SEC+
Lesson 11:
Enhance Application Security Capabilities

Lesson 11

Topic 11A

Application Protocol Security Baselines

Secure Protocols

- Many of the protocols used today were developed many decades ago
  - Functionality was primary focus
  - Trustworthiness was assumed
  - Cybersecurity was less of an issue than it is today
- Insecure Protocols
  - Transmit data in clear text format
  - Generally, cannot be secured
  - Must be avoided
- Secure Protocols
  - Same functionality and secure
  - More complex to configure

Insecure	Secure Alternative
Telnet	SSH
HTTP	HTTPS
FTP	FTPS/SFTP

Transport Layer Security

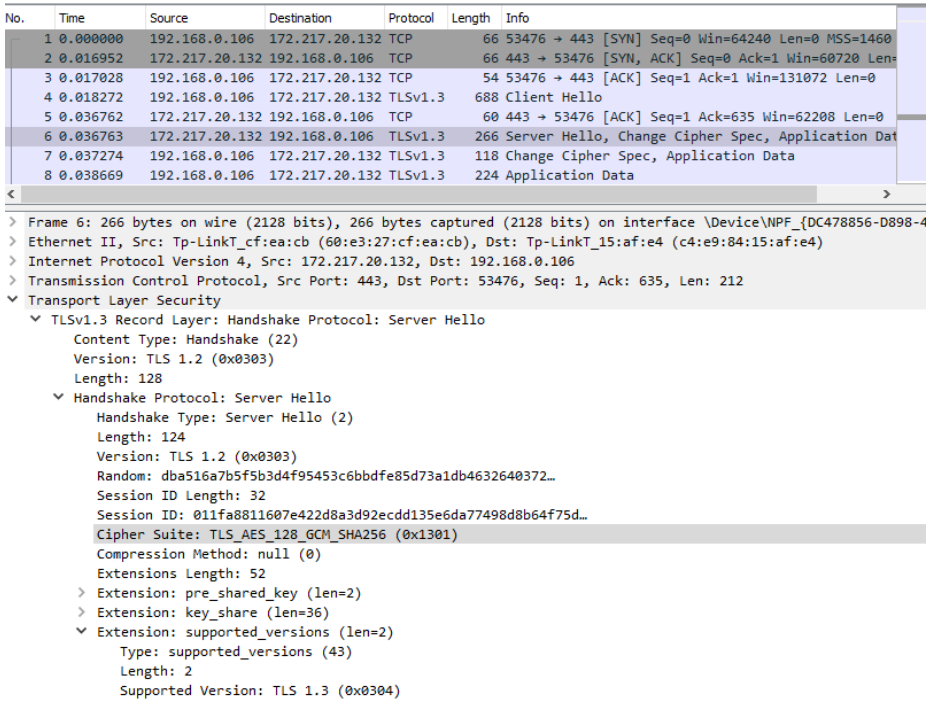
- Most Common Uses
  - Secure HTTP communications
  - Virtual Private Networking (VPN)
- SSL/TLS Versions
  - SSL 2.0, 3.0
  - TLS 1.0, 1.1, 1.2, 1.3
  - Only use TLS version 1.2 or newer
  - Disable all others
    - Downgrade attack

Transport Layer Security

- Cipher Suites
  - Describe the mix of algorithms used to implement TLS protections
- Prior to TLS 1.3

  `ECDHE-RSA-AES128-GCM-SHA256`
- TLS 1.3 uses shortened suites

  `TLS_AES_256_GCM_SHA384`
- Only lists bulk encryption key strength, mode of operation and hash type



Viewing the TLS handshake in a Wireshark packet capture. Note that the connection is using TLS 1.3 and one of the shortened cipher suites (TLS_AES_128_GCM_SHA256).

Secure Directory Services

- A Network directory contains
  - Subjects (users, computers, and services)
  - Objects (directories and files) available in the environment
  - Permissions that subjects have over objects
  - High-value attack target

- Lightweight Directory Access Protocol (LDAP)
  - Default is cleartext communication

Simple Network Management Protocol Security

- Simple Network Management Protocol (SNMP)
- Management and monitoring
- SNMP monitor + agents
- Provides very detailed information about systems
- Uses “Community Strings” default “Public” and “Private”
- Can be used to issue commands
- SNMPv3 has secure features, other versions should be avoided

File Transfer Services

- File Transfer Protocol
  - Cleartext
  - Used to host and share files
- SSH
  - Primarily used to access a shell remotely
  - Very versatile protocol
  - Can be used as a tunnel for other protocols
- FTP (SFTP) and FTP Over SSL (FTPS)
  - SFTP is FTP tunneled through SSH
  - FTPS is FTP secured using TLS

Email Services

Configuring mailbox access protocols on a server.

- SMTP
  - Cleartext by default
  - Transmit email between systems
  - SMTPS is secure configuration
- Open Relay
  - Improperly configured SMTP server
  - Used to send SPAM
- POP & IMAP
  - Used to access mailboxes
  - Cleartext by default
  - POPS & IMAPS are secure

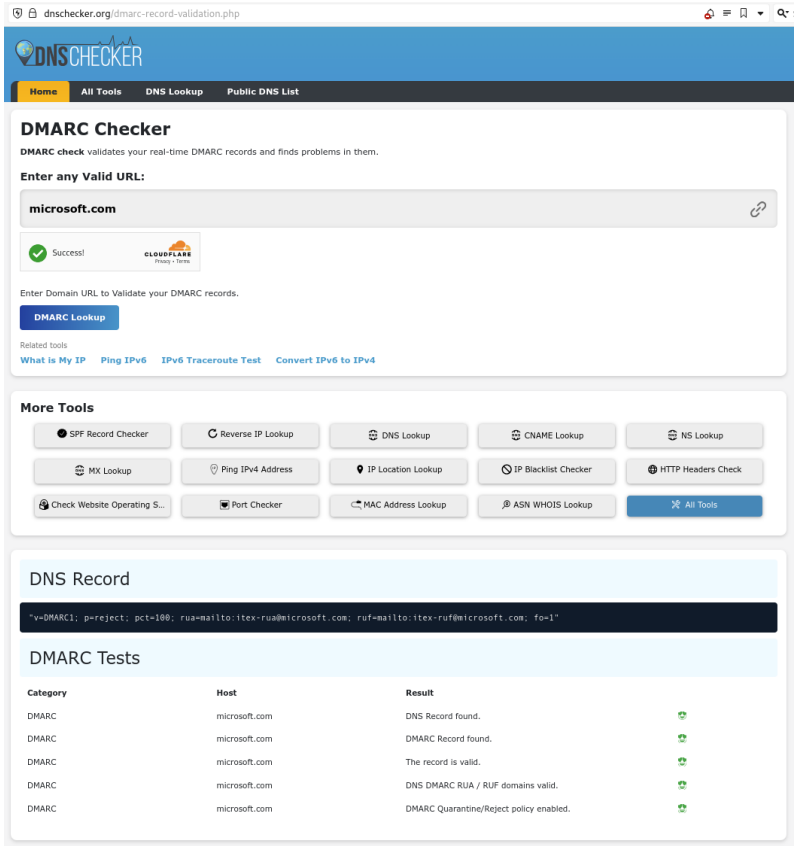
Email Security

- Sender Policy Framework (SPF)
  - Email validation method that helps detect and prevent sender address forgery
  - Uses data saved in DNS TXT Records
  - Can use to identify “authorized senders”
    - Hosted email
    - Marketing campaigns, etc.

```
└$ dig txt microsoft.com
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.18.12-1-Debian <<>> txt microsoft.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55789
;; flags: qr rd ra; QUERY: 1, ANSWER: 16, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;microsoft.com.                 IN      TXT

;; ANSWER SECTION:
microsoft.com.          1590    IN      TXT     "fg2t0gov9424p2tdcuo94goe9j"
microsoft.com.          1590    IN      TXT     "t7sebee51jrj7vm932k531hipa"
microsoft.com.          1590    IN      TXT     "google-site-verification=M--CVfn_YwsV-2FGbCp_HFaEj23BmT0cTF4l8hXgpvM"
microsoft.com.          1590    IN      TXT     "google-site-verification=GfDnTUdATPsK1230J0mXbfsYw-3A9BVMVaKSd4DcKgI"
microsoft.com.          1590    IN      TXT     "d365mktkey=SxDf1EZxLvMwx6eEZUxzjFFgHoapF8DvtWEUjwq7ZTwx"
microsoft.com.          1590    IN      TXT     "hubspot-developer-verification=OTQ5NGIwYWEtODNmZi00YWE1LTkyNmQtNDhjMDMxY2JjNDAx"
microsoft.com.          1590    IN      TXT     "d365mktkey=QDa792dLCZhvaAOOCe2Hz6WTzmTssOp1snABhxWibhMx"
microsoft.com.          1590    IN      TXT     "d365mktkey=6358r1b7e13hox60tl1uagv14"
microsoft.com.          1590    IN      TXT     "google-site-verification=uFg3wr5PWsK8lV029RoXXBBUW0_E6qf1WEWVHhetkOY"
microsoft.com.          1590    IN      TXT     "docusign=d5a3737c-c23c-4bd0-9095-d2ff621f2840"
microsoft.com.          1590    IN      TXT     "d365mktkey=j2qHWq9BHdaa3ZXZH8x64daJZxEWsFa0dxDeilxDoYYx"
microsoft.com.          1590    IN      TXT     "v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.msft.net include:spf-a.hotmail.com include:_spf1-meo.microsoft.com -all"
microsoft.com.          1590    IN      TXT     "8RPDXjBzBS9tu7Pbysu7qCACrwXPoDV8ZtLfthTnC4y9VJFLd84it5sQlEITgSLJ4KOIA8pBZxmyvPujuUvhOg=="
microsoft.com.          1590    IN      TXT     "d365mktkey=3uc1cf82cpv750lzk70v9bvf2"
microsoft.com.          1590    IN      TXT     "facebook-domain-verification=fwzwhbbzwmg5fzgotc2go51olc3566"
microsoft.com.          1590    IN      TXT     "google-site-verification=pjPOauSPcrfXOZS9jnPPa5axowcHGCDAl1_86dCqFpk"
```

Displaying the TXT records for microsoft.com using the dig tool. (Screenshot used with permission from Microsoft.)

Email Security



Performing a DMARC lookup using the DNSChecker website https://dnschecker.org.

- DomainKeys Identified Mail (DKIM)
  - Sender signs emails using a digital signature
  - Receiver uses a DKIM record in the sender's DNS to verify the signature
- Domain-based Message Authentication, Reporting & Conformance (DMARC)
  - Uses the results of SPF and DKIM checks to define rules for handling messages
  - Provides reporting capabilities
    - Email activity
    - Identify systems sending emails
    - Identify unauthorized activity

Email Security

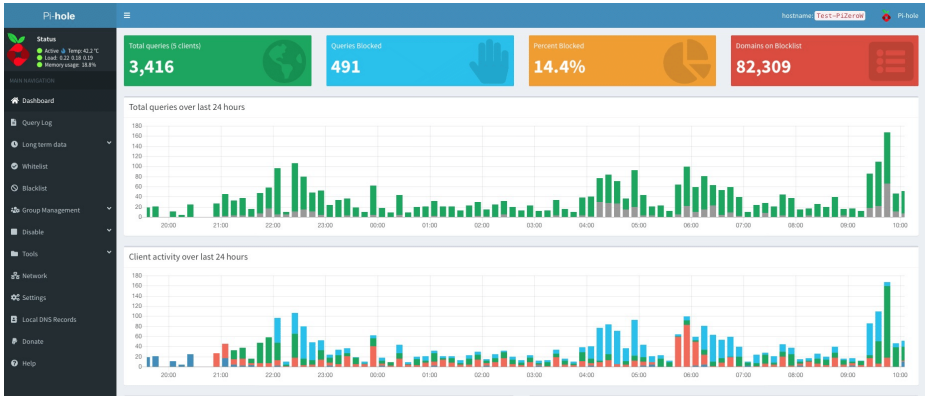
- Email Gateway
  - Control point for all incoming and outgoing email
  - Anti-spam filters and antivirus scanners
  - Sophisticated threat detection algorithms
    - Identify phishing attempts, Business Email Compromise (BEC) Attack
  - Harmful attachments and malicious URLs
    - URL Sanitization/Link Anonymization/Safe Linking/Web Link Transformation
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Encrypts emails to provide the confidentiality and integrity protections
  - Requires Public Key Infrastructure (PKI)

Email Data Loss Prevention

- Email is one of the most frequently used communication channels within organizations
  - Conduit for sensitive data
  - Encourages careless handling of sensitive data (ease of use) and prone to human error
  - Common channel for data loss
  - GDPR, HIPAA, and PCI DSS, (and others) have requirements for protecting data
- DLP scans emails and attachments for certain types of sensitive information
  - Prevents unauthorized sharing of sensitive information
  - Create organization-wide DLP policies
  - Actions are based on predefined rules, such as
    - Blocking the email, alerting the sender, automatically encrypting it

DNS Filtering

- Block or allow access to specific websites
  - DNS filter checks requests against a database of domain names
  - Block access to malicious sites
  - Content/Site Restrictions
  - Ad-blocking (Pi-Hole, AdGuard)
- OpenDNS opendns.com
- Quad9 quad9.net
- CleanBrowsing cleanbrowsing.org
- Cisco Umbrella umbrella.cisco.com/products/dns-layer-network-security
- CloudFlare DNS cloudflare.com/application-services/products/dns/



The Pi-hole administrative dashboard showing DNS resolution statistics. (Screenshot courtesy of Pi-hole.)

DNS Security

- DNS Contains valuable information about hosts on a network
- Internal records should not be accessible from the Internet
- DNS protocol is often exploited to perform data exfiltration
- DNS can be exploited to provide malicious data (ex. Attacker IP instead of real IP)

- DNS Security Extensions (DNSSEC)
  - Mitigate spoofing and poisoning attacks
  - Provides a validation process for DNS responses
  - Authoritative server for the zone creates a "package" of resource records (RRset)

Application Protocol Security Baselines

- Secure Protocols
- Transport Layer Security
- Secure Directory Services
- Simple Network Management Protocol Security
- File Transfer Services
- Email Services
- Email Security
- Email Data Loss Prevention
- DNS Filtering

Lesson 11

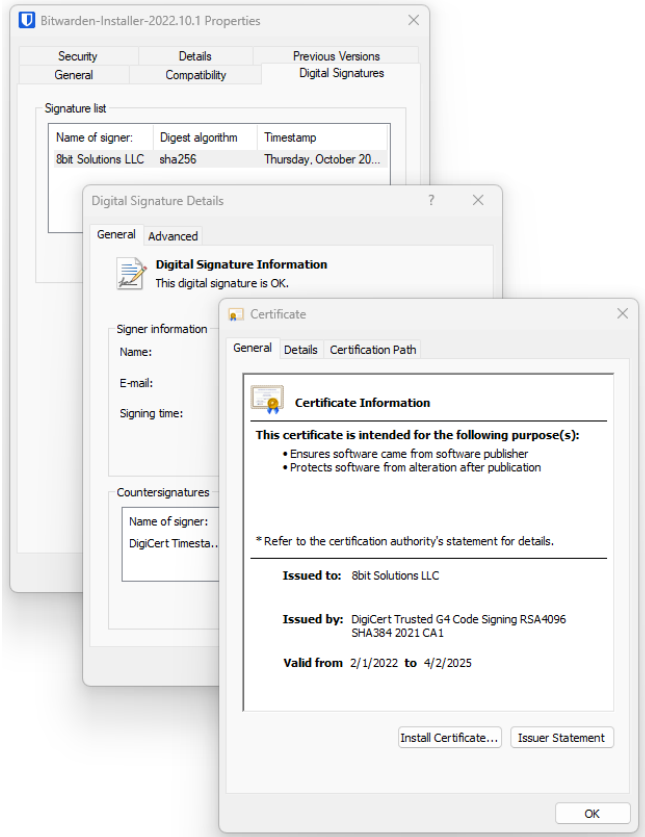
Topic 11B

Cloud and Web Application Security Concepts

Secure Coding Techniques

- Pressure to release an application often overshadows the requirement to ensure it is secure

- Coding practices must implement secure development practices
- Code Signing
- Secure Cookies
- Static/Dynamic Code Analysis
- Peer Review



Reviewing the digital signature associated with the Bitwarden desktop application installer

Secure Coding Techniques

- Input Validation
- Attacker provides specially crafted data to an application to manipulate its behavior
- Injection Attack
- Methods used to perform input validation:
  - Allow/Block Lists
  - Data Type checks
  - Range checks
  - Regular Expressions
  - Encoding

Application Protections

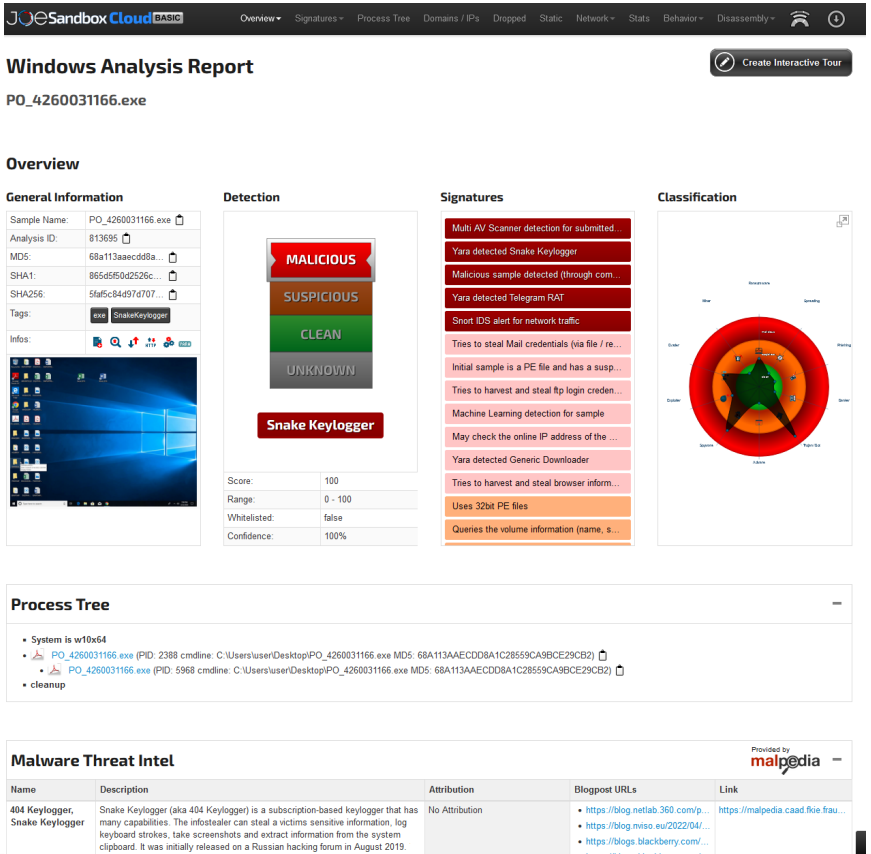
- Data exposure
- Allows privileged information to be read by unauthorized user
  - Access token
  - Password
  - Personal data
- Error Handling
  - Safely handle and control errors
  - Report errors to logs instead of user interface
- Application Security in the Cloud
  - Application security supports the shared responsibility model
  - Secure applications running on a secure cloud platform

Application Protections

- Memory Management
  - Buffer overflow attacks are a decades-old problem
  - Input validation is an important defense

- Client-Side vs. Server-Side Validation
  - Security checks should be performed server-side
  - Developers often use client-side checks to improve application performance
  - Client-side checks can be bypassed

Software Sandboxing



Joe Sandbox analysis of a malicious executable file. (Screenshot courtesy of Joe Security, LLC)

- A security mechanism used to isolate software
- Prevent it from accessing operating system features
- Isolate is from other processes/software
- Prevent access to network
- “Safe Detonation”

- Secure Coding Techniques
- Application Protections
- Software Sandboxing

Lesson 11

Summary