راهنمای دوره SEC504

شرکت SANS

جلد اول از مجموعه کتب مدرسه امنیت

مؤلفین:

احسان نیک‌آور

سید سعید حسینی

میثم منصف

NAGHOOS
PUBLICATION

۱۳۹۷

سرشناسه : نیک آور،احسان ۱۳۶۶-
عنوان و نام پدیدآور : راهنمای دوره SEC 504 شرکتSANS/ .مولفین احسان نیک آور،سید سعید حسینی،میثم منصف
مشخصات نشر : تهران: ناقوس،۱۳۹۷
مشخصات ظاهری : ۲۲۲ص
فروست : مجموعه کتب مدرسه امنیت،۱.
شابک : 978-964-377-526-1
وضعیت فهرست‌نویسی : فیپا
موضوع : کامپیوترها – ایمنی اطلاعات — مدیریت
موضوع : Computer Security-- Management
موضوع : شبکه های کامپیوتری – تدابیر ایمنی
موضوع : Computer Networks—Security Measures
موضوع : حفاظت داده ها
موضوع : Data Protection
شناسه افزوده : حسینی،سیدسعید، ۱۳۶۰-
شناسه افزوده : منصف،میثم ،۱۳۶۶ –
شناسه افزوده : Monsef,Meysam
رده بندی کنگره : ۱۳۹۷ ۹ن ۹ ک/۹ /QA۷۶
رده بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ۵۴۶۷[illegible]

برای خرید Online به آدرس زیر مراجعه کنید:
www.naghoospress.ir

NAGHOOS PUBLICATION

انتشارات ناقوس

نام کتاب : راهنمای دوره SEC 504 شرکتSANS
ناشر : انتشارات ناقوس
مولفین : احسان نیک آور، سید سعید حسینی، میثم منصف
چاپ اول : ۱۳۹۷
تیراژ : ۱۰۰۰نسخه
قیمت : ۵۰۰۰۰۰ ریال
چاپ و صحافی : نارنجستان
شابک : ۹۷۸-۶۰۰-۴۷۳-۱۵۲-۲
ISBN : 978-600-473-152-2

مرکز پخش: انتشارات ناقوس
۱-بلوار کشاورز-خیابان ۱۶آذر-کوچه پارسی-پلاک ۱۰
تلفن و فاکس : ۶۶۴۷۸۹۵۷- ۶۶۴۷۸۹۵۸
۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴
۳- کتابفروشی گلریزان: ضلع جنوب‌شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰

مقدمه

شرکت SANS یکی از معتبرترین شرکت‌های فعال در حوزه آموزش امنیت اطلاعات می‌باشد. این شرکت دوره‌های مختلفی را در این زمینه ارائه داده است که پیش‌نیاز اغلب دوره‌های ارائه شده توسط این شرکت، دوره آموزشی SEC504 می‌باشد. به همین منظور تصمیم گرفتیم، منابع مربوط به این دوره را گردآوری نموده و در قالب کتابی که پیش رو دارید، در اختیار علاقمندان به حوزه امنیت شبکه و اطلاعات قرار دهیم.

همچنین این کتاب، اولین جلد از مجموعه کتاب‌های مدرسه امنیت می‌باشد که به امید خداوند منان، جلدهای دیگر این مجموعه نیز به چاپ رسیده و در اختیار علاقمندان به این عرصه قرار خواهد گرفت. لازم به ذکر است مدرسه امنیت نام دوره جامعی است که توسط شرکت دهکده امن فناورانه صبا طراحی شده و هم اکنون که شما این کتاب را مطالعه می‌فرمایید، این دوره در حال برگزاری می‌باشد و کتاب حاضر نیز به عنوان یکی از منابع آموزشی در اختیار دانشجویان دوره جامع مدرسه امنیت قرار خواهد گرفت.

به منظور اطلاعات بیشتر در این زمینه می‌توانید به آدرس زیر مراجعه نمایید:

https://esecurity.ir/security-school

دوستان گرامی که این کتاب را تهیه نموده‌اند می‌توانند جهت بهره‌مندی از هدیه‌ای که برای این کتاب در نظر گرفته شده است به آدرس زیر مراجعه نموده و فیلم‌های آموزشی فارسی تولید شده توسط مهندس میثم منصف در خصوص آسیب‌پذیری سرریز بافر را مشاهده نمایند.

https://esecurity.ir/sec504-buffer

این کتاب قطعاً کامل نبوده و دارای نواقصی می‌باشد که بسیار خرسند می‌شویم دوستان عزیزی که این کتاب را مطالعه نموده‌اند، نظرات، پیشنهادات و انتقادات خود را به ایمیل info@esecurity.ir ارسال نمایند.

همچنین صفحه اختصاصی برای این کتاب در سایت Esecurity.ir ایجاد شده است که به امید خدا فیلم‌های آموزشی مرتبط با کتاب در این صفحه قرار داده خواهد شد. بدین پیشنهاد می‌کنیم بعد از تهیه این کتاب به بخش زیر نیز مراجعه نمایید

https://esecurity.ir/sec504

فهرست مطالب

فصل اول: Incident Handling

تعریف Incident Handling	۳
تعریف Incident	۳
تعریف Event	٤
Corroborating Evidance	٤
Share Your Experiences	٥
مراحل Incident Handling	٦
مراحل Incident Handling	۷
Preparation	۷
People	۸
Policy – Warning Banners	۸
Policy - Response Strategies	۹
Policy - Peer Notification	۱۰
Remain calm and Take Notes	۱۰
Key Points – Management Support	۱۱
Key Points - Building a Team	۱۲
Key Point – Checklists and Team Issues	۱۳
Key Points - Team Organization	۱۳
Key Points – Emergency Comm Plan	۱٤
Key Points - Getting Access to Systems and Data	۱٤
Key Points – Reporting Facilities	۱٤
Key Potnts - Cultivate Relationships	۱٥
GRR Rapid Respose	۱٦
Jump Bag	۱٦
Jump Bag – Software	۱۷
Jump Bag – Investigative Tools	۱۷
Jump Bag - Hardware	۱۸
Jump Bag – More Hardware	۱۹
Jump Bag – Additional Helpful Items	۱۹

Jump Bag – Final Items	١٩
Identification	٢٠
Points to Keep in Mind	٢٠
Assigning Handlers	٢٠
Control the Flow of Information	٢١
Communication Channels	٢٢
?Where Does Identification Occur	٢٣
Containment	٢٤
Deployment	٢٤
Characterize Incident	٢٥
Inform Management	٢٦
Notify Appropriate Officials and Create an Incident Tracking Entry	٢٦
Short-Term	٢٧
Creating Forensics Images	٢٨
Determine the Risk of Continuing Operations	٢٩
Long Term	٣٠
Long-term Actions	٣٠
Eradiction	٣١
Restoring from Backups	٣١
Removing Malicious Software	٣٢
Improving Defenses	٣٣
Vulnerability Analysis	٣٣
Monitor	٣٤
Lessons Learned	٣٤
Report	٣٥
Meeting	٣٥
Apply Fixes	٣٦
Enterprise Incident Response	٣٦
Ingress and Egress Data	٣٦
DNS Data	٣٧
Web Proxy Data	٣٧
Connection Data	٣٨
WMIC	٣٨

SCCM ۳۸
?What about PowerShell ۳۹

فصل دوم: Reconnaissance

Reconnaissance ۴۳
Whois ۴۳
راه‌های جلوگیری از افشای اطلاعات Whois ۴۴
DNS Interrogation ۴۴
DNS Zone Transfer ۴۴
استخراج اطلاعات DNS در لینوکس ۴۵
Website Searches ۴۶
موتورهای جستجو ۴۷
ابزار Maltego ۴۸

فصل سوم: Scanning

شناسایی شبکه با Nmap ۵۱
شناسایی سیستم‌های فعال در شبکه ۵۱
Trace Route ۵۲
شناسایی سیستم عامل با Nmap ۵۳
اسکن پورت با Nmap ۵۳
Three-Way Handshake ۵۴
flags TCP ۵۴
masscan ۵۵
EyeWitness ۵۵
Remux ۵۵
روش‌های پیشگیری از حملات اسکن پورت ۵۶
غیرفعال نمودن سرویس‌ها در ویندوز ۵۶
غیرفعال نمودن سرویس‌ها در لینوکس ۵۷
عبور از سیستم‌های تشخیص نفوذ ۵۷
Pattern Matching ۵۷
Fragmentation Type ۵۸
Tiny Fragment Attack ۵۸
Fragment overlap Attack ۵۸
Invalid TCP Checksum Bypass ۵۹

مقابله با عبور از سیستم‌های تشخیص نفوذ ۵۹
اسکن آسیب‌پذیری ۵۹
ابزارهای اسکن آسیب‌پذیری ۶۰
Nessus ۶۰
روش‌های مقابله با اسکن آسیب‌پذیری ۶۱
SMB Sessions ۶۲
Enum Tool ۶۳
Important Commands in SMB ۶۴
Empire Tool ۶۴
اتصال SMB از لینوکس به ویندوز با استفاده از smbclient ۶۵
Rpcclient Tool ۶۵
مشاهده Session و حذف آن ۶۶
روش‌های مقابله با حملات SMB Session ۶۶

فصل چهارم: Exploiting

BGP Hijacking ۷۱
راه‌های مقابله با BGP Hijacking ۷۱
ابزار NC ۷۲
Client Mode ۷۲
Listen mode ۷۳
دستورات ارتباطی در NC ۷۳
انتقال اطلاعات با NC ۷۴
اسکن پورت و آسیب‌پذیری ۷۴
ایجاد ارتباط با پورت باز ۷۵
ایجاد Backdoor ۷۵
دسترسی پایدار با NC ۷۶
Reverse Shell ۷۶
Netcat - Relays ۷۷
روش‌های ایجاد رله با Netcat ۷۸
Netcat بدون سوییچ c ۷۹
روش‌های مقابله با Netcat ۷۹
Snifling ۸۰
ابزار آنالیز Wireshark ۸۰

IP to MAC Mapping via ARP ۸۲
Gratuitous ARPs ۸۲
macof ۸۳
ابزار tcpkill و tcpicc ۸٤
ابزارهای Filesnarf، Mailsnarf، URLsnarf و Msgsnarf ۸٥
ابزار Xplico ۸٥
WebSpy ۸٥
ابزارهای DNSSpoof، Webmitm، SSHmitm ۸٦
DNS Attack ۸٦
تأثیرات DNSSpoof ۸۷
SSL and SSH Sniff ۸۷
جلوگیری از نمایش پیام‌های هشدار SSL ۸۹
روش‌های دیگر برای جلوگیری از پیام هشدار در SSL ۹۰
SSL Strip ۹۰
Session Hijacking ۹۱
Ack Storm ۹۳
سرقت نشست با استفاده از ARP Cache Poisoning ۹۳
Hijacking با Ettercap ۹٤
ابزار Subterfuge ۹٥
مقابله با حملات سرقت نشست ۹٥
شناسایی حملات سرقت نشست ۹٥
DNS cache poisoning ۹٦
نکاتی در خصوص DNS ۹۷
سناریوی DNS Cache Poisoning ۹۷
راه‌های مقابله با DNS Cache Poisoning ۱۰۰
Password Cracking ۱۰۱
احراز هویت در ویندوز ۱۰٥
Salt in Password ۱۰۷
مزایای استفاده از Salt ۱۰۸
ابزار Cain and Able ۱۰۹
پیکربندی Cain and Able ۱۱۱
استخراج hash ۱۱٤
بوت شدن با یک سیستم‌عامل دیگر و کپی فایل SAM ۱۱٥

راه‌های مقابله با حملات شکستن کلمه عبور ۱۱۶
ابزار John the Ripper ۱۱۶
ساختار ذخیره‌سازی حساب‌ها و کلمات عبور در یونیکس ۱۱۷
مدهای کارکرد ابزار john ۱۱۸
روش‌های مقابله با شکستن کلمات عبور در یونیکس ۱۱۹
حملات Pass The Hash ۱۲۰
ابزارهای مربوط به حمله Pass the Hash ۱۲۲
روش‌های جلوگیری از حملات Pass the Hash ۱۲۲
Worms ۱۲۳
سیر تکاملی کرم‌ها ۱۲۴
Multi-exploit ۱۲۴
Multiplatform Worm ۱۲۶
Zero-Day Exploit Worm ۱۲۷
Fast Spreading Worm ۱۲۸
تکنیکWarhol/Flash ۱۲۹
Polymorphic Worms ۱۲۹
چگونگی ایجاد یک کد polymorphic ۱۳۰
Truly Nasty Payload ۱۳۱
Bots ۱۳۱
گسترش Bot ۱۳۲
چگونگی ارتباط با Botها ۱۳۳
مقابله با بات‌ها و کرم‌ها ۱۳۴
حملات تحت وب ۱۳۵
Account harvesting ۱۳۵
Command Injection ۱۳۶
دستورات برای شناسایی تزریق ۱۳۷
راه‌های مقابله و پیشگیری از حملات تزریق دستور ۱۳۸
آسیب‌پذیری SQL Injection ۱۳۸
Dropping Data ۱۴۰
Grabbing More Data ۱۴۰
Getting Database Structure ۱۴۰
جداولی که توسط کاربر تعریف شده و متادیتاها ۱۴۱
دفاع در برابر حملات SQL Injection ۱۴۱

آسیب‌پذیری Cross Site Scripting یا XSS ۱۴۲
حمله XSS از نوع Stored ۱۴۵
حمله به مدیران با استفاده از XSS ۱۴۷
راه کارهای مقابله با حملات XSS ۱۴۸
Sessionها چگونه ردگیری می‌شوند؟ ۱۴۸
حملات انکار سرویس یا DoS ۱۵۱
DNS Amplification Attacks ۱۵۳
EDNS ۱۵۳
حملات انکار سرویس توزیع شده DDoS ۱۵۵
Reflected DDoS Attacks ۱۵۶
Pulsing Zombies ۱۵۶
Evolution of the Flood ۱۵۷
LOIC ۱۵۷
HOIC ۱۵۸
راه‌های مقابله با حملات DDoS ۱۵۸
نکاتی در مورد دفاع در برابر حملات DDoS ۱۵۹

فصل پنجم: Keeping Access

Backdoors and Trojans ۱۶۳
Malware Layers ۱۶۳
Application-Level Trojan Horse Backdoor Suites ۱۶۵
VNC ۱۶۵
VNC Platform ۱۶۶
WInVNC ۱۶۶
Poison Ivy Configuration ۱۶۷
Scareware ۱۶۷
Wrappers ۱۶۸
windows Anti-Reverse Engineering for Executables ۱۶۹
Defense: Unpacking Windows Executables ۱۶۹
Memory Analyze ۱۷۰
ماژول‌های مهم در Rekall ۱۷۰
User Mode Rootkits ۱۷۲
Linux User Mode Rootkit ۱۷۲

Windows User Mode Rotkits ۱۷٤
Kernel-Mode Rootkits ۱۷۷
The Kernel ۱۷۸
Kernel Mode Rootkits ۱۷۹
Altering the Kernel ۱۸۰
Method 1) Loadable Kernel Modules and Device Drivers ۱۸۱
Method 2) Altering Kernel in Memory ۱۸۲
Method 3) Changing Kernel File on Hard Drive ۱۸۳
Method 4) Virtualizing the System ۱۸٤
Kernel-Mode Rootkit Defenses – Configuration Lockdown ۱۸۵
Defenses - LinwdUNIX Rootkit Detection Tools ۱۸۵
Defenses: File Integrity CheckingTools ۱۸٦
Network Intelligence/Forensic ۱۸٦

فصل ششم: Covering Tracks

Covering Tracks in Linux and Unix ۱۹۱
Hiding Files in Unix ۱۹۱
Where Attackers Put Hidden Unix Files and Dirs ۱۹۱
Editing Unix Log Files ۱۹۲
Don't Forget Shell History ۱۹۳
Accounting Entries in Unix ۱۹۳
Covering Tracks in Windows ۱۹٤
Hiding Files in NTFS ۱۹٤
نحوه ایجاد یک ویژگی به کمک NTFS Stearm ۱۹٤
نحوه قرار دادن یک عکس در فایل متنی به کمک NTFS Stearm ۱۹۵
نحوه قرار دادن یک فایل اجرایی در فایل متنی به کمک NTFS Stearm ۱۹٦
Alternate Data Stream in NTFS ۱۹٦
Log Editing in Windows ۱۹۷
Editing Logs with Physical Access ۱۹۷
Defenses from Covering Tracks ۱۹۸
Covering Tracks on the Network ۱۹۸
Tunneling and Covert Channels ۱۹۸
Reverse HTTP Shells ۱۹۹

ICMP Tunnels ۱۹۹
Ptunnel ۱۹۹
Covert TCP ۲۰۰
جلوگیری از حملات Cover Channel ۲۰۱
Steganography ۲۰۱

منابع و مأخذ

منابع و مأخذ ۲۰۵