TRAINNING EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER - SECURITY IMPLEMENTATION

Progresso do curso

Módulo 16. Hacking Wireless Networks

Módulo 17. Hacking Mobile Applications

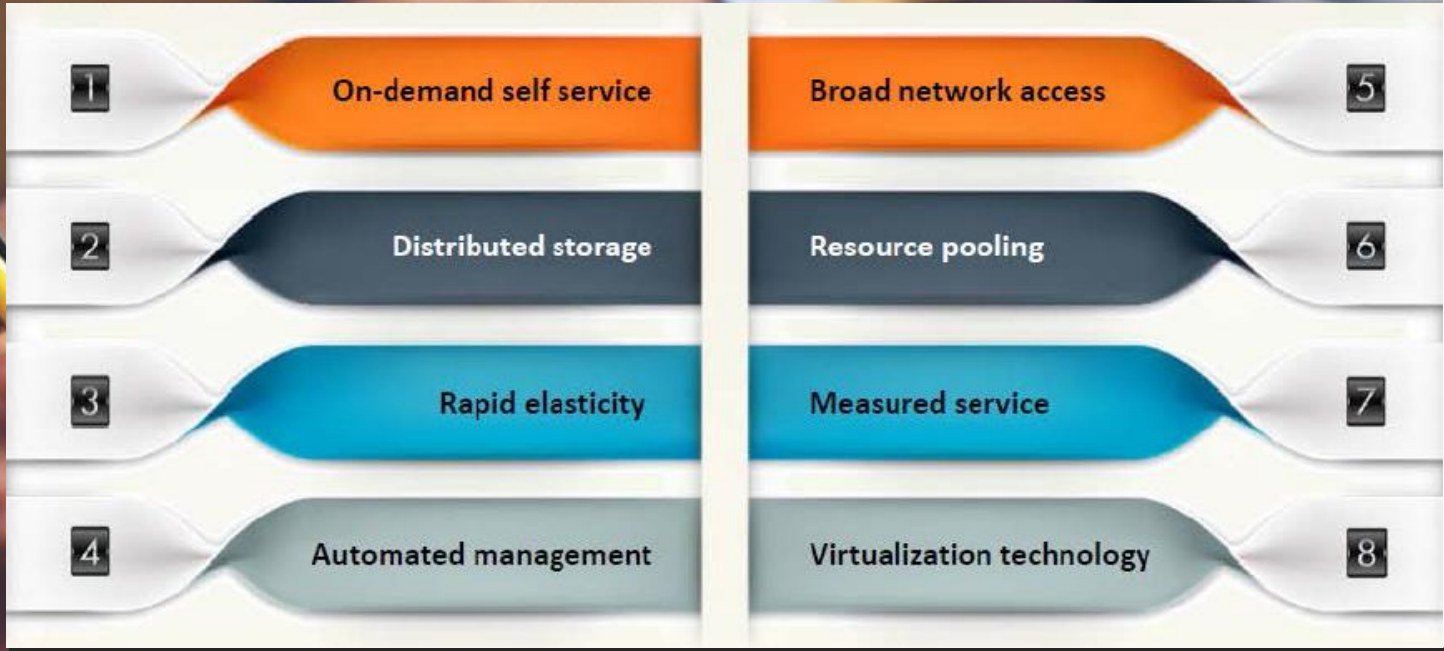
Módulo 18. IoT & OT Hacking

Módulo 19. Cloud Computing

Módulo 20. Cryptography

Conceitos de Cloud Computing:

A computação em nuvem é um tipo de computação baseada na Internet que fornece recursos compartilhados de processamento e dados para computadores e outros dispositivos sob demanda. É um modelo para permitir acesso universal sob demanda a um pool compartilhado de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente fornecidos e liberados com o mínimo esforço.



CEHv12 (ANSI)

19.Cloud Computing

Benefícios do Cloud Computing

Economic

- Business agility
- Less maintenance costs
- Acquire economies of scale
- Less capital expense
- Huge storage facilities for organizations
- Environmentally friendly
- Less total cost of ownership
- Less power consumption

Operational

- Flexibility and efficiency
- Resiliency and redundancy
- Scale as needed
- Less operational problems
- Deploy applications quickly
- Back up and disaster recovery
- Automatic updates

Staffing

- Streamline processes
- Well usage of resources
- Less personnel training
- Less IT Staff
- Multiple users utilize resources on cloud
- Evolution to new model of business
- Simultaneous sharing of resources

Security

- Less investment in security controls
- Efficient, effective, and swift response to security breaches
- Standardized, open interface to managed security services (MSS)
- Effective patch management and implementation of security updates
- Better disaster recovery preparedness
- Ability to dynamically scale defensive resources on demand
- Resource aggregation offers better manageability of security systems
- Rigorous internal audit and risk assessment procedures

Modelos de Serviço

Infrastructure-as-a-Service (IaaS)

- Provides **virtual machines** and other abstracted hardware and operating systems which may be **controlled through a service API**
- E.g. Amazon EC2, Go grid, Sungrid, Windows SkyDrive, etc.

Platform-as-a-Service (PaaS)

- Offers **development tools**, **configuration management**, and **deployment platforms** on-demand that can be used by subscribers to **develop custom applications**
- E.g. Intel MashMaker, Google App Engine, Force.com, Microsoft Azure, etc.

Software-as-a-Service (SaaS)

- Offers **software to subscribers** on-demand **over the Internet**
- E.g. web-based office applications like Google Docs or Calendar, Salesforce CRM, etc.

Modelos de Serviço

Infrastructure as a service (IaaS)

No modelo mais básico de serviço em nuvem e de acordo com o IETF (Internet Engineering Task Force) o IaaS oferece computadores físicos ou (mais frequentemente) máquinas virtuais de outros recursos. IaaS refere-se a serviços on-line que abstraem o usuário a partir dos detalhes da infraestrutura como recursos físicos de computação, localização, particionamento de dados, dimensionamento, segurança, backup etc. Um hypervisor, como Xen, o Oracle VirtualBox, o Oracle VM, KVM, VMware ESX/ESXi ou Hyper-V executam as máquinas virtuais como convidados.

Modelos de Serviço

Platform as a service (PaaS)

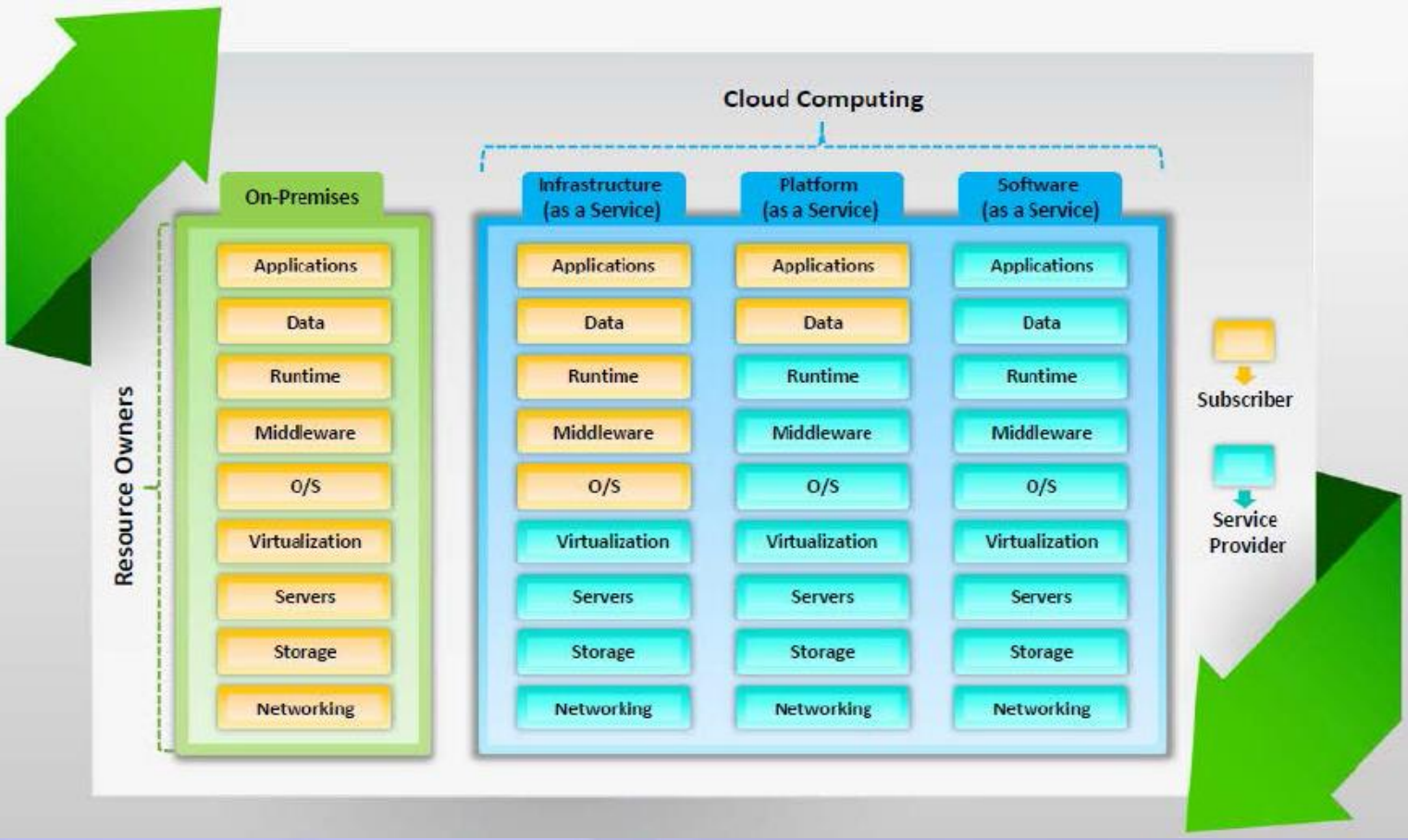
Fornecedores de PaaS oferecem um ambiente de desenvolvimento para desenvolvedores de aplicativos. O provedor tipicamente desenvolve kit de ferramentas e padrões para o desenvolvimento. Nos modelos de PaaS, provedores de nuvem entregam uma plataforma de computação, tipicamente incluindo o sistema operacional, ambiente de execução da linguagem de programação, banco de dados e servidor web.

Modelos de Serviço

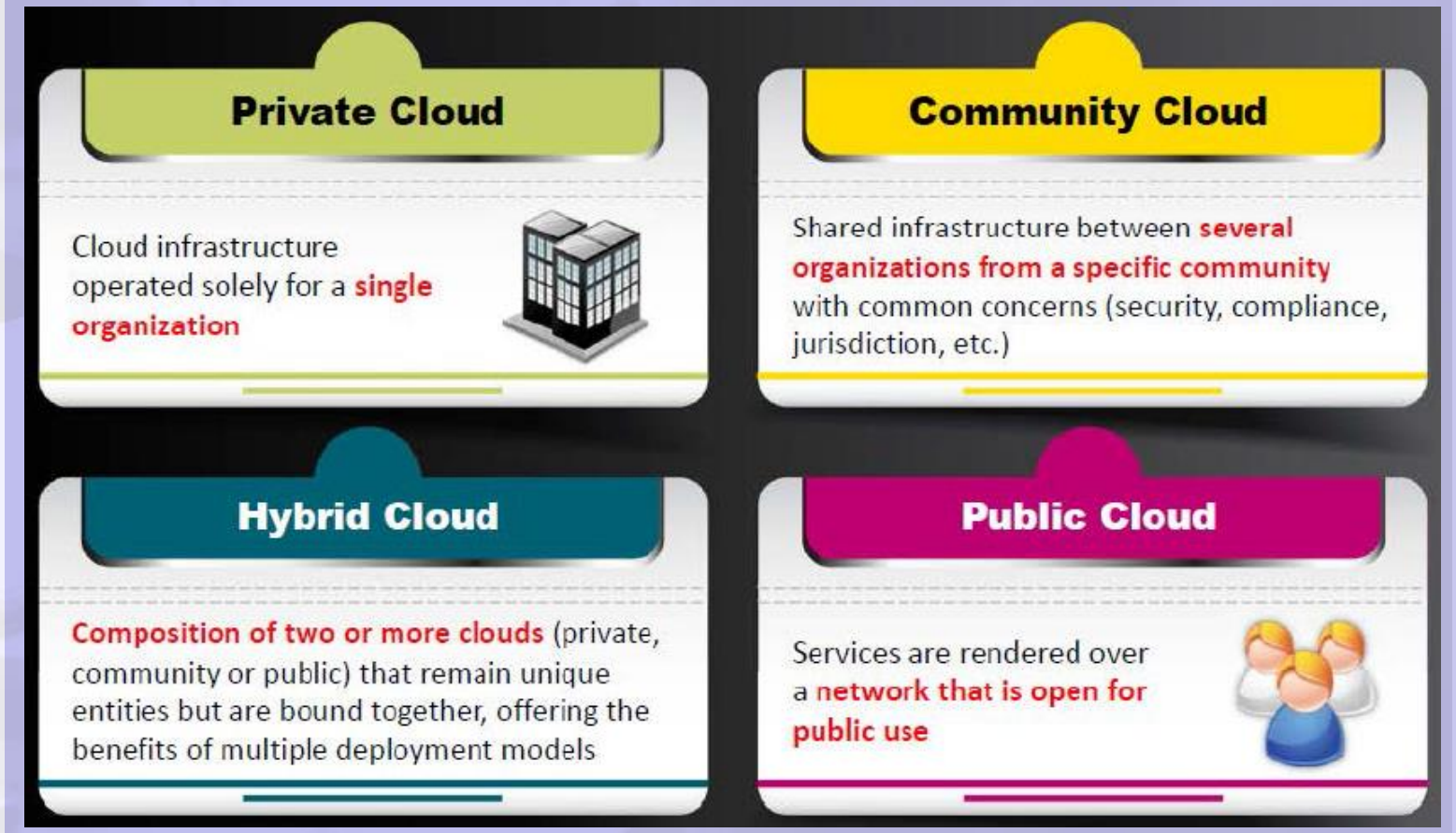
Software as a service (SaaS)

No software como um modelo de serviço (SaaS), os usuários ganham acesso ao software de aplicações e bancos de dados. Os provedores de nuvem gerenciam a infraestrutura e plataformas que rodam os aplicativos. O SaaS é muitas vezes referido como "software on-demand" e normalmente é fixado o preço em uma base de pay-per-use ou usando uma taxa de subscrição.

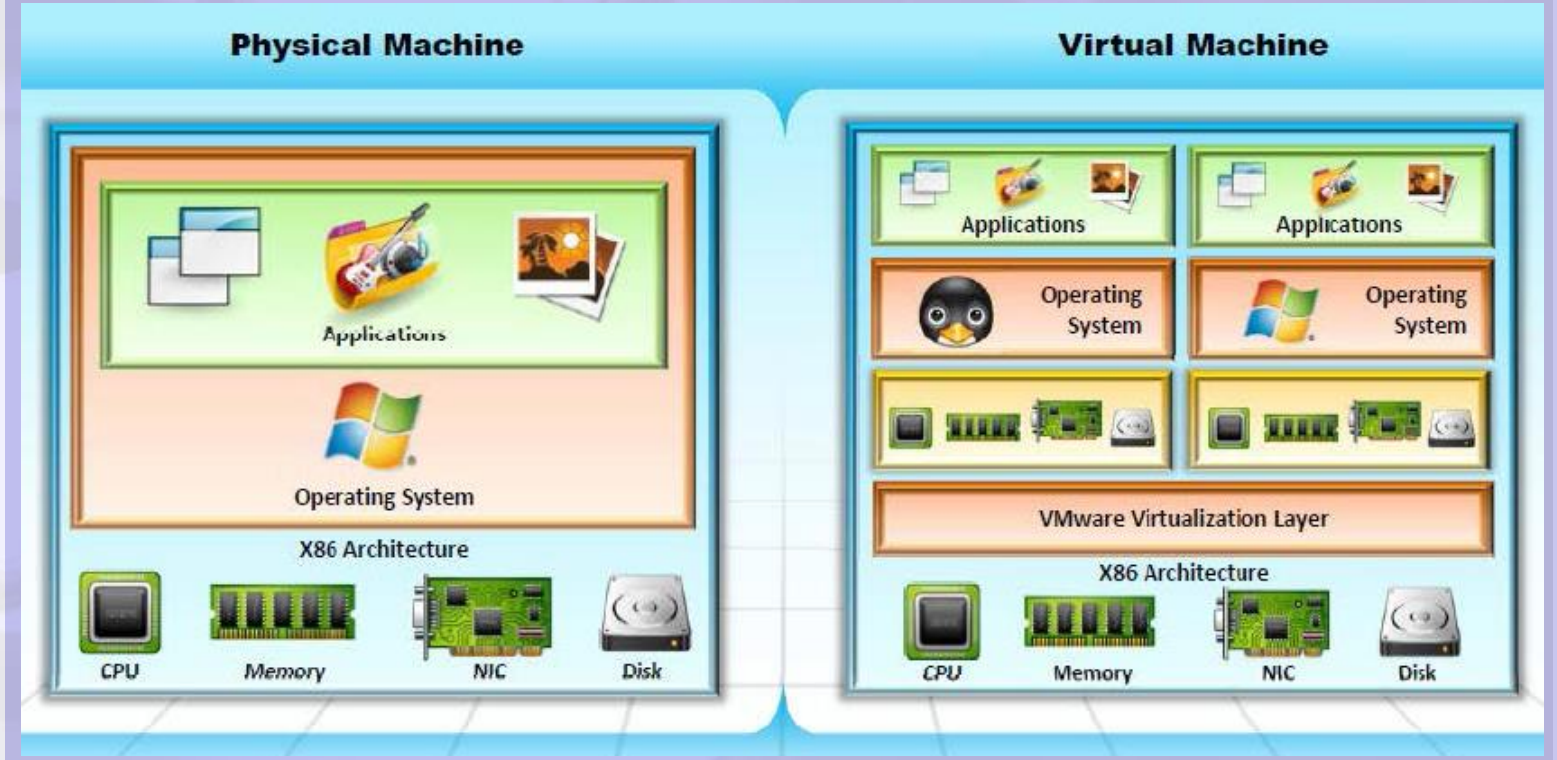
Segregação de responsabilidade



Modos de implementação



Entendendo a virtualização



Ameaças de Cloud Computing

1. Data breach/loss
2. Abuse of cloud services
3. Insecure interfaces and APIs
4. Insufficient due diligence
5. Shared technology issues
6. Unknown risk profile
7. Inadequate infrastructure design and planning
8. Conflicts between client hardening procedures and cloud environment
9. Loss of operational and security logs
10. Malicious insiders
11. Illegal access to cloud systems
12. Privilege escalation
13. Loss of business reputation due to co-tenant activities
14. Natural disasters
15. Hardware failure
16. Supply chain failure
17. Modifying network traffic
18. Isolation failure
19. Cloud provider acquisition
20. Management interface compromise
21. Network management failure
22. Authentication attacks
23. VM-level attacks
24. Lock-in
25. Licensing risks
26. Loss of governance
27. Loss of encryption keys
28. Risks from changes of Jurisdiction
29. Undertaking malicious probes or scans
30. Theft of computer equipment
31. Cloud service termination or failure
32. Subpoena and e-discovery
33. Improper data handling and disposal
34. Loss or modification of backup data
35. Compliance risks
36. Economic Denial of Sustainability (EDOS)

Segurança de Cloud Computing

01	Applications	SDLC. Binary Analysis, Scanners, Web App Firewalls, Transactional Sec
02	Information	DLP, CMF, Database Activity, Monitoring, Encryption
03	Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
04	Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
05	Trusted Computing	Hardware & software RoT & API's
06	Computer and Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/Log Management, Encryption, Masking
07	Physical	Physical Plant Security, CCTV, Guards

Melhores práticas para segurança

- Enforce **data protection**, **backup**, and **retention** mechanisms
- Implement strong **authentication**, **authorization** and **auditing** mechanisms
- Enforce **SLAs** for patching and vulnerability remediation
- Check for **data protection** at both design and runtime
- Vendors should regularly undergo **AICPA SAS 70 Type II audits**
- Implement **strong key generation**, storage and management, and destruction practices
- Verify one's own cloud in **public domain blacklists**
- Monitor the **client's traffic** for any malicious activities
- Enforce **legal contracts** in employee behavior policy
- Prevent unauthorized server access using **security checkpoints**
- Prohibit **user credentials sharing** among users, applications, and services
- Disclose applicable **logs** and **data** to customers

Melhores práticas para segurança

- Analyze **cloud provider security policies** and SLAs
- Assess security of **cloud APIs** and also log customer **network traffic**
- Ensure that cloud undergoes regular **security checks and updates**
- Ensure that physical security is a **24 x 7 x 365** affair
- Enforce **security standards** in installation/ configuration
- Ensure that the memory, storage, and network access is **isolated**
- Leverage strong **two-factor authentication** techniques where possible
- Baseline **security breach notification** process
- Analyze **API dependency chain software** modules
- Enforce stringent **registration and validation process**
- Perform vulnerability and configuration **risk assessment**
- Disclose infrastructure information, **security patching**, and firewall details

Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.