PenTest em Ambientes Cloud PT.1

JOAS ANTONIO

SOBRE

- Conceitos básicos de Cloud;
- Material de estudo prático de PenTest;
- Foca no AWS e Azure;

Autor

- Joas Antonio;
- Entusiasta em Segurança da Informação;

Conceitos de Cloud

O QUE É CLOUD?

- Computação em nuvem (em inglês, cloud computing), é a disponibilidade sob demanda de recursos do sistema de computador , especialmente armazenamento de dados e capacidade de computação, sem o gerenciamento ativo direto do utilizador. O termo geralmente é usado para descrever centros de dados disponíveis para muitos utilizadores pela Internet. Nuvens em grande escala, predominantes hoje em dia, geralmente têm funções distribuídas em vários locais dos servidores centrais. Se a conexão com o utilizador for relativamente próxima, pode ser designado um servidor de borda.

- O armazenamento de dados é feito em serviços que poderão ser acedidos de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas ou de armazenar dados. O acesso a programas, serviços e arquivos é remoto, através da Internet - daí a alusão à nuvem. O uso desse modelo (ambiente) é mais viável do que o uso de unidades físicas.

- Num sistema operacional disponível na Internet, a partir de qualquer computador e em qualquer lugar, pode-se ter acesso a informações, arquivos e programas num sistema único, independente de plataforma. O requisito mínimo é um computador compatível com os recursos disponíveis na Internet. O PC torna-se apenas um chip ligado à Internet — a "grande nuvem" de computadores — sendo necessários somente os dispositivos de entrada (teclado, rato/mouse) e saída (monitor).

TIPOS DE CLOUDS

- Atualmente, a computação em nuvem é dividida em dez tipos:

- IaaS - Infrastructure as a Service ou Infraestrutura como Serviço (em português): refere-se a serviços online que fornecem APIs de alto nível usadas para desreferenciar vários detalhes de baixo nível da infraestrutura de rede subjacente, como recursos de computação física, localização, particionamento de dados, dimensionamento, segurança, backup etc. Executa as máquinas virtuais como convidados. Pools de hipervisores dentro do sistema operacional de nuvem podem suportar um grande número de máquinas virtuais e a capacidade de escalonar os serviços de acordo com os diferentes requisitos dos clientes. Os contentores Linux são executados em partições isoladas de um único kernel do Linux em execução diretamente no hardware físico. Cgroups e namespaces do Linux são as tecnologias subjacentes do kernel do Linux usadas para isolar, proteger e gerenciar os contentores. Contentorização oferece maior desempenho do que virtualização, porque não há sobrecarga de hipervisor. Além disso, a capacidade do contentor é dimensionada automaticamente de maneira dinâmica com a carga computacional, o que elimina o problema de provisionamento excessivo e permite o facturamento baseado em uso.As nuvens de IaaS geralmente oferecem recursos adicionais, como uma biblioteca de imagem de disco de máquina virtual, armazenamento bruto de bloco, armazenamento de arquivos ou objetos, firewalls, balanceadores de carga, endereços IP, VLANs (redes locais virtuais) e pacotes de software.[4] Os provedores de nuvem IaaS fornecem esses recursos sob demanda a partir de seus grandes pools de equipamentos instalados nos datacenters. Para conectividade de área ampla , os clientes podem usar a Internet ou as nuvens da operadora (redes privadas virtuais dedicadas). Para implantar seus aplicativos, os utilizadores da nuvem instalam imagens do sistema operacional e seu software de aplicativo na infraestrutura de nuvem. Nesse modelo, o utilizador da nuvem corrige e mantém os sistemas operacionais e o software do aplicativo. Provedores de nuvem geralmente cobram serviços IaaS em uma base de computação utilitária: o custo reflete a quantidade de recursos alocados e consumidos.

TIPOS DE CLOUDS

- PaaS - Plataform as a Service ou Plataforma como Serviço (em português): dá aos desenvolvedores as ferramentas necessárias para criar e hospedar aplicativos Web. A PaaS foi desenvolvida para proporcionar aos utilizadores o acesso aos componentes necessários para desenvolver e operar rapidamente aplicativos Web ou móveis na Internet, sem se preocupar com a configuração ou gerenciamento da infraestrutura subjacente dos servidores, armazenamento, redes e bancos de dados. (p.ex.: IBM Bluemix, Windows Azure e Jelastic). A definição do NIST de computação em nuvem define Plataforma como um serviço como: A capacidade oferecida ao consumidor é implementar na infraestrutura em nuvem os aplicativos criados ou adquiridos ou controlados pelo consumidor criados usando linguagens de programação, bibliotecas, serviços e ferramentas suportados pelo provedor. O consumidor não controla a infraestrutura de nuvem subjacente, incluindo rede, servidores, sistemas operacionais ou armazenamento, mas tem controle sobre os aplicativos implantados e possivelmente configurações para o ambiente de hospedagem de aplicativos.

TIPOS DE CLOUDS

- DaaS - Desktop as a Service ou Área de trabalho como serviço (em português): O desktop como serviço (DaaS) é uma solução de computação em nuvem na qual a infraestrutura de desktop virtual é terceirizada para um provedor terceirizado. A funcionalidade DaaS conta com o desktop virtual, que é uma sessão controlada pelo utilizador ou uma máquina dedicada que transforma serviços de nuvem sob demanda para utilizadores e organizações em todo o mundo. Esse é um modelo eficiente no qual o provedor de serviços controla todas as responsabilidades de back-end que normalmente seriam fornecidas pelo software aplicativo. Desktop como um serviço também é conhecido como desktop virtual ou serviços de desktop hospedados. O DaaS facilita o gerenciamento de vários tipos de recursos de computadores, incluindo desktops, laptops, unidades de mão e thin clients. O DaaS usa execução distribuída ou execução remota, dependendo do tipo de implementação. O DaaS é uma alternativa econômica para soluções de TI convencionais e é usado por organizações e empresas que exigem altos níveis de desempenho e disponibilidade. Além disso, o DaaS serve como uma solução ideal para pequenas organizações com recursos limitados.

TIPOS DE CLOUDS

- SaaS - Software as a Service ou Software como Serviço (em português): O software como um serviço oferece um produto completo, executado e gerenciado pelo provedor de serviços. Na maioria dos casos, as pessoas que se referem ao software como um serviço estão se referindo às aplicações de utilizador final. Com uma oferta de SaaS, não é necessário pensar sobre como o serviço é mantido ou como a infraestrutura subjacente é gerenciada, você só precisa pensar em como usará este tipo específico de software.(p.ex.: Google Docs , Microsoft SharePoint Online).
- CaaS - Comunicativo as a Service ou Comunicação como Serviço (em português): uso de uma solução de Comunicação Unificada hospedada em Data Center do provedor ou fabricante (p.ex.: Microsoft Lync).
- XaaS - Everything as a Service ou Tudo como Serviço (em português): quando se utiliza tudo, infraestrutura, plataformas, software, suporte, enfim, o que envolve T.I.C. (Tecnologia da Informação e Comunicação) como um Serviço. Tudo como um serviço oferece a flexibilidade para que utilizadores e empresas personalizem seus ambientes de computação para criar as experiências que desejam, tudo sob demanda. O XaaS é dependente de uma forte plataforma de serviços em nuvem e conectividade confiável à Internet para ganhar com sucesso tração e aceitação entre indivíduos e empresas.

TIPOS DE CLOUDS

- DBaas - Data Base as a Service ou Banco de dados como Serviço (em português): O nome já deixa claro que essa modalidade é direcionada ao fornecimento de serviços para armazenamento e acesso de volumes de dados. A vantagem aqui é que o detentor da aplicação conta com maior flexibilidade para expandir o banco de dados, compartilhar as informações com outros sistemas, facilitar o acesso remoto por utilizadores autorizados, entre outros;
- SECaaS - Security as a Service - ou Segurança como Serviço (em português): é um modelo de negócio, onde o provedor de serviço integra serviços de segurança em uma infraestrutura corporativa por meio mais eficiente do que indivíduos ou corporações podem prover por si próprias - quando o custo total de posse é considerado.
- FaaS - Function as a Service - ou Função como Serviço (em português): é uma chamada de procedimento remoto hospedada em serviço que aproveita a computação sem servidor para permitir a implementação de funções individuais na nuvem que são executadas em resposta a eventos. O FaaS está incluído no termo mais amplo computação sem servidor, mas os termos também podem ser usados de forma intercambiável.

TIPOS DE CLOUDS

- MBaaS - Mobile "backend" as a Service - ou Backend móvel como Serviço (em português): também conhecido como Backend como um Serviço (BaaS), os desenvolvedores de aplicativos móveis e de aplicativos web são providos com uma maneira de vincular seus aplicativos a serviços de armazenamento em nuvem e computação em nuvem com Interface de programação de aplicações (APIs) expostas às suas aplicações e Kit de desenvolvimento de software personalizado (SDK). Os serviços incluem gerenciamento de utilizadores, notificações por push, integração com serviços de redes sociais, entre outros. Esse é um modelo relativamente recente na computação em nuvem, com a maioria das startups de BaaS datadas de 2011 ou posteriores, mas as tendências indicam que esses serviços estão ganhando tração significativa junto aos consumidores corporativos.

MODELOS DE CLOUD - PRIVADO

- As nuvens privadas são aquelas construídas exclusivamente para um único utilizador (uma empresa, por exemplo). Diferentemente de um data center privado virtual, a infraestrutura utilizada pertence ao utilizador, e, portanto, ele possui total controle sobre como as aplicações são implementadas na nuvem. Uma nuvem privada é, em geral, construída sobre um data center privado.
- Segundo Veras, a nuvem privada é uma infraestrutura em nuvem operada exclusivamente para uma única organização, e quase sempre operada pela própria organização ou por terceiros e hospedada interna ou externamente. Realizar um projeto de nuvem privada requer engajamento significativo para virtualizar o ambiente de negócios e exige que a organização reavalie as decisões sobre os recursos existentes. Pode melhorar os negócios, mas cada etapa do projeto levanta questões de segurança que devem ser abordadas para evitar vulnerabilidades sérias.
- A hospedagem interna é bastante interessante, quando o controle dos dados é algo muito crítico, nesses casos, hospedar através de algum provedor, não é uma solução interessante, devido a perda do controle do armazenamento das informações.

MODELOS DE CLOUD - PÚBLICO

- Uma nuvem é chamada de "nuvem pública" quando os serviços são disponibilizados em uma rede aberta para uso público. Os serviços de nuvem pública podem ser gratuitos. Tecnicamente, pode haver pouca ou nenhuma diferença entre a arquitetura de nuvem pública e privada, entretanto, a consideração de segurança pode ser substancialmente diferente para serviços (aplicativos, armazenamento e outros recursos) disponibilizados por um provedor de serviços para uma base de usuários pública e quando a comunicação é efetuada através de uma rede não confiável. Geralmente, os provedores de serviços de nuvem pública, como o Amazon Web Services (AWS), a Oracle, a Microsoft e o Google, possuem e operam a infraestrutura em seu data center e o acesso é geralmente feito pela Internet. A AWS, Oracle, Microsoft e Google também oferecem serviços de conexão direta chamados "AWS Direct Connect", "Oracle FastConnect", "Azure ExpressRoute" e "Cloud Interconnect" respetivamente. Essas conexões exigem que os clientes comprem ou concedam uma conexão privada a um ponto de peering oferecido pelo provedor de nuvem

MODELOS DE CLOUD - HIBRIDO

- Nas nuvens híbridas temos uma composição dos serviços disponibilizados por nuvens públicas, privadas e de terceiros com orquestração entre essas plataformas. Elas permitem que uma nuvem privada possa ter seus recursos acessados a partir de uma reserva de recursos em uma nuvem pública. Essa característica possui a vantagem de manter os níveis de serviço mesmo que haja flutuações rápidas na necessidade dos recursos. A conexão entre as nuvens pública e privada pode ser usada até mesmo em tarefas periódicas que são mais facilmente implementadas nas nuvens públicas, por exemplo. O termo computação em ondas é, em geral, utilizado quando se refere às nuvens híbridas.

MODELOS DE CLOUD - COMUNITÁRIA

- A nuvem comunitária é de uso exclusivo para específicas comunidades de consumidores de organizações com interesses compartilhados (Requerimentos de segurança, política, considerações de compliance, entre outros). Ela pode ser gerenciada por uma ou mais organizações na comunidade, por terceiros, ou por alguma combinação entre eles, e podem ser hospedadas tanto internamente ou externamente. Seu custo por utilizadores é maior a Nuvem pública (porém, menor do que na Nuvem privada), então apenas alguns recursos de menor custo da computação em nuvem podem ser aplicados.

MODELOS DE CLOUD - HPC

- Nuvem HPC se refere ao uso dos serviços e infraestrutura da computação em nuvem para executar aplicações de alta performance (em inglês, High Performance Computing Cloud ou HPC Cloud. Essas aplicações consomem uma porção considerável de poder de computação e de memória, e são tradicionalmente aglomerados de computadores. Vários vendedores oferecem servidores que suportam a execução dessas aplicações. Em nuvem HPC, o modelo de implantação permite que todos os recursos de HPC estejam dentro da infraestrutura do provedor da nuvem ou em diferentes porções de recursos HPC a serem compartilhados entre o provedor e o cliente no local em que a infraestrutura se encontra. A implementação de nuvem para rodar aplicações de alta performance (HPC applications) começou majoritariamente para aplicações compostas de tarefas independentes, sem Inter-process Communication (IPC). Conforme os provedores de nuvens começaram a oferecer tecnologias de rede de alta velocidade, como a InfiniBand, aplicações com multiprocessamento totalmente acopladas começaram a se beneficiar dos serviços de nuvem também.

MODELOS DE CLOUD - MULTICLOUD

- O Multicloud é o uso de vários serviços de computação em nuvem em uma única arquitetura heterogênea para reduzir a dependência de fornecedores individuais, aumentar a flexibilidade por meio de opções, mitigar desastres etc. Diferencia-se da nuvem híbrida em se referir a vários serviços em nuvem, em vez de várias implantações modos (público, privado, legado).

MODELOS DE CLOUD - BIGDATA

- Os problemas para transferir grandes quantidades de dados para a nuvem, assim como segurança desses dados uma vez que esses dados estão na nuvem inicialmente dificultaram a implementação de nuvem para Big Data, mas agora que muitos dados se originam na nuvem e com o advento dos servidores bare-metal, a nuvem se tornou uma solução para usada para diversos casos, incluindo análise de negócios (business analytics) e análises geoespaciais (geospatial analysis).

MODELOS DE CLOUD - DISTRIBUIDA

- Uma plataforma de computação em nuvem pode ser montada por máquinas distribuídas em diferentes locais, conectadas a uma rede ou a um serviço de hub. Existem dois tipos de nuvem distribuída: computação com recursos públicos (public-resource computing) e nuvem voluntária (volunteer cloud).
- Computação com recursos públicos: Este tipo de nuvem distribuída é resultado de uma extensa definição de computação em nuvem, porque eles são mais semelhantes à nuvem distribuída do que à computação em nuvem. De qualquer forma, esta é considerada uma subclasse da computação em nuvem, e alguns exemplos incluem plataforma distribuídas de computação como: BOINC e Folding@Home.
- Nuvem voluntária: Esta é caracterizada como a interseção entre nuvem distribuída e computação em nuvem, onde a infraestrutura da computação em nuvem é construída utilizando recursos voluntários. Muitos desafios surgem por conta deste tipo de infraestrutura, por causa da volatilidade dos recursos usados para a construção e por conta do ambiente dinâmico em que opera. Esta também pode ser chamada de nuvens de pessoa para pessoa (peer-to-peer cloud), ou nuvens ad-hoc. A Cloud@Home é uma iniciativa interessante nessa direção, ela tem como objetivo implementar uma infraestrutura de computação em nuvem utilizando recursos voluntários provendo um modelo de negócios que incentiva contribuições através de restituição financeira.

ARQUITETURA CLOUD

- https://br.claranet.com/blog/arquitetura-em-nuvem-entenda-o-conceito-do-cloud-computing#:~:text=Migrar%20dados%2C%20sistemas%20e%20aplica%C3%A7%C3%B5es,tend%C3%AAncia%20no%20cen%C3%A1rio%20de%20tecnologia.&text=Afinal%2C%20a%20Arquitetura%20em%20Nuvem,e%20mais%20seguran%C3%A7a%20de%20dados.
- https://blog.ccmtecnologia.com.br/post/arquitetura-em-nuvem-requisitos-para-cloud-computing
- https://aws.amazon.com/pt/training/awsacademy/cloud-computing-architecture/
- https://www.icloud.com.br/1626/arquitetura-de-cloud-computing
- https://br.claranet.com/blog/os-tres-pilares-da-arquitetura-cloud

ARQUITETURA CLOUD

- https://br.claranet.com/blog/arquitetura-em-nuvem-entenda-o-conceito-do-cloud-computing#:~:text=Migrar%20dados%2C%20sistemas%20e%20aplica%C3%A7%C3%B5es,tend%C3%AAncia%20no%20cen%C3%A1rio%20de%20tecnologia.&text=Afinal%2C%20a%20Arquitetura%20em%20Nuvem,e%20mais%20seguran%C3%A7a%20de%20dados.
- https://blog.ccmtecnologia.com.br/post/arquitetura-em-nuvem-requisitos-para-cloud-computing
- https://aws.amazon.com/pt/training/awsacademy/cloud-computing-architecture/
- https://www.icloud.com.br/1626/arquitetura-de-cloud-computing
- https://br.claranet.com/blog/os-tres-pilares-da-arquitetura-cloud

CLOUD PENTEST

RECON AWS and AZURE

- https://github.com/darkbitio/aws-recon
- https://cloudsecops.com/aws-reconnaissance-tools/
- https://github.com/dagrz/aws_pwn
- https://pt.slideshare.net/MichaelRodriguesdosS1/aws-pentesting
- https://notsosecure.com/cloud-services-enumeration-aws-azure-and-gcp/
- https://securityonline.info/azurite-enumeration-reconnaissance-microsoft-azure-cloud/
- https://kvaes.wordpress.com/2016/08/18/azure-enumeration-and-reconnaissance-activities-for-security-officers/
- https://dl.packetstormsecurity.net/papers/general/azure-pentest.pdf
- https://github.com/Azure/Stormspotter
- https://github.com/RhinoSecurityLabs/pacu
- https://attack.mitre.org/techniques/T1526/

SUBDOMAIN TAKEOVER AWS

- https://www.youtube.com/watch?v=srKlqhj_ki8&ab_channel=MohamedHaron
- https://medium.com/entersoftsecurity/weird-subdomain-take-over-pattern-of-amazon-s3-75165ab2e883
- https://medium.com/@gupta.bless/exploiting-subdomain-takeover-on-s3-6115730d01d7
- https://www.we45.com/blog/how-an-unclaimed-aws-s3-bucket-escalates-to-subdomain-takeover
- https://hackerone.com/reports/317005 (EXAMPLE)
- https://www.exploit-db.com/docs/english/46415-the-ultimate-guide-for-subdomain-takeover-with-practical.pdf
- https://github.com/EdOverflow/can-i-take-over-xyz

WEB APP VULNERABILITIES

- https://portswigger.net/web-security/xxe
- https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing
- https://www.netsparker.com/blog/web-security/xxe-xml-external-entity-attacks/
- https://www.acunetix.com/blog/articles/xml-external-entity-xxe-vulnerabilities/
- https://www.youtube.com/watch?v=IMw2C6EJaDo&ab_channel=StrongSecurityBrasil
- https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-perform-ssrf
- https://medium.com/@logicbomb_1/chain-of-hacks-leading-to-database-compromise-b2bc2b883915
- https://medium.com/@logicbomb_1/the-journey-of-web-cache-firewall-bypass-to-ssrf-to-aws-credentials-compromise-b250fb40af82
- https://resources.infosecinstitute.com/local-file-inclusion-code-execution/
- https://rhinosecuritylabs.com/cloud-security/aws-security-vulnerabilities-perspective/

WEB APP VULNERABILITIES

- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-i/
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/
- https://www.cybercureme.com/critical-rce-spoofing-vulnerabilities-in-microsoft-azure-cloud-let-hackers-compromise-microsofts-cloud-server/

WEB APP VULNERABILITIES

- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-i/
- https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/
- https://www.cybercureme.com/critical-rce-spoofing-vulnerabilities-in-microsoft-azure-cloud-let-hackers-compromise-microsofts-cloud-server/
- https://bit.ly/34l12xG (SSTI)
- https://bit.ly/33jFQJ5 (LFI)
- https://bit.ly/3l3jpOw (SSRF)

ACCOUNT HACKING

- https://www.virtuesecurity.com/aws-penetration-testing-part-2-s3-iam-ec2/
- https://github.com/RhinoSecurityLabs/Security-Research
- https://subscription.packtpub.com/book/virtualization_and_cloud/9781789136722/11 (Preview)
- https://rhinosecuritylabs.com/aws/aws-phished-persistent-cookies/
- https://www.pgs-soft.com/blog/hacking-into-an-aws-account-part-1-atlassian-apps/
- https://rhinosecuritylabs.com/aws/aws-iam-credentials-get-compromised/
- https://www.comparitech.com/blog/information-security/credential-stuffing-attacks/
- https://owasp.org/www-community/attacks/Credential_stuffing

LAMBDA EXPLOIT

- https://video.hacking.reviews/2018/02/hacking-serverless-runtimes-profiling.html?m=1
- https://rhinosecuritylabs.com/assessment-services/support-aws-penetration-testing-form/
- https://blog.eccouncil.org/all-you-need-to-know-about-pentesting-in-the-aws-cloud/
- http://blog.blueinfy.com/2018/08/lambda-event-assessment-and-pentesting_20.html
- https://www.securing.biz/why-should-you-consider-penetration-testing-aws-cloud/index.html
- https://github.com/torque59/AWS-Vulnerable-Lambda
- https://essay.utwente.nl/76955/1/Szabo_MSc_EEMCS.pdf
- https://www.cyberis.co.uk/penetration-testing-serverless-architectures.html
- https://blog.cobalt.io/is-your-serverless-app-secure-d863055deaf6
- https://rhinosecuritylabs.com/penetration-testing/penetration-testing-aws-cloud-need-know/

EXPLOITATION

- https://blog.scalesec.com/hacking-aws-with-pacu-learning-from-the-recent-capital-one-incident-c6042067ed04
- https://github.com/mattrotlevi/lava
- https://portswigger.net/daily-swig/cloud-security-attacking-azure-ad-to-expose-sensitive-accounts-and-assets
- https://posts.specterops.io/attacking-azure-azure-ad-and-introducing-powerzure-ca70b330511a
- https://blog.netspi.com/gaining-aws-console-access-via-api-keys/
- https://www.synacktiv.com/en/publications/azure-ad-introduction-for-red-teamers.html
- https://rhinosecuritylabs.com/aws/cloud-container-attack-tool/
- https://www.techrepublic.com/article/how-phishing-attacks-have-exploited-amazon-web-services-accounts/

EXPLOITATION

- https://github.com/puresec/awesome-serverless-security
- https://owasp.org/www-pdf-archive/OWASP-Top-10-Serverless-Interpretation-en.pdf
- https://www.youtube.com/watch?v=GZBiz-0t5KA&ab_channel=BlackHat
- https://snyk.io/blog/10-serverless-security-best-practices/
- https://theburningmonk.com/2017/08/many-faced-threats-to-serverless-security/
- https://www.assurainc.com/attack-against-azure-ad-pass-through-authentication-agent-can-compromise-azure-office-365-tenants/amp-on/
- https://www.blackhat.com/docs/us-17/wednesday/us-17-Krug-Hacking-Severless-Runtimes-wp.pdf

POST EXPLOITATION

- https://medium.com/@rzepsky/playing-with-cloudgoat-part-1-hacking-aws-ec2-service-for-privilege-escalation-4c42cc83f9da
- https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/
- https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation-part-2/
- https://www.youtube.com/watch?v=38FZgSEulow&ab_channel=Mr.Khan
- https://azure.microsoft.com/fr-fr/blog/azure-post-exploitation-techniques/
- https://cloudsecops.com/aws-post-exploitation-part-1/
- https://www.youtube.com/watch?v=2NF4LjjwoZw&ab_channel=BlackHat
- https://www.youtube.com/watch?v=pnwNtlwFYus&ab_channel=AmazonWebServices
- https://www.chrisfarris.com/post/lateral-movement-aws/
- https://www.blackhat.com/docs/us-14/materials/us-14-Riancho-Pivoting-In-Amazon-Clouds-WP.pdf
- https://medium.com/@iraklis/how-to-exfiltrate-aws-ec2-data-b2532862efda

POST EXPLOITATION

- https://github.com/Voulnet/barq
- https://portswigger.net/daily-swig/barq-post-exploitation-framework-plays-havoc-with-aws-infrastructure
- https://medium.com/@rzepsky/playing-with-cloudgoat-part-5-hacking-aws-with-pacu-6abe1cf5780d
- https://www.secsignal.org/en/news/how-i-hacked-a-whole-ec2-network-during-a-penetration-test/
- https://www.youtube.com/watch?v=5NbFcC3yPhM&ab_channel=BSidesLV
- https://medium.com/appsecengineer/dynamodb-injection-1db99c2454ac
- https://www.netspi.com/webinars/lunch-learn-webinar-series/adventures-in-azure-privilege-escalation/
- https://blog.netspi.com/maintaining-azure-persistence-via-automation-accounts/?print=print

Material Extra

- https://bit.ly/3invkFd (GUIDE)
- https://www.linkedin.com/pulse/hijacking-iam-roles-avoiding-detection-nick-frichette/
- https://github.com/opendevsecops/guide-aws-hacking
- https://www.amazon.com.br/Hands-Penetration-Testing-Kali-Linux-ebook/dp/B07C61YYJ4
- https://rhinosecuritylabs.com/cloud-security/common-azure-security-vulnerabilities/
- https://www.devopsgroup.com/blog/hacking-aws-blog/
- https://bit.ly/2ERpr5r (GUIDE 2)
- https://www.netskope.com/blog/a-mitre-based-analysis-of-a-cloud-attack
- https://attack.mitre.org/matrices/enterprise/cloud/azure/
- https://attack.mitre.org/matrices/enterprise/cloud/aws/
- https://www.scs.stanford.edu/~dm/home/papers/dauterman:true2f.pdf
- https://www.youtube.com/watch?v=lOhvlooWzOg
- https://phoenixnap.com/blog/best-penetration-testing-tools
- https://medium.com/@mancusomjm/aws-azure-google-cloud-penetration-testing-resources-ca4b2bf1a4a6

Material Extra

- https://www.youtube.com/watch?v=0PhKK-GHgBI&ab_channel=SecDSM
- https://www.youtube.com/watch?v=yDf-9LGYJi8&ab_channel=PapoBin%C3%A1rio
- https://www.youtube.com/watch?v=P1Bv6dfB0Vo&ab_channel=aloksaurabh
- https://www.youtube.com/watch?v=PyJu_LYosts&ab_channel=RaphaelMudge
- https://www.youtube.com/watch?v=ge6gJkb3nXE&ab_channel=Channel2600
- https://www.youtube.com/watch?v=BT4py9n2WTA&ab_channel=AdrianCrenshaw
- https://www.youtube.com/watch?v=5NbFcC3yPhM&t=1s&ab_channel=BSidesLV
- https://www.youtube.com/watch?v=ffBcIkjumBc&ab_channel=NetSPI
- https://www.youtube.com/watch?v=W5htGHdIc-M&ab_channel=RedTeamVillage
- https://www.youtube.com/watch?v=SA-HeOnOi2A&ab_channel=JorgeOrchilles
- https://www.youtube.com/watch?v=zYc7N9l_2_I&list=PLruly0ngXhPHlQ0ebMbB3XuKVJPq3B0qS&ab_channel=RedTeamVillage
- https://www.blackhat.com/us-18/training/aws-and-azure-exploitation-making-the-cloud-rain-shells.html
- https://github.com/jassics/awesome-aws-security

CONCLUSÃO

- Pentest em cloud é um assunto que está aos poucos sendo discutido, sendo trabalhado e que está tendo demanda aos poucos;
- Com certeza é essencial que você entenda tanto sua arquitetura para ter uma base e estude os vetores de ataques;
- Novas ferramentas, técnicas e metodologias vão surgir para auxiliar na realização dos pentests nesses ambientes, por isso sempre é bom ficar de olho;
- Adquira a base antes e vai subindo os degraus, pois com isso você vai conseguir desenvolver melhor suas habilidades;