Chapter 8: Infrastructure Threats and Security Monitoring

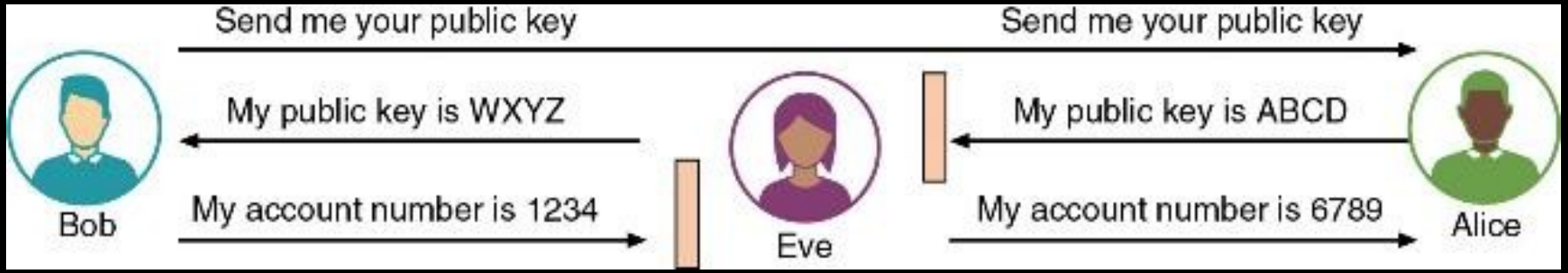
On-Path Attacks

- An **on-path attack** occurs when a threat actor positions themself in the middle between two communicating users or devices
- The following are advantages of an on-path attacks:
  - It can occur without the two targets knowing that an attacker is present
  - It gives the attacker flexibility because they can either eavesdrop to gather valuable information or they can modify the message before sending it on to the recipient

On-Path Attacks

- In a **man-in-the-middle** (**MITM**), a threat actor is positioned into a communication between two parties
  - The goal of an MITM attack is to eavesdrop on the conversation or impersonate one of the parties
- A typical MITM attack has the following two phases:
  - The first phase is intercepting the traffic
  - The second phase is to decrypt the transmissions

MITM Impersonation Attack



On-Path Attacks

- A replay attack makes a copy of a legitimate transmission before sending it to the recipient
  - Attacker uses the copy at a later time
- A **session replay** attack involves intercepting and then using a session ID to impersonate a user
- Threat actors use several techniques for stealing an active session ID:
  - Network attacks (MITM impersonation attacks)
  - Endpoint attacks (cross-site scripting, Trojans, and malicious JavaScript coding)

On-Path Attacks

- A **man-in-the-browser (MITB)** attack intercepts communication between parties to steal or manipulate the data
  - It occurs between a browser and the underlying computer
- A MITB attack usually begins with a Trojan infecting the computer and installing an “extension” into the browser configuration
  - When the browser is launched the extension is activated and waits for a specific webpage in which a user enters information such as account number and password for a financial institution
  - When users click “Submit” the extension captures all the data from the fields on the form

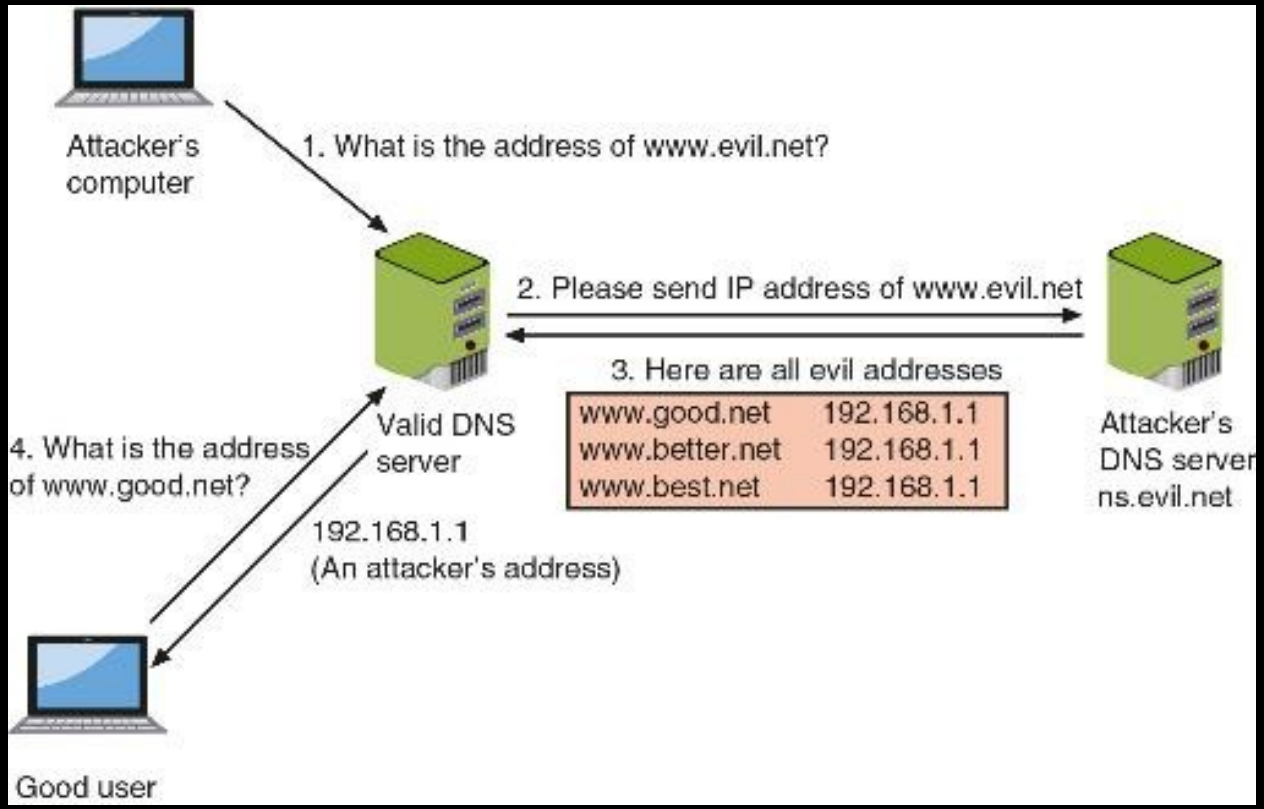
DNS Attacks

- **Domain Name System (DNS)** is a hierarchical name system for matching computer names and IP addresses
  - A DNS-based attack substitutes a DNS address so that the computer is silently redirected to a different device
  - A successful DNS attack has two consequences:
    - URL redirection
    - Domain reputation
  - Attacks using DNS include DNS poisoning and DNS hijacking

DNS Attacks

- **DNS poisoning** modifies a local host file on a device to point to a different domain
  - Threat actors will add a single entry that directs the computer to a DNS server that is under the control of the attackers
- **DNS hijacking** is intended to infect an external DNS server with IP addresses that point to malicious sites
  - DNS hijacking has the advantage of redirecting all users accessing the server
  - Attackers attempt to exploit a protocol flaw and convince the authentic DNS server to accept fraudulent DNS entries sent from the attackers' DNS server

DNS Server Poisoning



DDoS Attacks

- A **denial of service** (**DoS**) attack is a deliberate attempt to prevent authorized users from accessing a system by overwhelming it with requests
- Most DoS attacks today are **distributed denial of service (DDoS)**, which uses hundreds or thousands of devices flooding the server with requests
- The devices participating in a DDoS attack are infected and controlled by threat actors so that users are completely unaware that their endpoints are part of a DDoS attack

DDoS Attacks

- There are two means by which attackers can generate data to overwhelm a system:
  - Use large numbers of compromised devices, each sending bogus requests
  - Use **amplified attacks** (**reflection attacks**) where threat actors attack a misconfigured Internet device or service in such a way that causes the device or service to reflect and generate an even larger payload at the ultimate target

Malicious Coding & Scripting Attacks

- Some network attacks come from malicious software code and scripts
- **PowerShell** is a task automation and configuration management framework from Microsoft
  - Administrative tasks are performed by cmdlets, which are specialized .NET classes that implement a specific operation
  - PowerShell allows attackers to inject code from the PowerShell environment into other processes without first storing any malicious code on the hard disk

Malicious Coding & Scripting Attacks

- **Visual Basic for Applications (VBA)** is an event-driven Microsoft programming language
- VBA allows developers and users to automate processes that normally would take multiple steps or levels of steps
- VBA is most often used to create macros, which are used to automate a complex task or a repeated series of tasks
  - Macros date back to late 1990s but continue to be a key attack vector

Malicious Coding & Scripting Attacks

- **Python** is a programming language that can run on several OS platforms
- Best practices to follow when using Python include the following:
  - Use the latest version of Python
  - Stay current on vulnerabilities within Python
  - Be care when formatting strings in Python
  - Download only vetted Python libraries

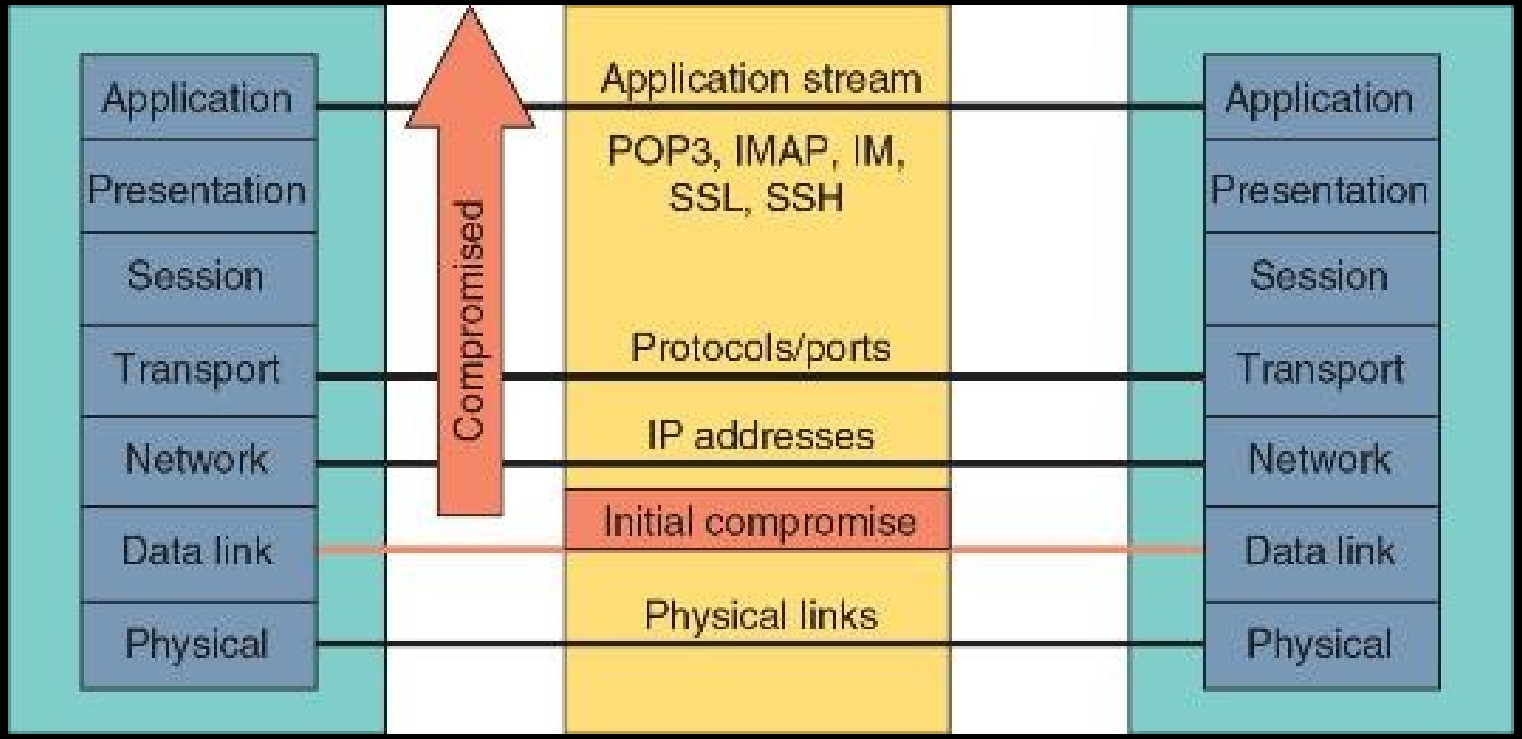
Malicious Coding & Scripting Attacks

- **Bash** is the command language interpreter for the Linux/UNIX OS
- Bash scripting is using Bash to create a script
- Exploits have taken advantage of vulnerabilities in Bash
  - For example, one vulnerability allowed attackers to remotely attach a malicious executable file to a variable that is executed when Bash is invoked

Layer 2 Attacks

- The OSI reference model separates networking steps into a series of seven layers
  - Within each layer, different networking tasks are performed that cooperate with the tasks in the layers immediately above and below it
- Layer 2, the Data Link Layer, is responsible for dividing the data into packets
  - A compromise at Layer 2 can affect the entire communication

Layer 2 Compromise



Layer 2 Attacks

- Address Resolution Protocol Poisoning
  - If the IP address for a device is known but the MAC address is not, the sending computer sends an **Address Resolution Protocol (ARP)** packet to determine the MAC address
  - MAC addresses are stored in an ARP cache for future reference
  - ARP poisoning relies upon MAC spoofing, which is imitating another computer by means of changing the MAC address

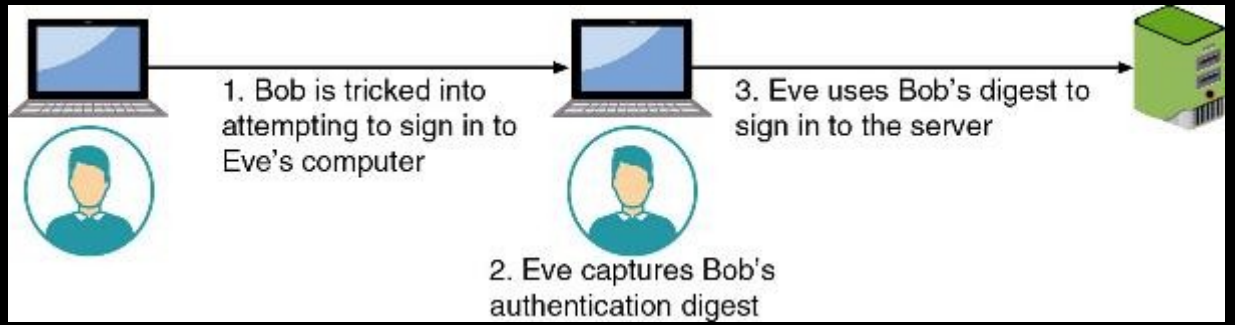
Layer 2 Attacks

- Two common attacks involving spoofing MAC addresses are MAC cloning and MAC flooding
  - In a **MAC cloning attack**, threat actors discover a valid MAC address of a device connected to a switch and spoof the MAC address on their own device and the switch changes its MAC address table to reflect the MAC address with the port to which the attacker's device is connected
  - In a **MAC flooding attack**, a threat actor overflows the switch with Ethernet packets that have been spoofed so that every packet contains a different source MAC address

Credential Relay Attack

- A **credential relay attack** attempts to steal authentication credentials and then use them to access a system

- Attackers intercept digests of user passwords as they are being transmitted and then relay the clients' credentials to impersonate the user



Question?

- Kelly has discovered that the network switch is broadcasting all packets to all devices. She suspects it is the result of an attack that has overflowed the switch MAC address table. Which type of attack would she report?

Answer

- Kelly has discovered that the network switch is broadcasting all packets to all devices. She suspects it is the result of an attack that has overflowed the switch MAC address table. Which type of attack would she report?
- MAC flooding attack; In a MAC flooding attack, a threat actor will overflow the switch with Ethernet packets that have been spoofed so that the switch enters a failure mode, which is a predefined set of actions based on a failure of a network component.

Monitoring Methodologies

- Monitoring involves examining network traffic, activity, transactions, or behavior to detect security-related anomalies
- **Anomaly monitoring** is designed for detecting statistical anomalies
  - A secure baseline of normal activities is compiled so if there is a deviation from the baseline, an alarm is raised
- **Signature-based monitoring** examines network traffic, activity, transactions, or behavior to look for well-known patterns to compare these activities against a predefined signature

Monitoring Methodologies

- **Behavior-based monitoring** uses the “normal” processes and actions as the standard
  - It continuously analyzes the behavior of processes and programs on a system and alerts the user if it detects any abnormal actions
- **Heuristic monitoring** is founded on experience-based techniques and attempts to answer the question, “Will this do something harmful if it is allowed to execute?”

Monitoring Activities

Activity	Description
Scanning	A frequent and ongoing process, often automated, that continuously searches for evidence of an attack
Reporting	Generating documentation on the results of monitoring activities
Quarantine	Isolating systems that have been compromised
Alerting	Detecting and notifying operators about meaningful events that may denote an attack
Alert tuning	“Tweaking” the altering function to weed out false positives
Archiving	Retaining historical documents and records of monitoring

Tools for Monitoring and Alerting

- Collecting and analyzing data packets that cross a network can provide valuable information
- Packet analysis typically examines the entire contents of the packet, which can be used extensively for security
- **Wireshark** is a popular GUI packet capture and analysis tool
- **Tcpdump** is a command-line packet analyzer
- **Tcpreplay** is a tool for editing packets and then “replaying” the packets back onto the network to observe their behavior

Tools for Monitoring and Alerting

- **Flow analysis** (network traffic analysis) is the process of monitoring the network's devices and sounding an alert if it exceeds a baseline
- Flow analysis for information security is different from traditional network traffic flow for several reasons:
  - Eliminates monitoring agents
  - Uses deep packet inspection
  - Provides richer information
- **NetFlow** is a session sampling protocol that collects IP network traffic

Network Traffic Analysis Output

Tools for Monitoring and Alerting

- **Data loss prevention** (**DLP**) is a system of security tools used to recognize and identify data that is critical to the organization and ensure it is protected
- Most DLP systems use content inspection, which is a security analysis of the transaction within its approved context
- Administrators create DLP rules, which are uploaded to a DLP server
- If a policy violation is detected by a DLP agent, it is reported back to the DLP server

Tools for Monitoring and Alerting

- The **Simple Network Management Protocol** (**SNMP**) is a protocol used to remotely monitor, manage, and configure devices on the network
  - An **SNMP trap** is a type of PDU that sends an unsolicited message to the manager about critical events in the managed device
- **Log aggregation** enables security personnel to gather events from disparate sources into a single entity so that it can be searched and analyzed
- **Security Content Automation Protocols** (**SCAP**) can help automate vulnerability management and determine whether the enterprise is compliant with required policies

Tools for Monitoring and Alerting

- A **Security Information and Event Management** (**SEIM**) product consolidates real-time security monitoring and management of security information with analysis and reporting of security events
- A SEIM typically has the following features:
  - Aggregation
  - Correlation
  - Automated alerting and triggers
  - Time synchronization
  - Event duplication and logs

SIEM Dashboard

Tools for Monitoring and Alerting

- A **security orchestration, automation, and response** (**SOAR**) product is similar to a SIEM in that it is designed to help security teams manage and respond to a high number of security warnings and alarms
- SOARs take it a step further by combining more comprehensive data gathering and analytics in order to automate incident response

Question?

- Which type of monitoring methodology looks for statistical deviations from a baseline?

Answer

- Which type of monitoring methodology looks for statistical deviations from a baseline?
- Anomaly monitoring is designed for detecting statistical anomalies. First, a secure baseline of normal activities is compiled over time (a baseline is a reference set of data against which operational data is compared). Whenever there is a significant deviation from this baseline, an alarm is raised.

Email Monitoring and Security

- The basic components involved in sending and receiving email are the Mail User Agent (MUA) and Mail Transfer Agent (MTA)
  - A MUA is what is used to read and send email from an endpoint
  - MTAs are programs that accept email messages from senders and route them toward their recipients
- As email is transferred from MTA to MTA, information is added to the email header
  - Email headers also contain an analysis of the email by the MTA

Email Threats

- Threats related to email include the following:
  - Malicious payload
  - Embedded links
  - Impersonation
  - Forwarding

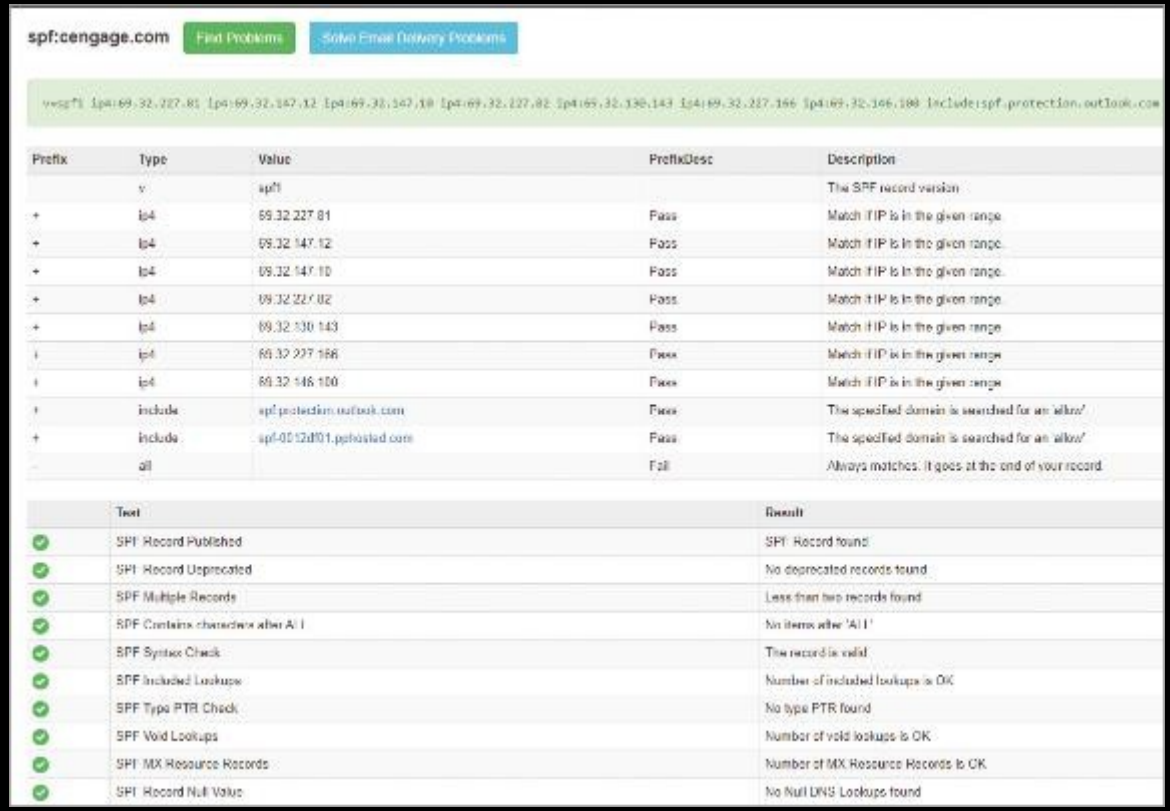
Email Defenses

- Spam and phishing filters can help address phishing attacks and anti-malware can be used to minimize malicious payloads
- Other defenses include the following:
  - Sender Policy Framework (SPF)
  - Domain Keys Identified Mail (DKIM)
  - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
  - Secure email gateway (SEG)

Email Defenses

- **Sender Policy Framework** (**SPF**) is an email authentication method that identifies the MTA email servers that have been authorized to send email for a domain
  - SPF helps protect a domain from spoofing and also helps prevent messages from a valid domain from being marked as unwanted spam
- **Domain Keys Identified Mail** (**DKIM**) is an authentication technique that validates the content of the email message
  - The validation is accomplished through a digital signature

Cengage SPF Record



spf:cengage.com

Find Problems | Solve Email Delivery Problems

v=spf1 ip4:69.32.227.81 ip4:69.32.147.12 ip4:69.32.147.10 ip4:69.32.227.82 ip4:69.32.130.143 ip4:69.32.227.166 ip4:69.32.146.100 include:spf.protection.outlook.com

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	ip4	69.32.227.81	Pass	Match if IP is in the given range
+	ip4	69.32.147.12	Pass	Match if IP is in the given range
+	ip4	69.32.147.10	Pass	Match if IP is in the given range
+	ip4	69.32.227.82	Pass	Match if IP is in the given range
+	ip4	69.32.130.143	Pass	Match if IP is in the given range
+	ip4	69.32.227.166	Pass	Match if IP is in the given range
+	ip4	69.32.146.100	Pass	Match if IP is in the given range
+	include	spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'
+	include	spf-0012d101.pphosted.com	Pass	The specified domain is searched for an 'allow'
	all		Fail	Always matches. It goes at the end of your record

	Test	Result
✓	SPF Record Published	SPF Record found
✓	SPF Record Deprecated	No deprecated records found
✓	SPF Multiple Records	Less than two records found
✓	SPF Contains characters after ALL	No items after 'ALL'
✓	SPF Syntax Check	The record is valid
✓	SPF Included Lookups	Number of included lookups is OK
✓	SPF Type PTR Check	No type PTR found
✓	SPF Void Lookups	Number of void lookups is OK
✓	SPF MX Resource Records	Number of MX Resource Records is OK
✓	SPF Record Null Value	No Null DNS Lookups found

Email Defenses

- **Domain-based Message Authentication, Reporting, and Conformance** (**DMARC**) allows the administrative owner of a domain to publish a policy in their DNS records to specify which mechanism (DKIM, SPF, or both) is used when sending email from that domain
- **Secure Email Gateway** (**SEG**) acts as a “proxy” for the organization’s email server
  - SEG can filter and inspect emails for malicious content
- Limitations of SEG include single-layer security, exposing protections, multiple root domains