# Securing Networks

AP Cybersecurity · Vocabulary in context

| Word | Example |
| --- | --- |
| **ARP poisoning** /ɑːp ˈpɔɪzənɪŋ/ | **ARP poisoning** sends local traffic to the attacker's computer. |
| **address resolution protocol (ARP)** /əˈdres ˌrezəˈluːʃn ˈprəʊtəkɒl/ | The **address resolution protocol (ARP)** finds the MAC address for an IP address.<br>IP MAC |
| **MAC addresses** /mæk əˈdresɪz/ | **MAC addresses** identify each network card. |
| **on-path attack** /ɒn pæθ əˈtæk/ | In an **on-path attack**, the attacker sits between two computers. |
| **MAC flooding** /mæk ˈflʌdɪŋ/ | **MAC flooding** fills a switch's table with fake addresses. |
| **switch** /swɪtʃ/ | A **switch** sends data only to the computer it is for. |
| **eavesdropping** /ˈiːvzdrɒpɪŋ/ | **Eavesdropping** means secretly listening to messages. |
| **DNS poisoning** /ˌdiː en ˈes ˈpɔɪzənɪŋ/ | **DNS poisoning** sends you to a fake website. |
| **domain name system (DNS)** /dəˈmeɪn neɪm ˈsɪstəm/ | The **domain name system (DNS)** turns names into IP addresses.<br>IP |
| **credential harvesting** /krɪˈdenʃl ˈhɑːvɪstɪŋ/ | **Credential harvesting** uses fake login pages to steal passwords. |
| **denial of service (DoS)** /dɪˈnaɪəl ɒv ˈsɜːvɪs/ | A **denial of service (DoS)** attack floods a website so no one can use it. |

| Word | Example |
| --- | --- |
| **distributed denial of service (DDoS)** /ˈdɪstrɪbjuːtɪd dɪˈnaɪəl ɒv ˈsɜːvɪs/ | A **distributed denial of service (DDoS)** attack uses thousands of computers. |
| **rogue access point** /rəʊg ˈækses pɔɪnt/ | A **rogue access point** lets attackers get around the firewall. |
| **automated vulnerability scanner** /ˈɔːtəmeɪtɪd ˌvʌlnərəˈbɪlɪti ˈskænə/ | An **automated vulnerability scanner** looks for known weaknesses. |
| **mitigation** /ˌmɪtɪˈgeɪʃn/ | A firewall is a **mitigation** for network attacks. |
| **split tunneling** /splɪt ˈtʌnəlɪŋ/ | With **split tunneling**, only some traffic goes through the VPN.<br>VPN |
| **WPA3** /ˌdʌbljuː piː eɪ ˈθriː/ | **WPA3** is the newest Wi-Fi security standard.<br>Wi-Fi |
| **Network segmentation** /ˈnetwɜːk ˌsegmənˈteɪʃn/ | **Network segmentation** splits a network into separate zones. |
| **subnets** /ˈsʌbnets/ | A big network is split into smaller **subnets**. |
| **screened subnet** /skriːnd ˈsʌbnet/ | A **screened subnet** keeps public servers apart from the inside network. |
| **DMZ** /ˌdiː em ˈzed/ | The web server sits in the **DMZ**.<br>Web |
| **VLANs** /ˈviːlænz/ | **VLANs** separate traffic on the same switch. |
| **firewall** /ˈfaɪəwɔːl/ | A **firewall** blocks unsafe data. |
| **Stateless** /ˈsteɪtləs/ | A **stateless** firewall checks each packet on its own. |



exercises.lol exercises.com.cn

| Word | Example |
| --- | --- |
| **Stateful** /ˈsteɪtfl/ | A **stateful** firewall remembers which connections are open. |
| **access control list (ACL)** /ˈækses kənˈtrəʊl lɪst/ | An **access control list (ACL)** lists which traffic is allowed. |
| **log files** /lɒg faɪlz/ | **Log files** record what happened on the system. |
| **network intrusion detection system (NIDS)** /ˈnetwɜːk ɪnˈtruːʒn dɪˈtekʃn ˈsɪstəm/ | A **network intrusion detection system (NIDS)** warns of attacks. |
| **network intrusion prevention system (NIPS)** /ˈnetwɜːk ɪnˈtruːʒn prɪˈvenʃn ˈsɪstəm/ | A **network intrusion prevention system (NIPS)** can block attacks. |
| **security information and event management (SIEM)** /sɪˈkjʊərɪti ˌɪnfəˈmeɪʃn ænd ɪˈvent ˈmænɪdʒmənt/ | A **security information and event management (SIEM)** tool collects all the logs in one place. |
| **Signature-based** /ˈsɪgnɪtʃə beɪst/ | **Signature-based** detection looks for known attack patterns. |
| **Anomaly-based** /əˈnɒməli beɪst/ | **Anomaly-based** detection looks for unusual activity. |
| **baseline** /ˈbeɪslaɪn/ | Compare network traffic with its normal **baseline**. |
| **network-based indicators of compromise** /ˈnetwɜːk beɪst ˈɪndɪkeɪtəz ɒv ˈkɒmprəmaɪz/ | Strange connections at night are **network-based indicators of compromise**. |
| **probabilistic** /ˌprɒbəbɪˈlɪstɪk/ | Anomaly detection is **probabilistic**: it can be wrong. |
| **threshold** /ˈθreʃəʊld/ | The alarm goes off above a **threshold** temperature. |

| Word | Example |
| --- | --- |
| **alert fatigue** /əˈlɜːt fəˈtiːg/ | **Alert fatigue** happens when there are too many warnings. |



exercises.lol exercises.com.cn