CompTIA Network+ Exam N10-008

Lesson 13

Explaining Common Security Concepts

Objectives

- Explain common security concepts
- Explain authentication methods

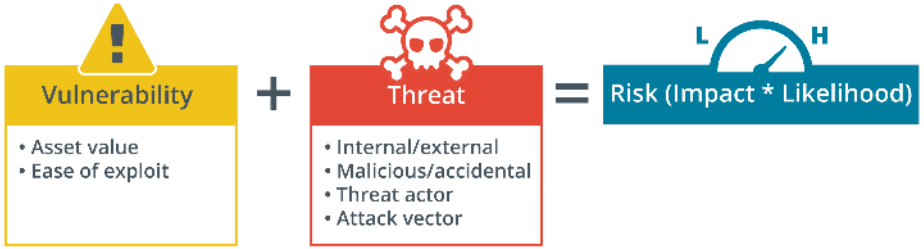
Lesson 13

Topic 13A

Explain Common Security Concepts

Security Concepts

- Confidentiality
  - Certain information should only be known to certain people
- Integrity
  - Data is stored and transferred as intended, and any modification is authorized
- Availability
  - Information is accessible to those authorized to view or modify it
- Vulnerability, threat, and risk

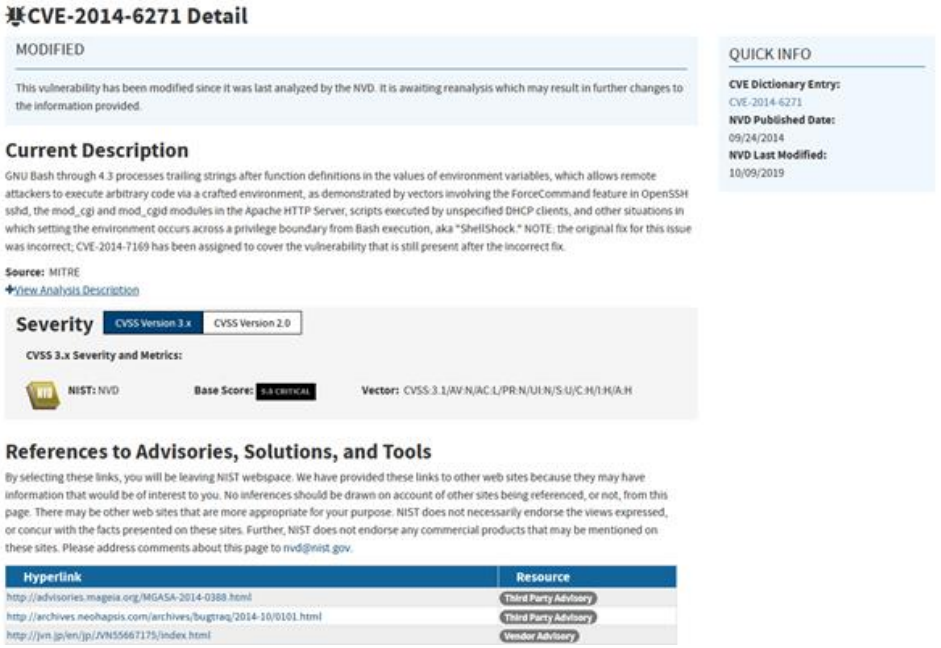


Security Risk Assessments

- Posture assessment
  - Enterprise risk management
  - Comparison with standard frameworks
  - Assess use of security controls
- Process assessment
  - Mission essential function (MEF)
  - Business impact analysis (BIA)
  - Business continuity planning (BCP)

Vulnerability and Exploit Types

- Vulnerabilities
  - Misconfiguration and poor practice or faults in software code
- Exploits
  - Code or method by which a vulnerability is used maliciously
- Zero-day vulnerabilities and exploits
- Unpatched and legacy systems
- Vulnerability assessment
  - Manual and automated scanning
  - Identify deviation from configuration baseline
- Common Vulnerabilities and Exposures (CVE)



CVE-2014-6271 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.

Source: MITRE

View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://advisories.mageia.org/MGASA-2014-0388.html	Third Party Advisory
http://archives.neohapsis.com/archives/bugtraq/2014-10/0101.html	Third Party Advisory
http://jvn.jp/en/jp/JVN55667175/index.html	Vendor Advisory

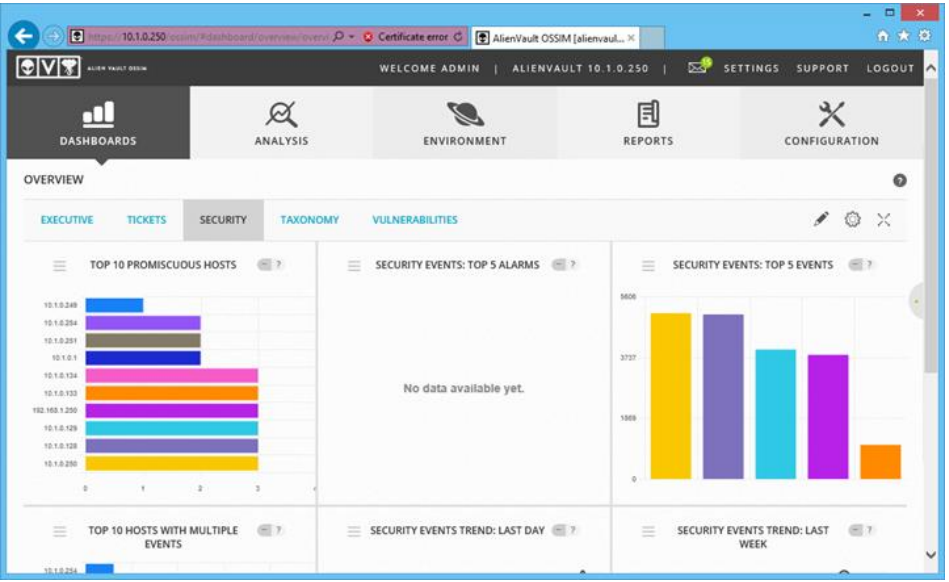
QUICK INFO

CVE Dictionary Entry:
CVE-2014-6271
NVD Published Date:
09/24/2014
NVD Last Modified:
10/09/2019

Threat Types and Assessment

- External versus internal threats
- Threat assessment
  - Identify adversary tactics, techniques, and procedures (TTPs)
  - Research sources
  - Data feeds for automated detection tools

Security Information and Event Management



- Log aggregation
- Event correlation
  - Indicator of Compromise (IoC)
  - Alerting
- Log storage and retention (compliance)

Penetration Testing

- Authorized or ethical hacking
- Goes beyond vulnerability scanning to actively test controls

Privileged Access Management

- Policies, procedures, and technical controls to prevent the malicious abuse of privileged accounts
- Mitigate risks from weak configuration controls over privileges
- Least privilege
- Role-based access
- Zero trust

Vendor Assessment

- Supply chain vulnerability management
- Onboarding suppliers
- Validate supplier security maturity level

Review Activity: Common Security Concepts

- CIA, Vulnerability, Threat, and Risk
- Security Risk Assessments
- Vulnerability and Exploit Types
- Threat Types and Assessment
- Security Information and Event Management
- Penetration Testing
- Privileged Access Management
- Vendor Assessment

Lesson 13

Topic 13B

Explain Authentication Methods

Authentication Methods and Access Controls

- Subjects and objects
- Access control list (ACL)
- Identity and access management (IAM)
  - Identification
  - Authentication
  - Authorization
  - Accounting

Multifactor and Two-Factor Authentication

- Account identity and credentials
- Authentication factors/credential format
  - Knowledge factor - something you know (such as a password)
  - Ownership factor - something you have (such as a smart card)
  - Human factor - something you are (such as a fingerprint)
  - Behavioral factor - something you do (such as making a signature)
  - Location factor - somewhere you are (such as using a mobile device with location services)
- Multifactor requires more than one type

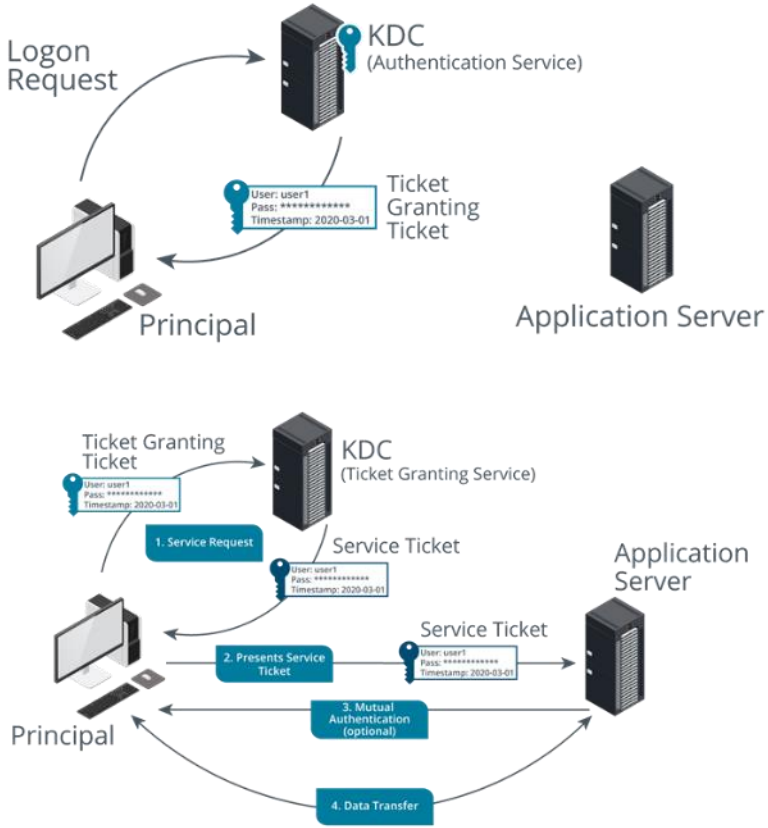
Local Authentication and Single Sign-on

- Cryptographic hashing of passwords
- Windows authentication
  - Local sign-in, Windows network sign-in, Remote sign-in
- Linux authentication
  - /etc/passwd user file and /etc/shadow password file
  - Secure Shell (SSH)
  - Pluggable authentication modules (PAM)
- Single sign-on (SSO)
  - Authenticate once – authorize many

```
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Type........: NetNTLMv2
Hash.Target......: ADMINISTRATOR::515support:2f8cbd19fd1bfac9:881c5503...000000
Time.Started.....: Mon Jan  6 11:25:16 2020 (1 min, 38 secs)
Time.Estimated...: Sat Jan 11 07:49:57 2020 (4 days, 20 hours)
Guess.Mask.......: ?1?1?1?1?1?1?1?1 [8]
Guess.Charset....: -1 pPaAsSwWoOrRdD0123456789$, -2 Undefined, -3 Undefined, -4
Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   364.1 kH/s (11.09ms) @ Accel:128 Loops:32 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 34233472/152587890625 (0.02%)
Rejected.........: 0/34233472 (0.00%)
Restore.Point....: 2176/9765625 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:1824-1856 Iteration:0-32
Candidates.#1....: $87r8678 -> dSDoRS12
```

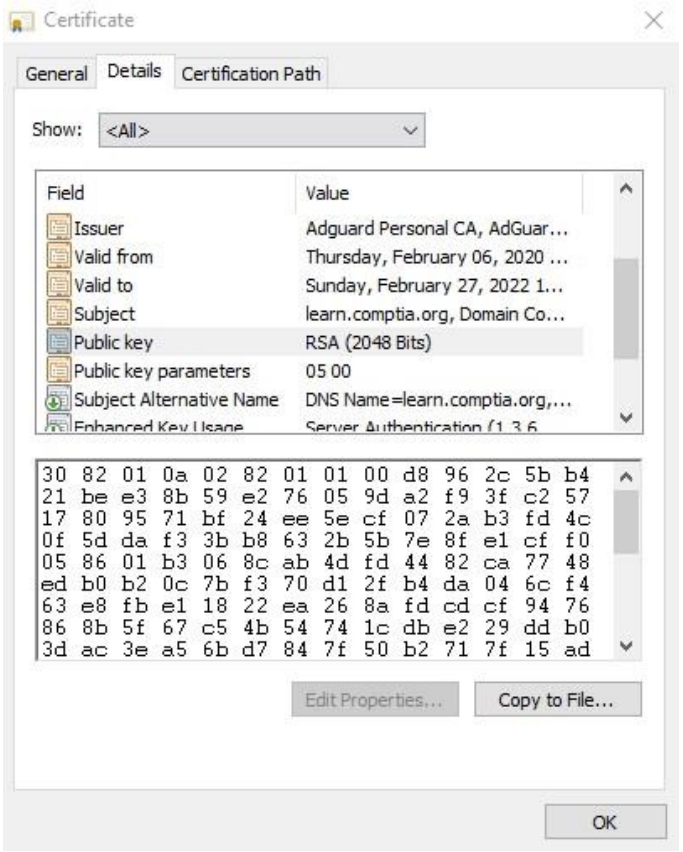
Kerberos



- Single sign-on and mutual authentication
- Three parts
  - Client
  - Server
  - Key Distribution Center (KDC)
- Authentication Service – Ticket Granting Ticket
- Ticket Granting Service – Service Ticket

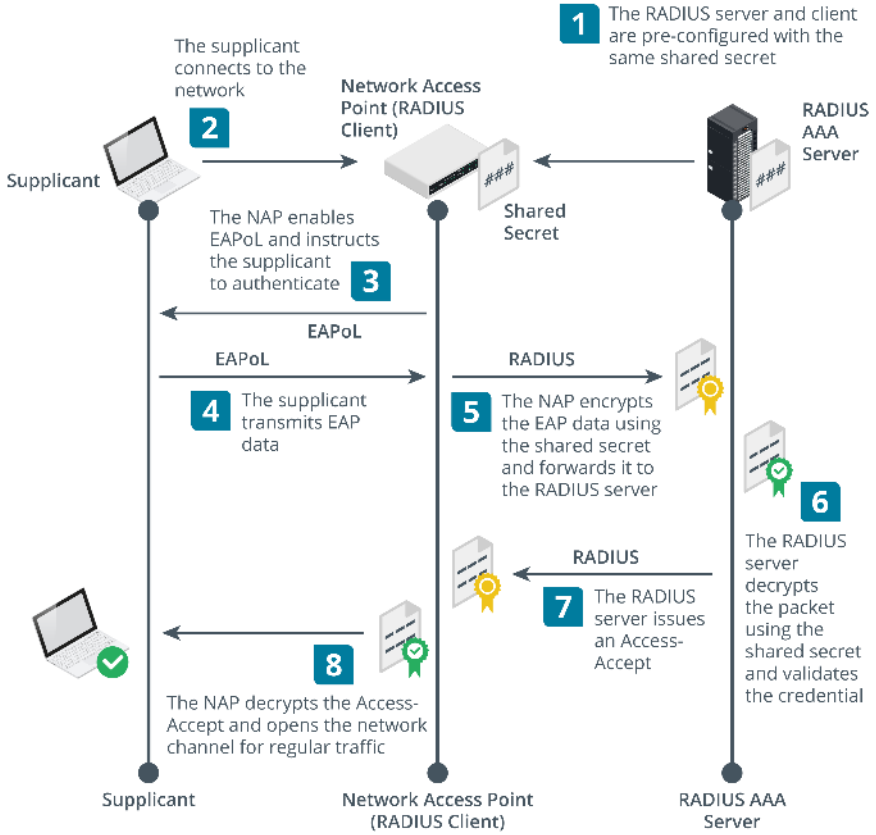
Digital Certificates and PKI

- Public key cryptography (asymmetric encryption)
  - Confidentiality: public key can encrypt but not decrypt
  - Authentication: private key encrypts a signature
- Public Key Infrastructure (PKI) authenticates the public key
  - Public key is wrapped in a digital certificate signed by a certificate authority (CA)
  - If client trusts the CA, they can also trust that a certificate is valid
- Subject is the certificate holder (user or server)

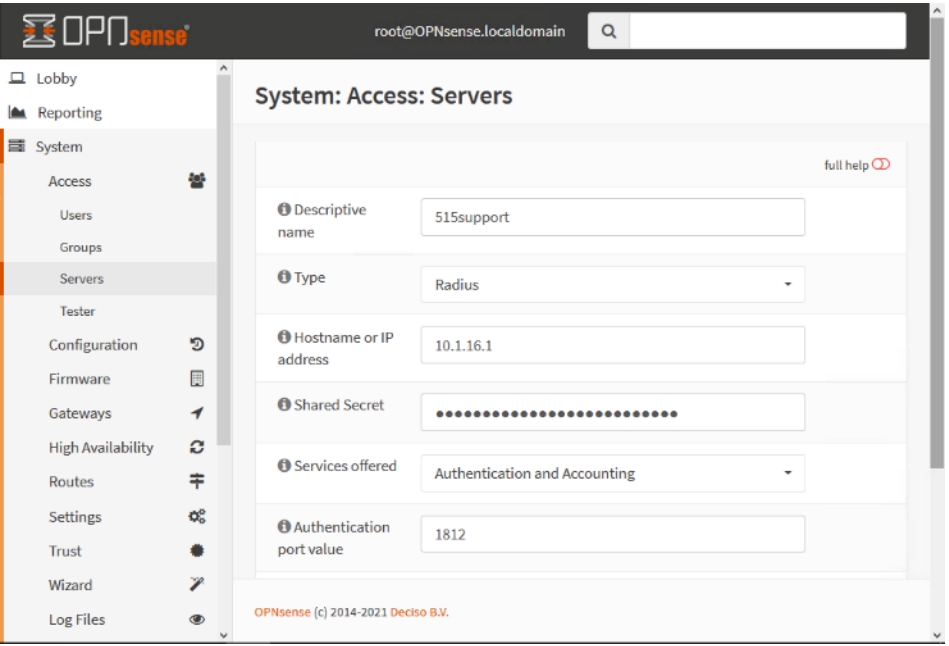


Extensible Authentication Protocol and IEEE 802.1X

- Extensible Authentication Protocol (EAP)
  - Framework for deploying authentication technologies
- IEEE 802.1X Port-based Network Access Control (NAC)
  - Allows use of EAP when connecting to a switch
  - Authentication, authorization, and accounting (AAA) architecture
    - Supplicant
    - Network access server (NAS)/RADIUS client/authenticator
    - AAA server



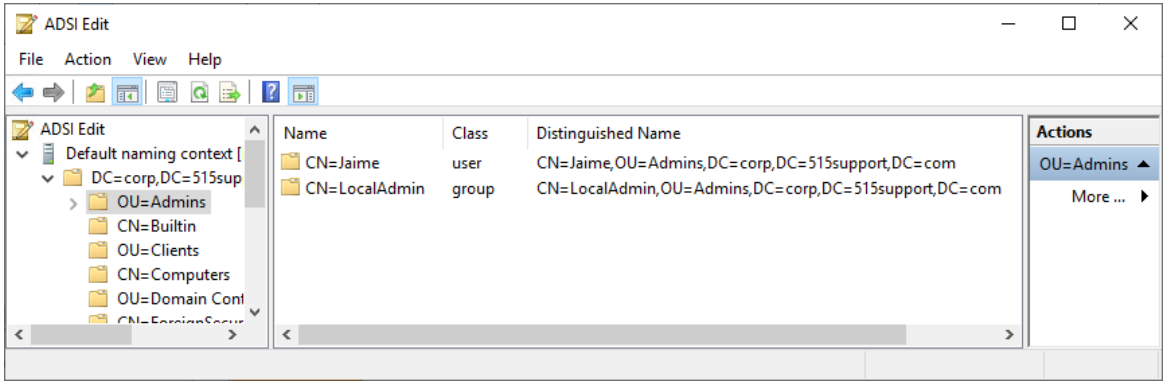
RADIUS and TACACS+



- Remote Authentication Dial-in User Service (RADIUS)
  - Widely used to implement AAA for client device access and remote access VPNs
- Terminal Access Controller Access Control System (TACACS+)
  - Used to authenticate to network switches and routers
  - Uses TCP not UDP
  - Better support for fine-grained authorization policies

Lightweight Directory Access Protocol

- List of network users and resources
- Access control lists (ACLs)
- Authorizations
- Directory database
  - Objects
  - Attributes
- X.500 Distinguished Names
  - Attribute=Value pairs
  - Schema



LDAP Secure

- Binding methods
  - None
  - Simple authentication
  - Simple Authentication and Security Layer (SASL)
  - LDAPS (TLS over TCP port 636)
- Access control policy
  - Read-only
  - Read/write

Review Activity: Authentication Methods

- Authentication Methods and Access Controls
- Multifactor and Two-Factor Authentication
- Local Authentication and Single Sign-on
- Kerberos
- Digital Certificates and PKI
- Extensible Authentication Protocol and IEEE 802.1X
- RADIUS and TACACS+
- Lightweight Directory Access Protocol
- LDAP Secure

CompTIA Network+ Exam N10-008

Lesson 13

Summary