

رایانش ابری؛ مخاطرات و روش‌های مقابله با آن

حمید انیسوی - مجید عبقری

www.ketab.ir

سرشناسه	:	انیسی، حمید، ۱۳۷۴-
عنوان و نام پدیدآور	:	رایانش ابری، مخاطرات و روش‌های مقابله با آن / حمید انیسی، مجید عبقری.
مشخصات نشر	:	تهران: نشر زهره، ۱۳۹۸.
مشخصات ظاهری	:	۹۰ ص.
شابک	:	۹۷۸-۹۶۴-۲۹۸۱-۷۹-۳
وضعیت فهرست نویسی	:	فیفا
یادداشت	:	کتابنامه.
موضوع	:	محاسبات ابری
موضوع	:	Cloud computing
موضوع	:	محاسبات ابری --- تدابیر ایمنی
موضوع	:	Cloud computing-- Security measures
شناسه افزوده	:	عبقری، مجید، ۱۳۷۳-
رده بندی کنگره	:	۸۹۳۱ ۲۶۸/۵۸۵/QA۷۶
رده بندی دیویی	:	۶۷۸۲/۰۰۴
شماره کتابشناسی ملی	:	۵۶۷۵۰۶

کرایانش ابری؛ مخاطرات و روش‌های مقابله با آن

حمید انیسی، مجید عبقری

ناشر: زهره

صفحه آرا: معین دلاوری

نوبت چاپ: اول - ۱۳۹۸

شمارگان: ۱۰۰۰ جلد

شابک: ۹۷۸-۹۶۴-۲۹۸۱-۷۹-۳

قیمت: ۲۰۰۰۰ تومان

کلیه حقوق چاپ و نشر مخصوص و محفوظ ناشر است

تهران خیابان انقلاب خیابان وصال شیرازی کوچه ماهان پلاک ۴ زنگ اول

۶۶۴۹۸۴۵۹-۰۹۳۰۲۴۳۴۳۴۱

فهرست مطالب

۸	پیشگفتار.....
۹	مقدمه.....
۱۱	فصل اول: تاریخچه و آشنایی با محاسبات و زیرساخت‌های ابر
۱۳	۱-۱- تاریخچه رایانش ابری.....
۱۳	۲-۱- تعریف رایانش ابری.....
۱۳	۱-۲-۱- تعریف مفهومی.....
۱۴	۲-۲-۱- تعریف اقتصادی.....
۱۴	۳-۲-۱- تعریف کاربردی.....
۱۴	۳-۱- مفهوم ابر در رایانش ابری.....
۱۴	۴-۱- مفهوم میان ابر.....
۱۵	۵-۱- سطوح مختلف رایانش ابری.....
۱۵	۱-۵-۱- بستر به عنوان سرویس (IaaS).....
۱۵	۲-۵-۱- زیرساخت به عنوان سرویس (PaaS).....
۱۶	۳-۵-۱- نرم‌افزار به عنوان سرویس (SaaS).....
۱۶	۶-۱- مدل‌های بکارگیری ابر.....
۱۶	۱-۶-۱- ابر عمومی.....
۱۷	۲-۶-۱- ابر خصوصی.....
۱۸	۳-۶-۱- ابر ترکیبی.....
۱۹	۴-۶-۱- ابر جامعه.....
۲۱	فصل دوم: انواع حملات تداخلی در محیط ابر
۲۳	۱-۲- تداخل‌ها برای سیستم‌های ابری.....
۲۳	۱-۱-۲- حملات داخلی.....
۲۳	۲-۱-۲- حملات طفیانی.....
۲۴	۳-۱-۲- حملات اساسی به کاربر.....
۲۴	۴-۱-۲- اسکن پورت.....
۲۴	۵-۱-۲- حمله به ماشین مجازی.....
۲۵	۶-۱-۲- حملات کانال پنهانی.....
۲۶	مسائل امنیتی محاسبه ابری.....
۲۶	۲-۲- امنیت محاسبه ابری.....
۲۶	۳-۲- مسائل امنیتی وابسته به ابر.....

۲۶	۴-۲- چندگانه امنیت و حفظ حریم خصوصی
۲۷	۵-۲- هفت تهدید امنیتی محاسبات ابری
۲۷	۱-۵-۲- سرقت اطلاعات
۲۷	۲-۵-۲- از دست دادن اطلاعات
۲۸	۳-۵-۲- سرقت حساب کاربری یا ترافیک سرویس
۲۸	۴-۵-۲- رابط‌های کاربری نا امن
۲۸	۵-۵-۲- حملات عدم پاسخگویی سرویس
۲۹	۶-۵-۲- همکار خیانت کار
۲۹	۷-۵-۲- سوءاستفاده از سرویس ابر
۲۹	۸-۲- چالش‌های محاسبات ابری
۲۹	۷-۲- امنیت اطلاعات
۳۰	۱-۷-۲- از دست دادن کنترل بر داده‌ها
۳۰	۲-۷-۲- یکپارچگی داده‌ها
۳۰	۳-۷-۲- خطر تشنج
۳۰	۸-۲- امنیت شبکه
۳۰	۱-۸-۲- حمله متوسط
۳۱	۲-۸-۲- شنود بسته
۳۱	۹-۲- مسائل امنیت دیتا و حفاظت از حریم خصوصی
۳۱	۱-۹-۲- چرخه عمر دیتا
۳۶	۱۰-۲- مدل‌های اولیه امنیت داده در رایانش ابری
۳۷	۱۱-۲- مدل‌های جدید امنیت داده در رایانش ابری
۳۷	۱-۱۱-۲- مدل امنیت داده ترکیبی
۴۱	۲-۱۱-۲- مدل امنیت داده مبتنی بر سطح
۴۲	۱۲-۲- روش‌های کنونی ایجاد امنیت در انتقال داده و ذخیره در فضای ابر
۴۵	فصل سوم، سیستم تشخیص نفوذ و روش‌های تشخیص نفوذ
۴۷	۱-۳- سیستم تشخیص نفوذ
۴۷	۲-۳- روش‌های تشخیص نفوذ
۴۸	۱-۲-۳- شناسایی بر پایه امضاء
۴۸	۲-۲-۳- شناسایی غیرمتعارف
۵۰	۳-۲-۳- IDS بر پایه شبکه عصبی مصنوعی
۵۱	۴-۲-۳- IDS بر مبنای منطق فازی
۵۱	۵-۲-۳- IDS بر پایه قوانین پیوسته

۵۲	IDS-۶-۲-۳ بر پایه ماشین‌ی برداری پشتیبانی (SVW).....
۵۲	IDS-۷-۲-۳ بر پایه الگوریتم ژنتیکی (GA).....
۵۳	IDS-۸-۲-۳- فنون هیبرید.....
	فصل چهارم: بررسی فنون مختلف IDS/IPS، سرویس‌ها و تکنیک‌های تشخیص نفوذ در محیط ابری
۵۷	
۵۹	۱-۴- سرویس سیستم تشخیص نفوذ ابری.....
۵۹	۲-۴- ساختار سرویس تشخیص نفوذ ابری.....
۶۰	۱-۲-۴- عامل سرویس تشخیص نفوذ.....
۶۱	۲-۲-۴- مؤلفه سرویس رایش ابری.....
۶۱	۳-۲-۴- مؤلفه سرویس تشخیص نفوذ.....
۶۱	۱-۳-۲-۴- جمع‌آوری کننده.....
۶۱	۲-۳-۲-۴- موتور تحلیل.....
۶۱	۳-۳-۲-۴- منتشر کننده رویداد.....
۶۲	۴-۳-۲-۴- کنترل‌گر IDS.....
۶۲	۳-۴- ملزومات سرویس تشخیص نفوذ ابری.....
۶۴	۴-۴- انواع مختلف IDS/IPS مورد استفاده در محیط ابری.....
۶۴	۱-۴-۴- سیستم شناسایی تداخل بر اساس میزبان (HIDS).....
۶۸	۲-۴-۴- سیستم شناسایی تداخل بر اساس شبکه (NIDS).....
۷۲	۱-۲-۴-۴- شناسایی خطا در شبکه بر اساس روش SNORT.....
۷۲	۳-۴-۴- سیستم توزیع شده شناسایی تداخل (DIDS).....
۷۵	۴-۴-۴- سیستم‌های شناسایی تداخل بر مبنای هایپروپژر.....
۷۶	۵-۴- سیستم ممانعت از تداخل (IPS).....
۷۸	۶-۴- سیستم ممانعت و شناسایی تداخل (IDPS).....
۸۷	منابع و مآخذ.....

پیشگفتار

محاسبات ابری خدمات مورد تقاضای بصری را برای کاربران جزء با انعطاف‌پذیری بیشتر و سرمایه‌گذاری زیرساختی کمتر فراهم می‌کند. این خدمات تامین‌کننده اینترنت با استفاده از پروتکل‌های شبکه‌ای شناخته شده، استانداردها و قالب‌بندی‌هایی با نظارت مدیریت‌های مختلف است. اشکالات و آسیب‌پذیری‌های موجود در تکنولوژی‌های پایه و پروتکل‌های برجا مانده سبب بازگشایی دروازه‌هایی برای اختلال می‌شود. این کتاب پیمایشی را بر تداخل‌های مختلف که بر دسترسی، محرمانگی و انسجام منابع و خدمات ابری اثرگذار است انجام می‌دهد. پیشنهادات سیستم‌های شناسایی تداخل‌های مشترک (IDS^1) را در محیط ابری آزمون می‌کند و انواع و فنون مختلف IDS و سیستم‌های ممانعت از تداخل‌ها (IPS^2) را مورد بحث قرار می‌دهد و بر توزیع IDS/IPS در اختیار ابری توصیه‌هایی برای دستیابی به امنیت مطلوب در شبکه‌های نسل بعدی دارد.

¹ - intrusion detection system

² - intrusion prevention system