیابی وضع موجود، بررسی محیط موجود برای تشخیص⁸ است. نظارت مستمر

-
1. Security Architecture
 2. Security Operations Centers
 3. Network Security Monitoring (NSM)
 4. Continuous Security Monitoring (CSM)
 5. landscape
 6. End-point
 7. Compromise
 8. detection

امنیتی یک جزء مورد نیاز برای معماری امنیتی مدرن است و پاسخگویی سریع به تهدیدات پیش نشده بعدی را تسهیل می‌کند.

در روز دوم از مجموعه کتاب‌های مرکز عملیات امنیت، تأکید کلیدی بر معماری امنیت شبکه قابل دفاع^۱ است. در بخش اول شاخصه‌های کلیدی^۲ یک معماری امنیتی شبکه قابل دفاع تعریف می‌شود و بعد از تعریف اصول^۳ یک معماری امنیت شبکه قابل دفاع، دستگاه‌هایی که می‌توانند این اصول را پیاده سازی کنند مانند روترها و سوئیچ‌ها، فایروال‌ها، سیستم‌های پیشگیری و تشخیص نفوذ^۴، فایروال‌های برنامه‌های تحت وب^۵، سیستم‌های اطلاعات امنیتی و مدیریت رویداد^۶ و غیره، معرفی و بررسی می‌شوند.

هدف از این کار ایجاد یک چک لیست از ابزارهای امنیتی نیست که با قرار دادن علامت در کنار هر یک، تصور امن بودن شبکه برپایمان ایجاد شود. ممکن است دو سازمان با داشتن دستگاه‌هایی دقیقاً شبیه و یکسان در دو سطح کاملاً متفاوت امنیتی عمل کنند. نکته کلیدی در تفاوت نحوه انجام تنظیمات، افرادی که این کار را انجام می‌دهند و کاری که برای این دستگاه‌ها تعریف شده است، می‌باشد. تنظیمات^۷، افراد^۸ و رویه‌ها^۹ دارند هستند که این دستگاه‌ها را برای یک معماری امنیت شبکه قوی^{۱۰} کارآمد می‌کنند.

حتی در معماری امنیت شبکه در کار نهایی^{۱۱} با وجود استفاده از حداکثر توانایی‌ها و قابلیت‌ها، رخنه^{۱۲} وجود خواهد داشت. یکی از چندهرگ‌های کلیدی در معماری امنیتی، تشخیص وجود سیستم‌هایی که به آن‌ها رخنه شده و یا تشخیص سوء استفاده از ظرفیت‌های موجود، می‌باشد. فقط تولید داده‌های مربوط به امنیت کافی نیست و ما باید به طور مؤثر کارآمد از حجم زیاد داده تولید شده، استفاده کنیم. منابع کلیدی داده‌ها، داده‌های همبسته^{۱۳}، داده مربوط به هشدارها^{۱۴}، داده مربوط به جلسات^{۱۵}،

1. Defensible network security architecture.
2. key characteristics
3. Principles
4. IDS/IPS
5. web applications firewall
6. Security information and event management systems (SIEMs)
7. configuration
8. people
9. processes
10. Robust network security architecture.
11. End-point
12. compromise
13. correlated data
14. alert data
15. session data

داده مربوط به بسته‌های شبکه^۱، داده لاگ‌ها^۲، داده مربوط به کاربر نهایی^۳، کاربر و داده‌های مربوطه^۴ و مربوطه^۵ و فراداده‌ها^۶ می‌باشند که در نظارت بر امنیت شبکه^۷ مورد استفاده قرار می‌گیرند.

در روز سوم از مجموعه کتاب‌های مرکز عملیات امنیت، بر روی معماری امنیتی کاربر نهایی تمرکز می‌شود. زیرا دشمنان^۸ بر روی رخنه^۹ به کاربران نهایی از طریق اکسپلویت‌های سمت کاربر، متمرکز شده‌اند. دفاع در برابر این نوع خاص از حملات، با راه‌های ساده‌ای که توسط معماری امنیت شبکه سنتی^{۱۰} پیشنهاد می‌شود، بسیار مشکل است.

با افزایش وجود و حضور دستگاه‌های موبایل و دستگاه‌های قابل حمل در محدوده محیط سازمانها، حملات سمت کاربران نیز افزایش یافته است و این دستگاه‌ها نیز از معماری امنیت شبکه مدرن بهره‌ای نمی‌برند.

انجام عملیات pivot^{۱۱} یکی دیگر از جنبه‌های حملات مدرن است که نیاز به داشتن امنیتی قوی در کاربر نهایی را افزایش می‌دهد. بعد از رخنه به یک کاربر نهایی ضعیف، تکنیک رایج دشمنان، pivot کردن و دسترسی به بقیه سازمان است. این حملات این گونه به نظر می‌رسند که توسط دشمنان داخلی انجام شده است در حالی که نونگ^{۱۲} سیستم رخنه شده اولیه^{۱۳} به عنوان نقطه‌ای برای شروع حمله^{۱۴} به شبکه داخلی استفاده می‌کند. پس کاربر نهایی^{۱۵} باید بتواند از خود دفاع کند و به شناسایی حملات نیز کمک کند.

بعد از طراحی یک معماری امنیتی قوی^{۱۶}، به کارگیری اصول نظارت بر امنیت شبکه^{۱۷}، باید اطمینان حاصل کنید وضعیت سیستم‌ها و شبکه‌ها با اصول و قوانین امنیتی دلخواه سازمان شما هماهنگی و سازگاری داشته باشد.

تهدیدها و آسیب‌پذیری‌ها هر روزه افزایش پیدا می‌کنند و باکتبک‌های جدید به طور مؤثری کارایی و امنیت سازمان شما را دستخوش تغییر می‌کنند. اگر ما از وضعیت آگاهی^{۱۸} نداشته باشیم، نمی‌توانیم تصمیمات آگاهانه در مورد اقدامات امنیتی اتخاذ کنیم. در روز چهارم مجموعه کتاب‌های مرکز عملیات

1. packet data
2. log data
3. endpoint data
4. user and attribution data
5. Metadata
6. Network Security Monitoring
7. adversaries
8. compromise
9. Traditional Network Security architecture

۱۰. معادل دیجیتالی جهش نظامی (military leapfrogging) یا پرش جزیره‌ای (island hopping) می‌باشد.

11. initially compromised system
12. beachhead
13. End-point
14. robust security architecture
15. network Security Monitoring principles
16. situational awareness

امنیت، نظارت مستمر بر امنیت¹ که امکان بررسی و آگاهی از وضعیت فعلی امنیت سازمان را فراهم می کند، بررسی می شود. اگرچه بررسی و مرور مستمر وضعیت اجزای سیستم های یک سازمان، نسبتاً مطلوب و ساده به نظر برسد ولی بدون داشتن یک پروسه و رویه مشخص، اینکار بسیار سنگین و پرزحمت خواهد بود.

اگرچه سازمان ها و شرکتها معمولاً بر طبق زمانبندی به تعمیر و نگهداری سیستم عامل های ویندوز و بررسی و حسابرسی² می پردازند ولی دشمنان³ برای انجام حمله و رخنه⁴ به سیستم ها هیچ زمان بندی مشخصی ندارند و منتظر اسکن های سه ماهه و یا حسابرسی های سالانه⁵ سازمان ها نمی شوند. باید آگاه باشیم که چگونه تغییرات تهدیدها، آسیب پذیری ها و دارایی ها⁶ بر روی امنیت سازمان ها تأثیر گذارند و این بستلزم ارزیابی مستمر سازمان است. برای دستیابی به ارزیابی مستمر تغییرات حوزه تهدیدها و آسیب پذیری ها، خودکارسازی⁷ نیاز است. در این کتاب از پاورشل⁸، دستورات ساده اسکریپت نویسی در خط فرمان ویندوز و اسکریپت نویسی Bash، برای این کار استفاده خواهیم کرد.

-
1. Continuous Security Monitoring
 2. audit
 3. adversaries
 4. compromise
 5. Quarterly scans or annual audits
 6. assets
 7. automation
 8. PowerShell