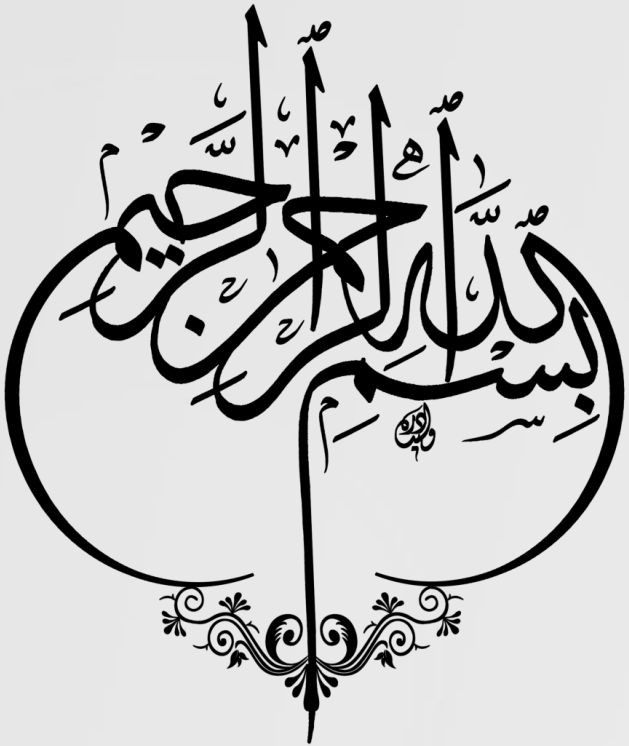


الحمد لله رب العالمين

والصلاة والسلام على أشرف المرسلين سيدنا محمد

وعلى آله وصحبه ومن تبعهم بإحسان إلى يوم الدين.

تأمين الشبكة والخوادم و البرامج

وقاية و تأمين,تعريف

جدول المحتويات

01 **الحماية الالكترونية**
تعاريف و المشاكل التي يجب حلها

02 **المنهج و الطرق**
المنهج المتبع لحل المشاكل المطروحة و الطرق المتبعة

03 **التطبيق العملي**
إنشاء منهج حماية في شبكة افتراضية مطابقة للواقع

04 **حماية التطبيقات**
من جانب البرمجة و متابعة والتصحيح

01

الحماية الالكترونية

تعاريف و المشاكل التي يجب حلها

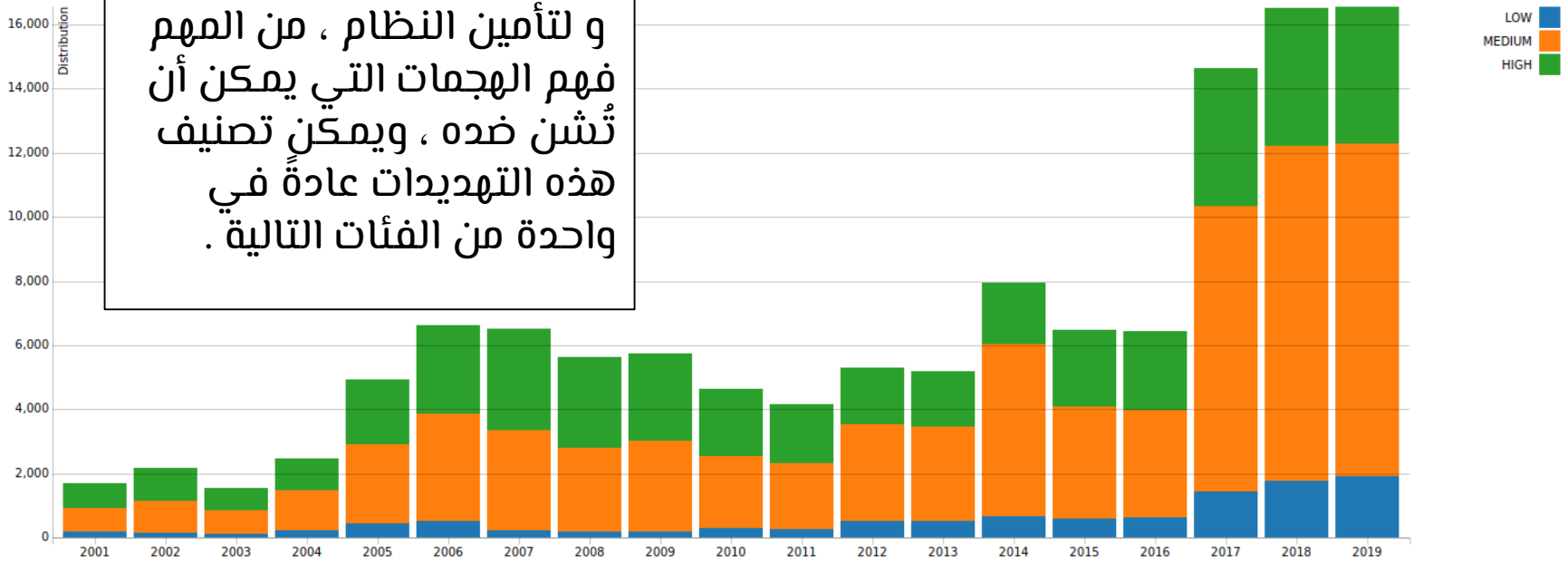
تعريف الحماية الإلكترونية

الحماية الالكترونية هي مجموعة التقنيات والعمليات والممارسات المصممة لحماية الشبكات والأجهزة والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به. يمكن الإشارة إله أيضًا باسم أمن تكنولوجيا المعلومات.

تعريف نقاط الضعف

نقطة الضعف هي ضعف في التصميم أو التنفيذ أو
والتي يمكن استغلالها ، لأداء .التشغيل أو الرقابة الداخلية
.إجراءات غير مصرح بها داخل النظام

و لتأمين النظام ، من المهم فهم الهجمات التي يمكن أن تُشن ضده ، ويمكن تصنيف هذه التهديدات عادةً في واحدة من الفئات التالية .



01

الباب الخلفي (BackDoor)

هو أي وسيلة سرية لتجاوز المصادقة أو الضوابط الأمنية العادية.

03

هجمات الوصول المباشر

مستخدم غير مصرح له يحصل على وصول فعلي إلى جهاز كمبيوتر)خادم.(

05

Multi-vector, polymorphic attack

التهديدات التي تجمعت عدة أنواع من الهجمات وتغيرت شكلها لتجنب ضوابط الأمن عند انتشارها.

02

هجوم قطع الخدمة (DoS)

هجمات رفض الخدمة (DoS) مصممة لجعل جهاز أو مورد شبكة غير متاح للمستخدمين الشرعيين.

04

التنصت

التنصت هو فعل الاستماع الخفي إلى "محادثة " كمبيوتر خاص)اتصال (، عادة بين الخوادم على الشبكة.

09

(Spoofing) انتحال

هو عمل التنكر ككيان صالح من خلال تزوير البيانات ، من أجل الوصول إلى المعلومات أو الموارد التي لا يحق لأحد الحصول عليها.

07

تجاوز الصلاحيات

هو مهاجم لديه مستوى معين من الصلاحية قادر على رفع الامتيازات أو مستوى الصلاحية دون إذن.

التلاعب (Tampering)

هو فعل التعديل الضار للمنتجات .مثل نظام المراقبة.

10

الهندسة الاجتماعية

هو إقناع المستخدم بالكشف عن الأسرار ، من خلال انتحال الهوية

08

الخداع (Phishing)

هي محاولة الحصول على معلومات حساسة مباشرة من المستخدمين من خلال خداع المستخدمين.

06

02

المنهج و الطرق

المنهج المتبع لحل المشاكل المطروحة و الطرق المتبعة

لتحقيق الأمن الفعال ، تحتاج المنظمة إلى تنسيق جهودها في جميع أنحاء نظام المعلومات الخاص بها .تشمل العناصر التالية:

01 أمن الشبكة

02 أمان التطبيق

03 أمن البيانات

04 إدارة الهوية

05 أمن قاعدة البيانات والبنية التحتية

06 امن الهاتف

07 التعافي من الكوارث /تخطيط استمرارية الأعمال

08 تعليم المستخدم

الاستراتيجية الدفاعية

الحماية

يجب تهيئة الأنظمة والشبكات الخاصة بشكل صحيح قدر الإمكان

الكشف والتحليل

تحديد الأنشطة المشبوهة والتحقيق فيها لتأكيد وقوع حادث أمني ، وتحديد أولويات الاستجابة بناءً على التأثير وتنسيق إشعار الحادث

رد الفعل

بعد تحديد المشكلات بسرعة ، يجب الاستجابة لها و العودة إلى حالة الأمان في أسرع وقت ممكن

نشاط ما بعد الحوادث

تحليل ما بعد الحادث ، السبب الجذري واستجابة النضام بقصد التحسين.

أنواع أمان الشبكات

يمكننا حماية النظام لدينا بطرق مختلفة ،
بناءً على نوع الهجوم و غيرها من الأسباب .
هناك العديد من الحلول ، و سنقوم بمناقشة
بعضها في الآتي.

برامج مكافحة الفيروسات ومكافحة البرامج الضارة

يستخدم هذا البرنامج للحماية من البرامج الضارة.حيث يقوم بالمسح بحثًا عن البرامج الضارة ويتعقب الملفات بانتظام بعد ذلك من أجل اكتشاف الحالات الشاذة وإزالة البرامج الضارة وإصلاح الضرر.

منع فقدان البيانات

هو الحفاظ على سرية البيانات والموارد من خلال التأكد من عدم تسرب أي من المعلومات الداخلية من قبل أي من الموظفين إلى العالم الخارجي.

التحليلات السلوكية

من أجل اكتشاف السلوك غير الطبيعي للشبكة ، يجب معرفة شكل السلوك العادي.و ذلك أدوات التحليل السلوكي قادرة على تمييز الأنشطة تلقائيًا .حتى يكون نظام الأمان قادرًا بالتالي على الكشف عن مؤشرات الخرق الأمني المحتملة وعلاجها بسرعة.

الجدار الناري

هذه جزء لا يتجزأ من نظام الشبكات .يعمل كجدار بين شبكتين أو بين جهازين .في الأساس هي مجموعة من القواعد المحددة مسبقًا والتي تستخدم لتحصين الشبكة من الوصول غير المصرح به.

الجهاز المحمول والأمن اللاسلكي

تحتوي الأجهزة اللاسلكية على كل الثغرات الأمنية المحتملة من أي أداة شبكية أخرى و هو المستهدف الأول حيث يمكنها الاتصال بأي شبكة لاسلكية في أي مكان ، مما يتطلب فحصًا إضافيًا.

كشف التسلل والوقاية منه

Intrusion prevention system (IPS)

تفحص هذه الأنظمة حركة مرور البيانات خلال الشبكة لتحديد الهجمات وحظرها ، غالبًا عن طريق ربط توقيعات نشاط الشبكة بقواعد بيانات تقنيات الهجوم المعروفة.

صلاحية التحكم و صلاحية الدخول (ACL)

يجب أن تكون الشبكة قادرًا على منع المستخدمين والأجهزة غير المصرحة منالدخول و الاتصال .حيث فقط المستخدمين المسموح لهم بالوصول إلى الشبكة قادرين على العمل مع المجموعة المحدودة من الموارد التي تم التصريح لهم بها.

المعلومات الأمنية و إدارة الأحداث

Security information and event management (SIEM)

تهدف هذه البرامج أو الأنظمة إلى جمع المعلومات تلقائيًا من مجموعة متنوعة من أدوات الشبكة لتوفير البيانات التي تحتاجها لتحديد التهديدات والرد عليها.

ZABBIX

ICINGA

Nagios®

Nagios
Current Network Status
Last Updated: Tue Jun 7 11:46:01 CDT 2016
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as nagiosadmin
Host Status Totals
Up Down Unreachable Pending
All Problems All Types
Service Status
General
Home
Documentation
Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends
Alerts
History
Summary
Histogram
Notifications
Event Log
System
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Configuration
net-sales-demo.int.netways.de
sales-demo-windows
Network
ZABBIX
Zabbix Global View
Storage IOPs
UTC time
Zabbix Cluster
Detected problems
API calls/s
Value cache misses
Collected values/s
TPS
CPU usage

أمن الإنترنت

يجب التحكم في استخدام الموظفين الإنترنت من أجل منع التهديدات الآتية من الانترنت من استخدام المتصفحات كوسيلة للوصول و لإصابة الشبكة.

أمن التطبيقات

غالبًا ما تكون التطبيقات غير الآمنة هي الوسيلة أو البوابة التي يستطيع المهاجمون من خلالها الوصول إلى الشبكة .حيث يجب القيام بإجراءات و تدابير خاصة لعزلها و تثبطها حين الاستخدام .

الشبكة الافتراضية الخاصة (VPN)

يمكن جعل النظام آمنًا للغاية باستخدام شبكات VPN جنبًا إلى جنب مع استخدام أساليب التشفير للمصادقة و تاكيد حركة مرور البيانات عبر الإنترنت إلى جهاز أو شبكة متصلة عن بُعد.

نصائح أخرى لأمن النظام والشبكة

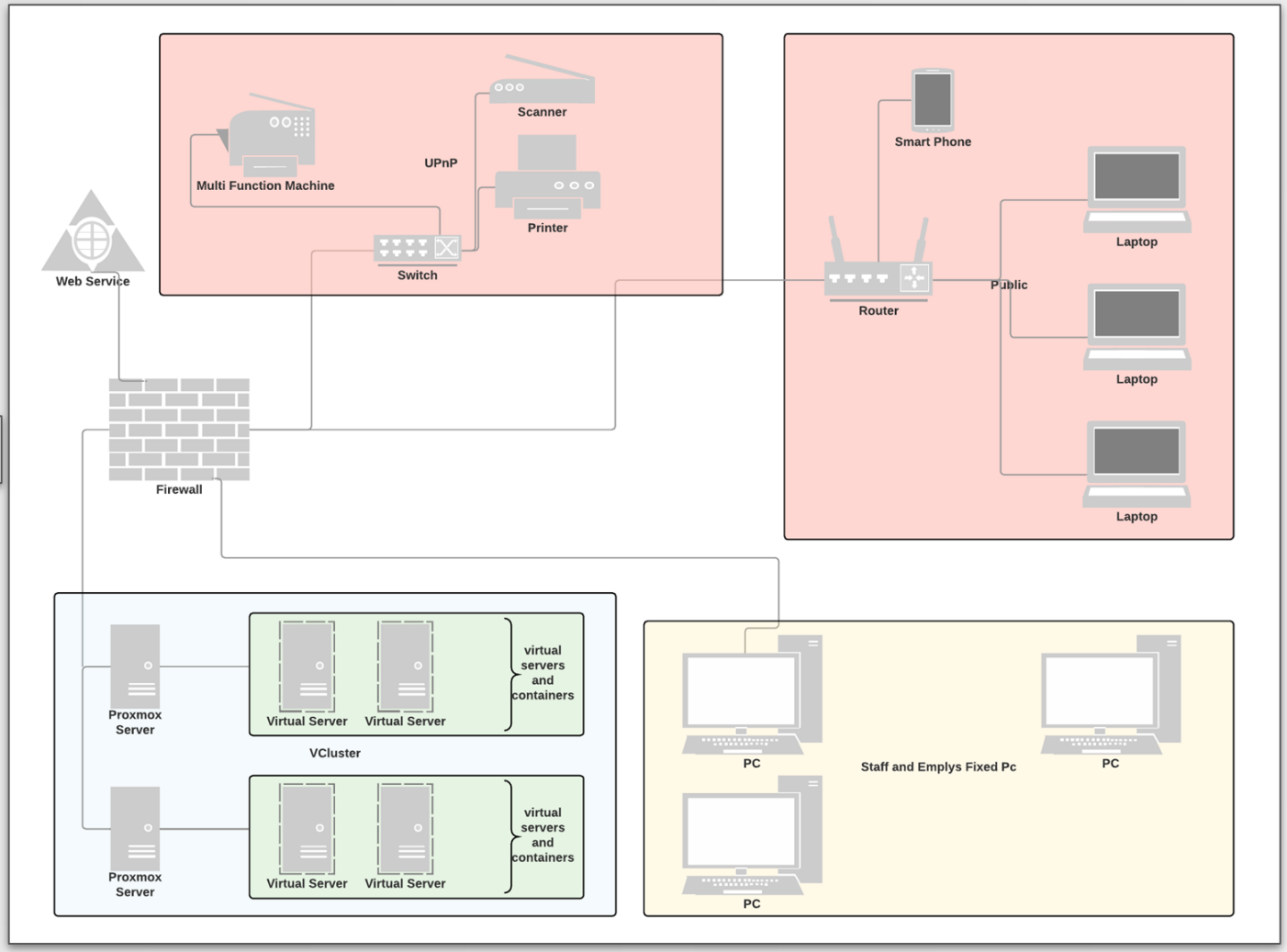
- إنشاء كلمات مرور قوية
- تحديث
- وضع تدابير خاصة لأجهزة الكمبيوتر المحمولة والهواتف المحمولة
- النسخ الاحتياطي في الوقت المحدد
- التصفح الذكي على المواقع
- تكوين الموظفين حول الأمآن و أهميته
- التحكم في الوسائط القابلة للإزالة
- VLAN, SubNets
- UPnP

03

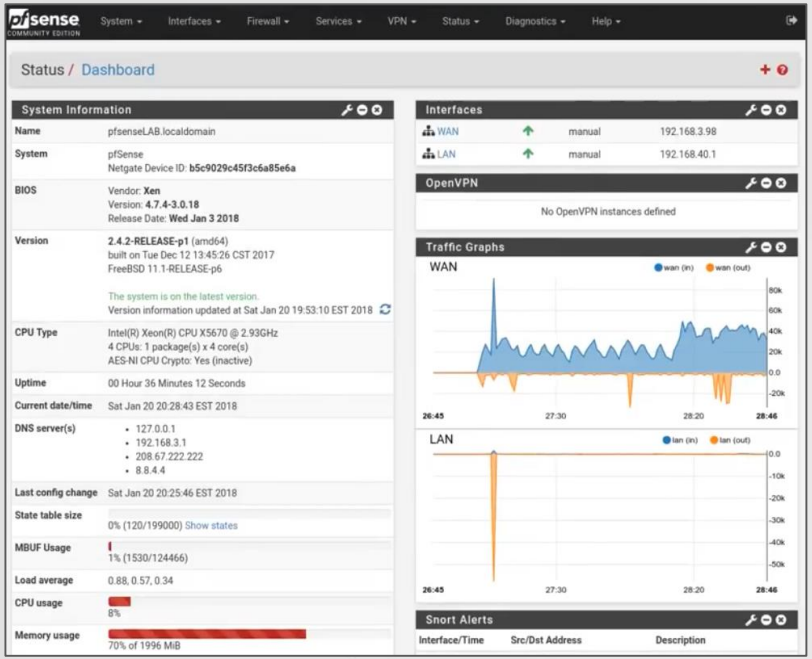
التطبيق العملي

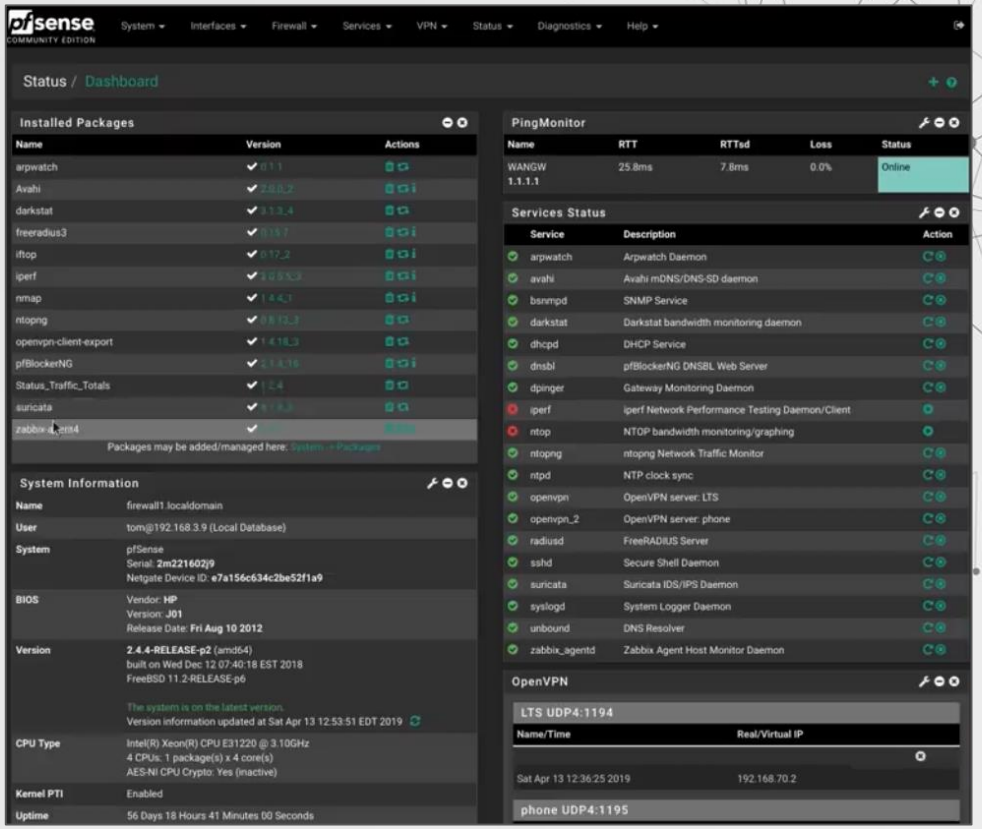
إنشاء منهج حماية في شبكة افتراضية مطابقة للواقع

pfsense
pf BlockerNG
SNORT
SquidGuard
SQUID
OPENVPN
docker
PROXMOX
ZABBIX
portainer
BIND 9
LXC

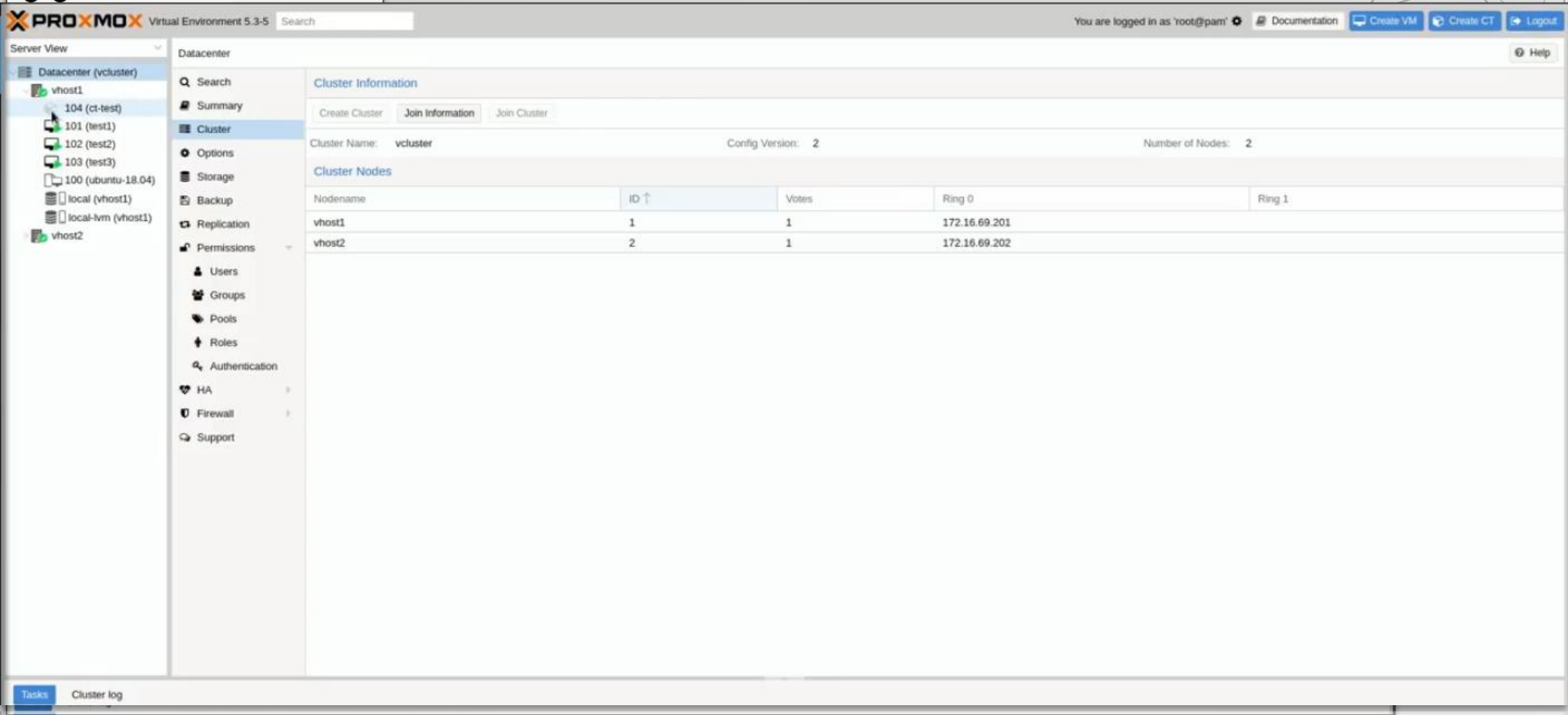

Multi Function Machine
UPnP
Scanner
Printer
Switch
Web Service
Smart Phone
Router
Public
Laptop
Laptop
Laptop
Firewall
Proxmox Server
Virtual Server
Virtual Server
virtual servers and containers
VCluster
Proxmox Server
Virtual Server
Virtual Server
virtual servers and containers
PC
Staff and Emplys Fixed Pc
PC
PC

الجدار الناري

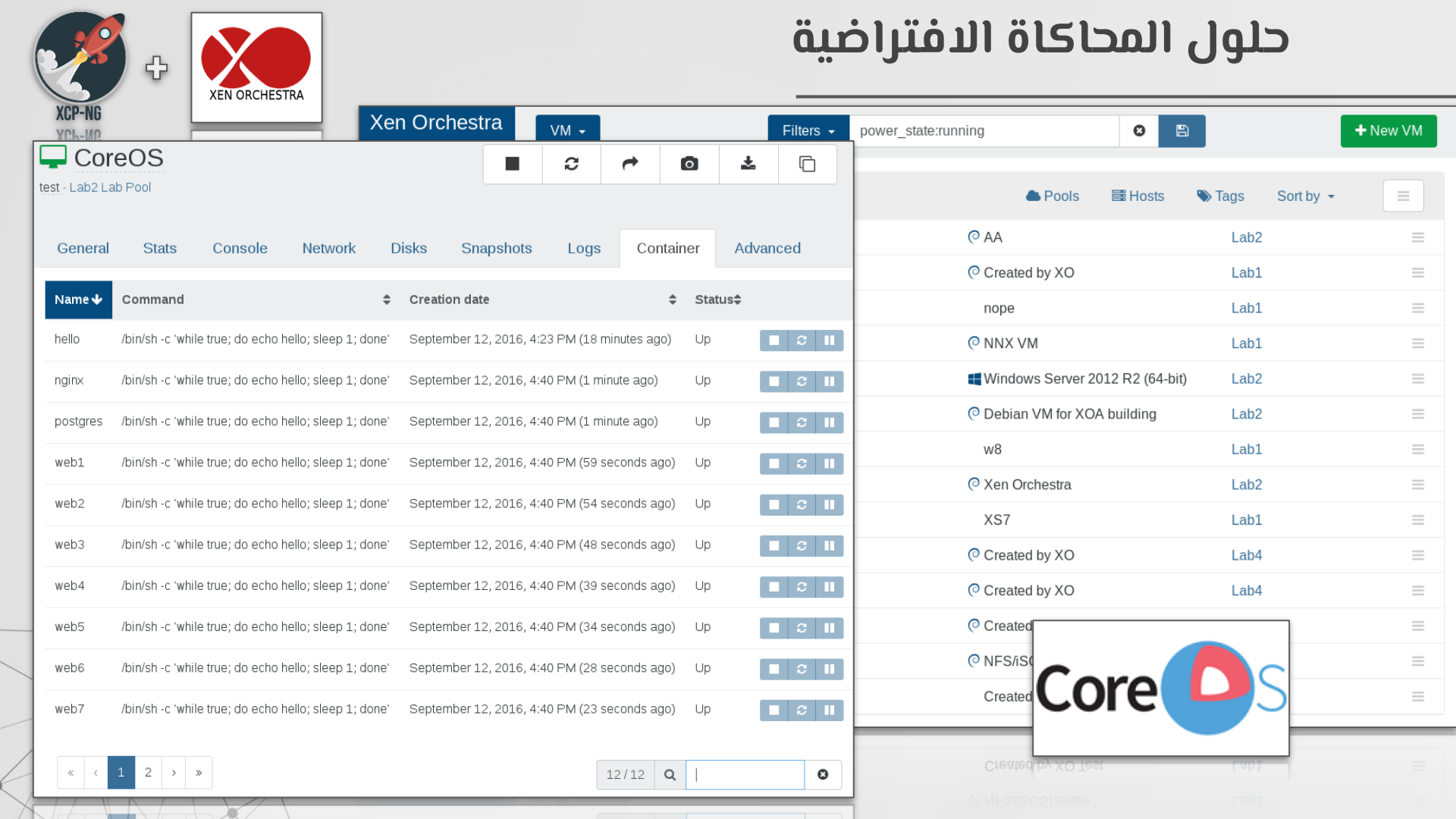




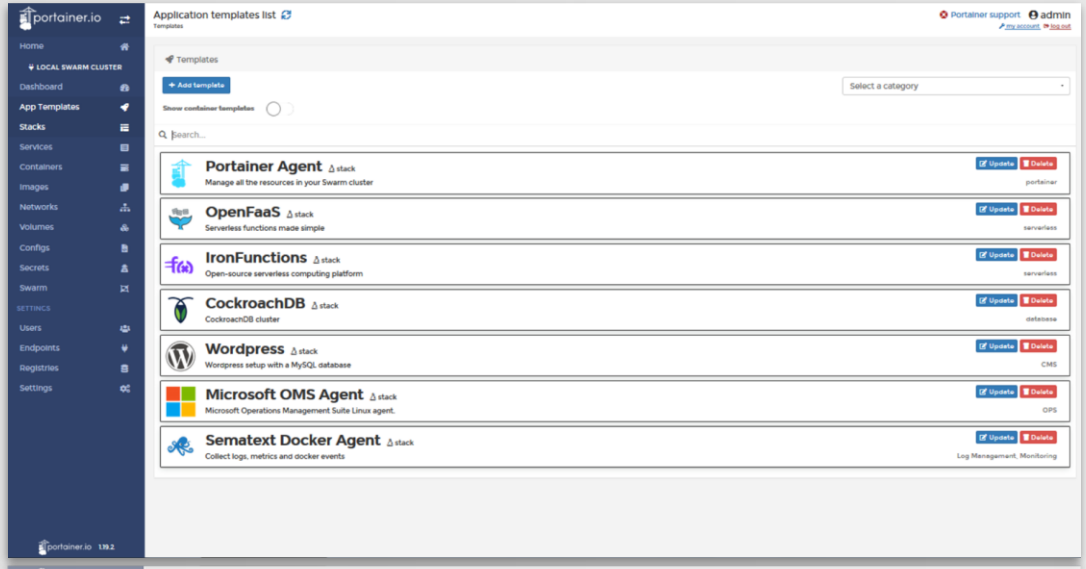
حلول المحاكاة الافتراضية

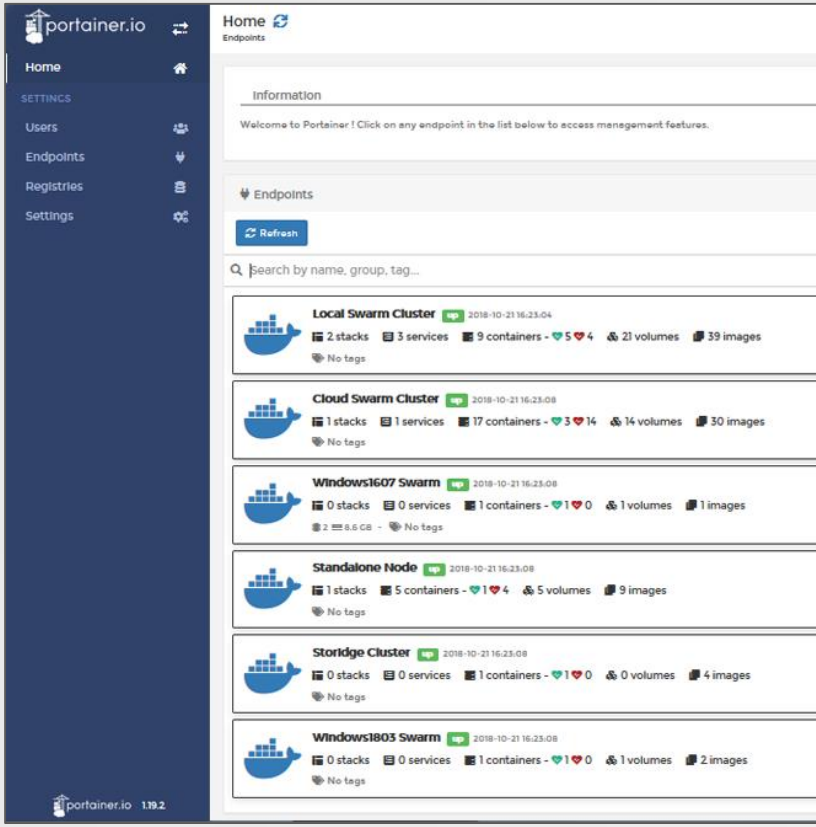


حلول المحاكاة الافتراضية



Docker Containers





حلول ال IPS IDS

Open *icmp.rules /etc/snort/rules Save

```
#-----------
# ICMP RULES
#-----------
#
# Description:
# These rules are potentially bad ICMP traffic.  They include most of the
# ICMP scanning tools and other "BAD" ICMP traffic (Such as redirect host)
#
# Other ICMP rules are included in icmp-info.rules

alert icmp any any -> 192.168.1.23 any (msg: "ICMP Packet found"; sid: 10000001; )
#alert tcp any any -> 192.168.1.23 8001 (msg: "HTTP Packet found"; sid: 10000002; )
#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP ISS Pinger"; itype: 8; content:"ISSPNGRQ"; depth:32; reference:arachnids,158; classtype:attempted-recon; sid:465; rev:3;)
#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; icode:0; itype:8; content:"ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"; depth:32; reference:arachnids,311; classtype:attempted-recon; sid:466; rev:4;)
#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Nemesis v1.1 Echo"; dsize:20; icmp_id:0; icmp_seq:0; itype:8; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; reference:arachnids,449; classtype:attempted-recon; sid:467; rev:3;)
```

2018-01-20 20:27:25			Leak					
2018-01-20 20:27:20	2	TCP	Potentially Bad Traffic	192.168.3.9	54201	192.168.3.98	5432	1:2010939 ET POLICY Suspicious inbound to PostgreSQL port 5432
2018-01-20 20:27:20	2	TCP	Potentially Bad Traffic	192.168.3.9	54200	192.168.3.98	5432	1:2010939 ET POLICY Suspicious inbound to PostgreSQL port 5432

حلول الـ: SIEM

Zabbix templates, modules & more

Log in

Search…

Advanced Search

Applications
Cloud
Databases
Network Appliances
Network Devices
Official Templates
Operating Systems
Power (UPS)
APC
Eaton
Eaton Powerware
Emerson NP
Engetron
Entel
Gamatronic
HP
Ippon
Legrand Inform
Others
Powercom
Tripplite
UPS Templates
Printers
SCADA, IoT, Energy, Home Automation, Industrial monitoring
Server Hardware
Storage Devices

APC

Add new listing

APC Networ
This is Zabbix 2.0+
Supports: AP9630
parameters li ...
Type Template

APC PDU Te
Tested in models A
/magaiverpr/templa
Type Template

APC PDU N
UPDATE: Uploade
This APC Template
loa ...
Type Template

APCUPSd
Monitoring APC UP
APCUPSd. На рус
Напряжение на вх
Type Template

APC UPS (U

Applications
Cloud
Databases
Network Appliances
Network Devices
Official Templates
Operating Systems
Power (UPS)
Printers
Brother
Canon
HP
Konica
Kyocera
Lexmark
OKI
Ricoh
Samsung
SAMSUNG
Universal
Xerox
SCADA, IoT, Energy, Home Automation, Industrial monitoring
Server Hardware
Storage Devices
Telephony
Unsorted
Virtualization
Zabbix
Recently Added
Recently Updated
Popular

Printers

Triumph-Adler (0)
Panasonic (0)
Universal (1)
Lexmark (13)
Konica (3)
Ricoh (5)
Kyocera (8)
SAMSUNG (1)
Ricoh (0)
Brother (3)
Samsung (4)
OKI (5)
Canon (9)
HP (12)
Xerox (20)

Add new listing | Add Category

Results 1 - 20 of 27 **This Category** · All Listings

Universal Printer Template Popular

This template is valid for all printer manufacturers and all devices that are attached to the RFC1759 and RFC3805 (Printer-MIB). The serial number, trays, toner and output trays are discovered (LLD) and monitored. The counter and filling levels are displ ...

Type Template Min Zabbix version 2.4.x

Generic printers monitoring template (Any brand) Popular

A simple generic template to monitor printers tested on 3.2, but minimum version should be 2.0 as SNMP LLD and trigger dependencies are available since this version Use of default ICMP template (provide with zabbix) and standard PRINTER-MIB (1.3.6 ...

Type Template Min Zabbix version 2.0.x

Printer SNMP universal Popular

Corrected SNMPv2 printer monitoring template for Zabbix 4.0 Also add one Graph for printed page counter Just add template to your library. Please, don't add if your version is < 4

Type Template Min Zabbix version 4.0.x

Dell Laserprinter

Good day! This is my first attempt at creating a public template. As far as I'm aware, it should be operatable on multiple Dell laser printers. The model this was created on was the 'Dell 3115CN'. Confirmed models that are supported: Dell 31

Type Template Min Zabbix version 3.4.x

Support Share

Group Zabbix servers Host Zabbix server Edit dashboard

Zoom out Last 1 hour

High	Average	Warning	Information	Not classified
0	1	4	0	3

ailability

	Zabbix agent	SNMP	JMX	IPMI
	3	9	0	0
able	0	0	0	0
	101	8	1	0
	104	17	1	0

2
1.6
1.2
0.8
0.4

10-03 14:40 10-03 14:49 10-03 14:59 10-03 15:08 10-03 15:18 10-03 15:28

rocessor load (5 min average per core)) max(Zabbix server: Processor load (5 min average per c...

Debug

SNMP
Simple Network Management Protoco

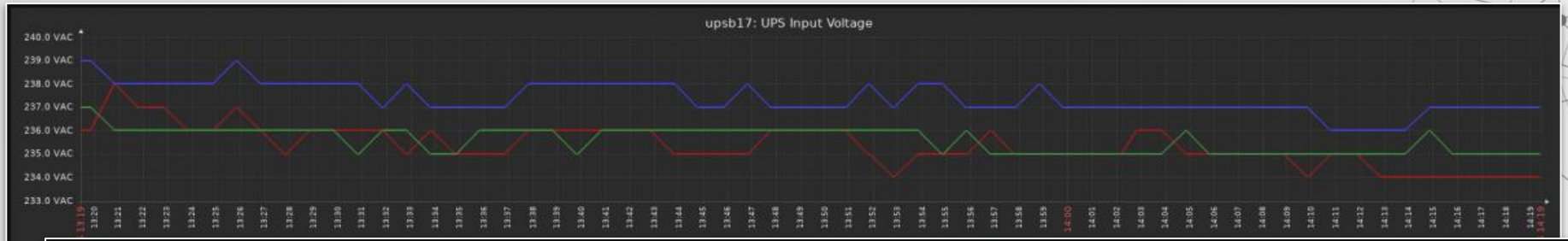
ZABBIX

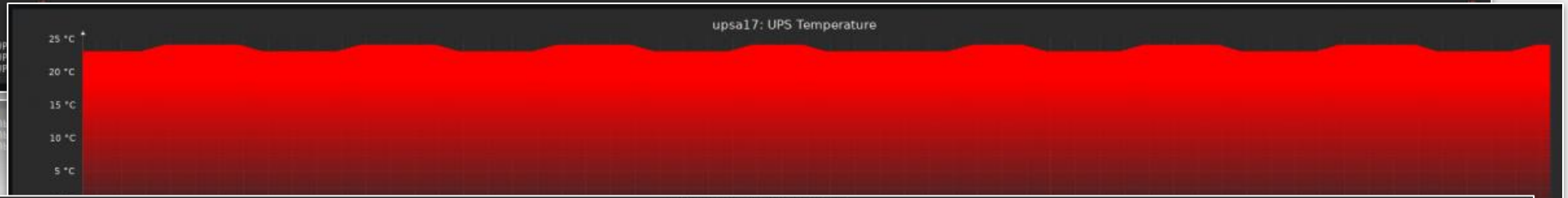
حلول الـ: SIEM

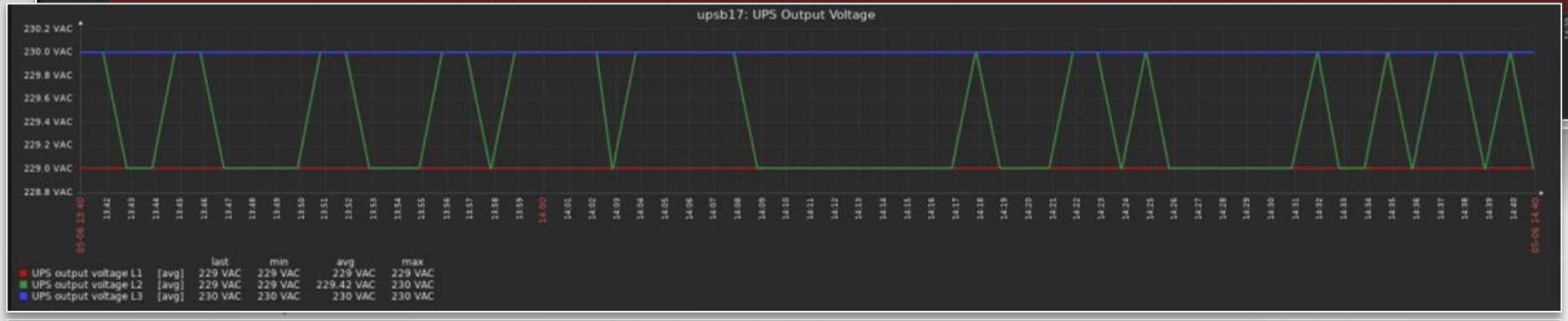
مثال علي
UPS

ZABBIX

SNMP
Simple Network Management Protocol







04

حماية التطبيقات

من جانب البرمجة و متابعة والتصحيح

إرشادات أمان البرامج

على الرغم من عدم وجود طرق شاملة للتطوير الآمن للبرامج ، إلا أن هناك بعض الإرشادات العامة التي يمكن استخدامها للمساعدة .حيث تمتد هذه الإرشادات في كل مرحلة من دورة حياة تطوير البرمجيات.

لا تثق في المستخدم

```
<?xml version="1"?>
    <!DOCTYPE stockCheck [ <!ENTITY
xxe SYSTEM "file:///etc/passwd"> ]>
<stockCheck><productId>&xxe;
</productId></stockCheck
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
```

أربعة ثغرات أمنية تأتي من الوثوق بالمستخدم أكثر من اللازم :
الحقن (injection)، الكيانات الخارجية لـ XXE XML، البرمجة النصية عبر المواقع (XSS)، و Deserializationغير الآمن.

اعتماد حل مبدأ الأقل ثقة .حيث يجب التحقق من صحة أي بيانات (validation) تدخل إلى التطبيق الخاص بك قبل استخدامه.

اعتماد مبدأ (KiSS)اجعلها آمنة وبسيطة

بسيط هو أسهل للتأمين .حافظ على تصميماتك بسيطة ، حيث يمكن تأمينه بسهولة.

لسوء الحظ ، يفكر بعض المطورين في التصميم ويضيفون أشياء كثيرة يعتقد أنه قد يحتاجها ، ومع مرور الوقت قد ينمو التطبيق ويصبح عملاقًا معقدًا يصعب فهمه ويصعب تأمينه.

الاوتوماتيـكية
Automation

طريقة فعالة لدمج الأمن في التعليمات البرمجية الخاصة بك من خلال الأتمتة .الأتمتة يقلل من فرصة الخطأ البشري.حيث يقوم بعمليات مهمة آليا ويمكنه القضاء على المتغيرات الخطيرة.

بدون التشغيل الآلي ، لا يمكن تحقيق الأمن الحقيقي على نطاق واسع . يساعد التنفيذ التلقائي في تضمين الأمان في وقت مبكر وغالبًا في عملية تطوير البرامج.

و هدا ايضا يتعلق بالاختبارات التلقائية فيقدم تعليقات سريعة.

نمذجة التهديد

نمذجة التهديد هي ممارسة فحص تصميم البرنامج للعثور على الأماكن التي يمكن للمهاجمين اختراقها .نمذجة التهديد تساعد المطورين على فهم كيف يمكن للمهاجمين اختراق البرامج الخاصة بهم حتى يتمكنوا من بناء الدفاعات المناسبة .و من بعض النقاط المساعدة هي:

- توثيق كيفية عمل التطبيق ، مع التركيز على تدفق البيانات من خلال التطبيق.
- ابحث عن التهديدات ضد التطبيق من خلال متابعة تدفق البيانات وتحديد الأماكن التي تكون ضعيفة .مع الاطلاع علي قواعد بيانات الهجمات الواضحة في الصورة
- معالجة التهديدات

MITRE | ATT&CK

Matrices | Tactics | Techniques | Mitigations | Groups | Software | Resources | Blog | Contribute | Search site

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense	Steal Web Session	System Owner/User			Standard Non-Application		

التشفير الصحيح

عندما يتم بشكل غير صحيح ، يكون مضيعة أو حتى يفتح ثغرات .إن ارتكاب أخطاء تشفير شائعة يؤدي إلى كارثة عندما يكتشف المهاجمون .في ما يلي بعض المهام والواجبات المتعلقة بالتشفير:

- عدم تخزين مفاتيح التشفير في نفس المكان الذي تشفر فيه البيانات.
- عدم كتابة رمز التشفير ثابت في التعليمات البرمجية.
- لا تنشئ خوارزميات التشفير الخاصة بك أو تستخدم الخوارزميات المعطلة .أو السهلة الفك.
- لا تستخدم خوارزميات جيدة معروفة توفرها المكتبة التي تستعملها (AES-256، ....، PBKDF2) بل يجب اضافة المتغيرات Salting.
- تشفير البيانات في النقل الخارجي وفي العبور.

MessagePack

Let's Encrypt

JWT

JSON 27 bytes

“schema”: 0 }

A6 schema 00

6-byte string

integer 0

Encoded

PASTE A TOKEN HERE

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

اتبع مشروع أمان تطبيق الويب المفتوح

Open Web Application Security Project (OWASP)

هي منظمة تركز على تحسين أمن البرمجيات .تتمثل مهمتها في جعل أمان البرامج مرئيًا ، بحيث يتمكن الأفراد والمؤسسات من اتخاذ قرارات والتدابير اللازمة .و تقوم بتشكيلها في شكل قائمة ملخصة.

و من المستغرب ،القائمة لا تتغير كثيرا .للأسف ، العديد من المشكلات نفسها تظل عامًا بعد عام ، على الرغم من الوعي الأمني المتزايد في مجتمع المطورين.

البقاء على آخر التحديثات
و مواكبة أحدث نقاط الضعف

بالإضافة إلى تحديث نظام التشغيل ، يلزم تحديث إطار عمل التطبيق ومكتبات الجهات الخارجية أيضًا.

تحتوي المكتبات و الاطارات ، مثلها مثل أنظمة التشغيل ، على نقاط ضعف .إذا تم دعمها بشكل صحيح ، فسيتم أيضًا تصحيحها وتحسينها بسرعة .نظرًا لذلك ، من المهم التأكد من استخدم أحدث إصدار ثابت.

و ايضا البقاء علي اطلاع علي أحدث نقاط الضعف المتواجدة و تحديث برامجك.

05

البرامج المستخدمة في المكتبات و جاهزيتها للربط الشبكي

سوف نقوم بسرد بعض التقنيات المستعملة في الأنظمة المكتبية (ILS) للتواصل و الربط بينها ,و كمثال . Koha , evergreen ILS

- يتم استخدام مارك لنقل السجلات ومعلومات الطلب والبيانات إلى أنظمة المكتبة .
- حيث ترسل عبر بناء XMLلتوصيل أي نوع من البيانات تقريبًا علي عدة أشكال منها.
  - MODS
  - MARCXML
  - Dublin Core

```xml
<?xml version="1.0"?>
<sru:searchRetrieveResponse xmlns:sru="https://www.loc.gov/zing/srw/"
  xmlns:diag="https://www.loc.gov/zing/srw/diagnostic/"
  xmlns:xcql="https://www.loc.gov/zing/cql/xcql/" xmlns:dc="http://purl.org/dc/elements/1.1/">
  <sru:version>1.1</sru:version>
  <sru:numberOfRecords>4</sru:numberOfRecords>
  <sru:records>
    <sru:record>
      <sru:recordSchema>info:srw/schema/1/dc-v1.1</sru:recordSchema>
      <sru:recordPacking>XML</sru:recordPacking>
      <sru:recordData>
        <sru:dc>
          <sru:title>Darwinism</sru:title>
          <sru:creator>Dennett</sru:creator>
          <sru:subject>The rule of the Local is a basic principle of Darwinism -  </sru:subject>
        </sru:dc>
      </sru:recordData>
      <sru:recordNumber>1</sru:recordNumber>
    </sru:record>
  </sru:records>
</sru:searchRetrieveResponse>
```

- Z39.50هو بروتوكول البحث والاسترجاع .لكن هي تقنية ما قبل الويب ,و لهادا هناك محاولات لتحديثها لتلائم البيئة الحديثة بشكل أفضل .تندرج هذه المحاولات تحت اسم ZING Z39.50.
- ومنها SRU/SRWالتي تسقط بروتوكول اتصالات Z39.50)استبداله بـ (HTTPحيث يتم استخدام HTTP GET
  - WEBSITE/XML/sru.php?version=1.1&operation=search Retrieve&query=dc.title=Darwinism
- و ايضا OpenURLمثل SRU/SRWلنقل المعلومات الببليوغرافية عبر الويب

وشكرا على حسن الاصغاء و المتابعة

و المجال مفتوح للمناقشة والأسئلة