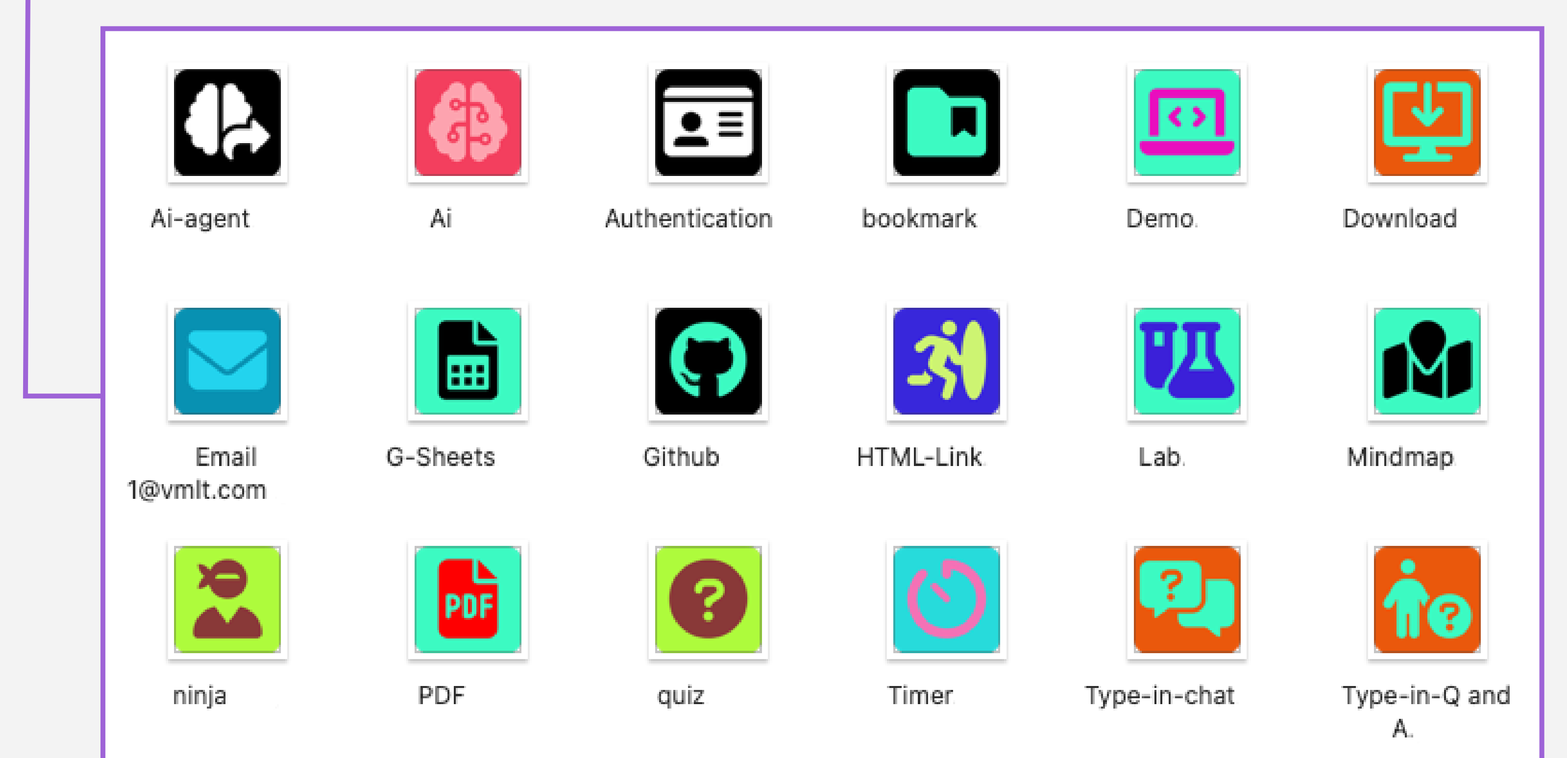
AWS-Security
Dean Bushmiller
2024-12-02

- **Meta**
  - Hands-On AWS Security
  - Design of all Dean Bushmiller courses
    - Talk 1, See 1, Do 1, Teach 1
    - We progress toward independence
    - More in each course than we can cover in the allotted time
  - Minimum security looks like
    - Cloud Security Alliance / Cloud Controls Matrix
    - Dean's top 2 -What could save most of us
      - Identity and Access Management (IAM)
        - MFA & Bastion host as manual configuration tool
        - Firewalls & DNS resolution
    - How often do all organizations fail at basics?
      - Threat and Vulnerability Management (TVM)
      - Patch Management (TVM-02)
      - Incident Management, e-Discovery and Forensics (SEF)
  - Class Icons - in upload Slides also



  - Class start questions
    - Where are you? City / Country
    - **Cloud** skills - business general deployments (years)
    - **AWS** platform deployment skills (years)
    - **Programming** skills - business deployments (years)
    - **Security** skills (years)
    - **Management** experience (years)
    - What is your maximum participation level?
    - Do you intend to do labs live?
    - Expectations, Goals & Metrics
      - Open ended
  - For today: level of activity
    - You can do it all- but it will take a long time
    - Novice - watch and move through each activity
    - Beginner - do all inputs
    - Intermediate - do basic labs
    - Advanced - do all labs in class
  - To play along, get the CSA egregious 11
    - cloudsecurityalliance.org/artifacts/top-threat...
- **Overview**
  - General cloud security advice
  - Narrow scope of discussion
  - AWS vendor-supported enterprise tools
  - Today's use cases = not all things to all people
    - < 5 regions
    - > 5 administrators
    - < 200 instances of compute
    - < $10,000 per month spending in cloud
    - Traditional compute workloads in the cloud
    - Virtual machines migrated to EC2
    - At each summary we point to large enterprise use cases
  - AWS Security services
  - What we will do
    - 2020 top threats from CSA
    - Example of a failure
    - Solutions from AWS
      - Enterprise scalable solutions
      - Built-in deployable tools
    - Sometimes: You decide based upon options
    - Demonstration & Deployment
    - Optional lab - as we go along
    - **My goal:** change how you think about security in the cloud
- **Process**
  - IN CHAT
  - Lab Setup
  - Steps
    - How I do it: Process Threats and solutions
    - What local tools do I use?
    - Prerequisite knowledge
    - In Chat: What authentication tools do you use?
      - FIDO2 / Yubikey
      - Google authenticator app
      - 2FA phone
      - Password vault
      - Other list in chat
    - In Chat: What connection tools do you use?
      - Terminal
      - AWS connect
      - Royal TSX
      - Putty
      - Other list in chat
    - Get doc from CSA
      - cloudsecurityalliance.org/artifacts/top-threat...
- **Content**
  - Lab 1
    - Setup - before class
      - github.com/deanbushmiller/aws-sec-e11/wiki...
    - Demo #1 = 7 minutes
      - 1-Lab-AWS-SEC-E11
  - Lab 2
    - THREAT #1A: Identity & Access Management
      - Pause & Read- Concept: Page 8
      - Threat / Vulnerability: Focus EE4
        - Insufficient Identity and Credential Management
        - Overprovisioned EC2 and S3 roles for WAF and storage.
        - CWE-288: Authentication Bypass Using an Alternate Path or Channel
          - cwe.mitre.org/data/definitions/288.html
        - More data
          - krebsonsecurity.com/tag/capital-one-breach
    - In CHAT
      - When you read "former engineer" as part of the problem, what solutions do you think of?
    - In CHAT
      - Which of these have you used?
      - AWS
MFA EC2 Hosts
Guacamole
None
    - SOLUTION #1A: Cloud Admin MFA, authorization, and activity monitor-ing
      - Multi-Factor Authentication (MFA) for IAM
        - aws.amazon.com/iam/features/mfa
        - Prerequisites: phone / fido
      - Demonstration: IAM Dashboard
    - SOLUTION #1B Access Control via Bastion Host
      - Guacamole
      - Setup LAB 2
        - github.com/deanbushmiller/aws-sec-e11/wiki...
    - Enterprise version
      - If we must manually configure hosts
      - > 20 EC2 instances
      - Automate access to new servers
      - Option GuAWS Netcube link
        - netcubed-ami.s3-website-us-east-1.amazon...
  - Lab 3
    - THREAT #1C: protocol access management
      - How do we stop SSH RDP ICMP?
        - But still allow it from valid hosts
    - SOLUTION #1C: Geo Filtering
      - Problem with the solution?
      - How do we test GEO filtering from other side of internet?
    - Lab 3 Firewall
  - Lab 4
    - THREAT #2 Misconfiguration
      - Pause & Read- Concept: Page 12
      - Threat / Vulnerability: Focus EE2
        - github.com/deanbushmiller/aws-sec-e11/wiki...
        - Misconfiguration and Inadequate Change Control
        - CWE: 16 (not specific enough)
          - cwe.mitre.org/data/definitions/16.html
        - More
          - techcrunch.com/2019/02/27/dow-jones-wat...
    - In CHAT
      - What are the best ways to address misconfiguration?
      - Baseline Configuration management
Change management
CIS Benchmarks
Declarative
Imperative
    - SOLUTION #2A: Change control practices, Baseline configuration, best practices
      - Security tools
        - Amazon Inspector
          - aws.amazon.com/inspector
        - Config
          - aws.amazon.com/config
        - Prerequisites: Understanding Architecture
          - aws.amazon.com/architecture
      - 4 Monitor Lab
        - https://github.com/deanbushmiller/aws-sec-...
        - Deployment: Dean-config , Dean-inspector
      - In CHAT
        - Can you test for these flaws across entire environment?
  - Lab 5
    - THREAT #2 Misconfiguration
    - SOLUTION #2B: Vulnerability Management
      - Pause & Read- Concept: Page 16
      - Threat / Vulnerability:
        - Unsafe Application Programming Interfaces (APIs)
        - Vendor supplied API
        - CVE NIST (in products / not design)
          - nvd.nist.gov/vuln/search/results?form_type=...
    - 5 Vulnerability Management Lab
      - github.com/deanbushmiller/aws-sec-e11/wiki...
      - Systems Manager - Patch
  - Discussion 6
    - THREAT #3: Embedded passwords
      - Pause & Read- Concept: Page 22
      - Threat / Vulnerability:
        - github.com/deanbushmiller/aws-sec-e11/wiki...
        - Insufficient credential management and effective encryption measures facilitated lateral movement across the network.
        - CWE CATEGORY: Key Management Errors
          - cwe.mitre.org/data/definitions/320.html
        - More
          - osradar.com/tesla-cloud-account-data-brea...
    - SOLUTION #3: (You choose) Encryption key management / rotation
      - AWS Systems Manager Parameter Store
        - docs.aws.amazon.com/systems-manager/lat...
      - Key Management Service
        - aws.amazon.com/kms
      - AWS Secrets Manager
        - aws.amazon.com/blogs/security/how-to-cent...
    - In CHAT
      - Read 3 links in solution and choose 1
      - Which is best for Tesla?
      - Systems Manager Parameter Store
Secrets Manager
Key Management Service
  - Discussion 7
    - THREAT #5: DOS
      - Pause & Read- Concept: Page 14
      - Threat / Vulnerability:
        - github.com/deanbushmiller/aws-sec-e11/wiki...
        - Availability DDOS-network or application
        - The actor used a technique known as Memcrashing
        - DDOS amplification: 203-byte request = 50,000 times the amount of data
        - Github Inbound network traffic peaked at 1.35Tbps
        - CWE: CWE-406: Insufficient Control of Network Message Volume (Network Amplification)
          - cwe.mitre.org/data/definitions/406.html
    - In CHAT
      - What/ when is the requirement to protect against DOS?
    - SOLUTION #5: Architecture / Monitoring / Content Delivery Network (CDN)
      - CloudFront
        - aws.amazon.com/cloudfront
      - Shield3000 per month
        - aws.amazon.com/shield
        - Prerequisites: CloudFront distributions
        - Application Load Balancers and / or Amazon API Gateway
    - Demonstration
      - 6 DDOS
      - Must own FQDN