SIGPwny

FA2024 Week 08 • 2024-10-24

Secure DNS, E-Mail, FTP, & SMB

Michael Khalaf, Sagnik Chakraborty

DNS: Threat Mitigation

1. DNS Spoofing (MiTM Attacks)
2. DNS Amplification (DoS & DoS)
3. DNS Cache Poisoning

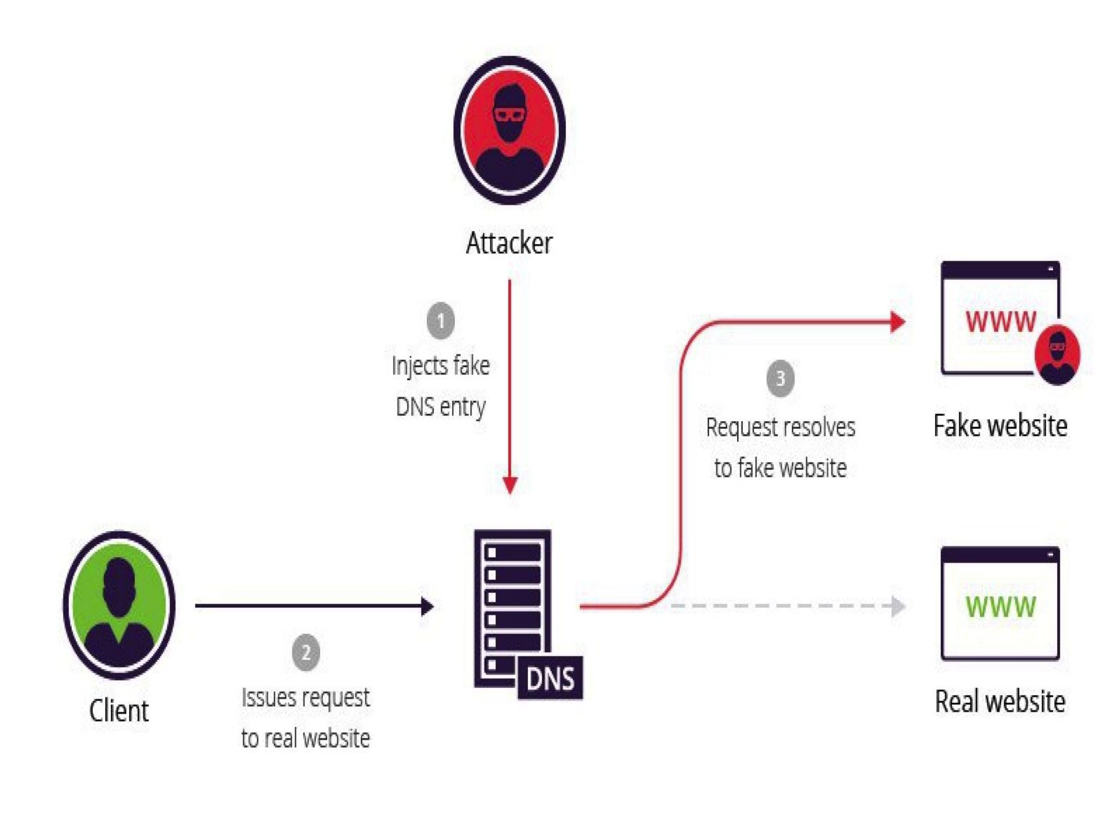
DNS: Threat Mitigation

1. DNS Spoofing (MiTM Attacks)

2. DNS Amplification (DoS & DoS)

3. DNS Cache Poisoning

DNS Spoofing: MiTM



Tools popularly used: ettercap, dnsspoof

DNS Spoofing & MiTM Mitigation

Implementation:

DNSSEC: Digital signatures (keys)

Wireshark: Analyze DNS traffic for unusual patterns and suspected attacks.

Splunk: Monitors DNS logs for indicators of DNS attacks (e.g., high traffic volume, spoofed responses).

Tools:

```
sudo apt install bind9 bind9utils bind9-doc
```

Unbound, dnssec-tools

Kali → Wireshark

https://www.splunk.com/en_us/download/splunk-cloud.html

DNS Spoofing & MiTM Mitigation

Implementation:

Red teaming tools help find our weaknesses. We can use them to our advantage in addition to planning for their use against us.

Tools:

dnsspoof

ettercap

Metasploit DNS Modules

DNS Tool Implementation

Red Team Tools:

- **dnsspoof:** Intercepts and alters DNS responses.
- **Ettercap:** Used for DNS spoofing within a larger MITM attack.
- **Bettercap:** A modern tool that can perform DNS spoofing during MITM attacks.
- **Responder:** Can poison LLMNR, NBT-NS, and DNS traffic to redirect users to malicious sites.

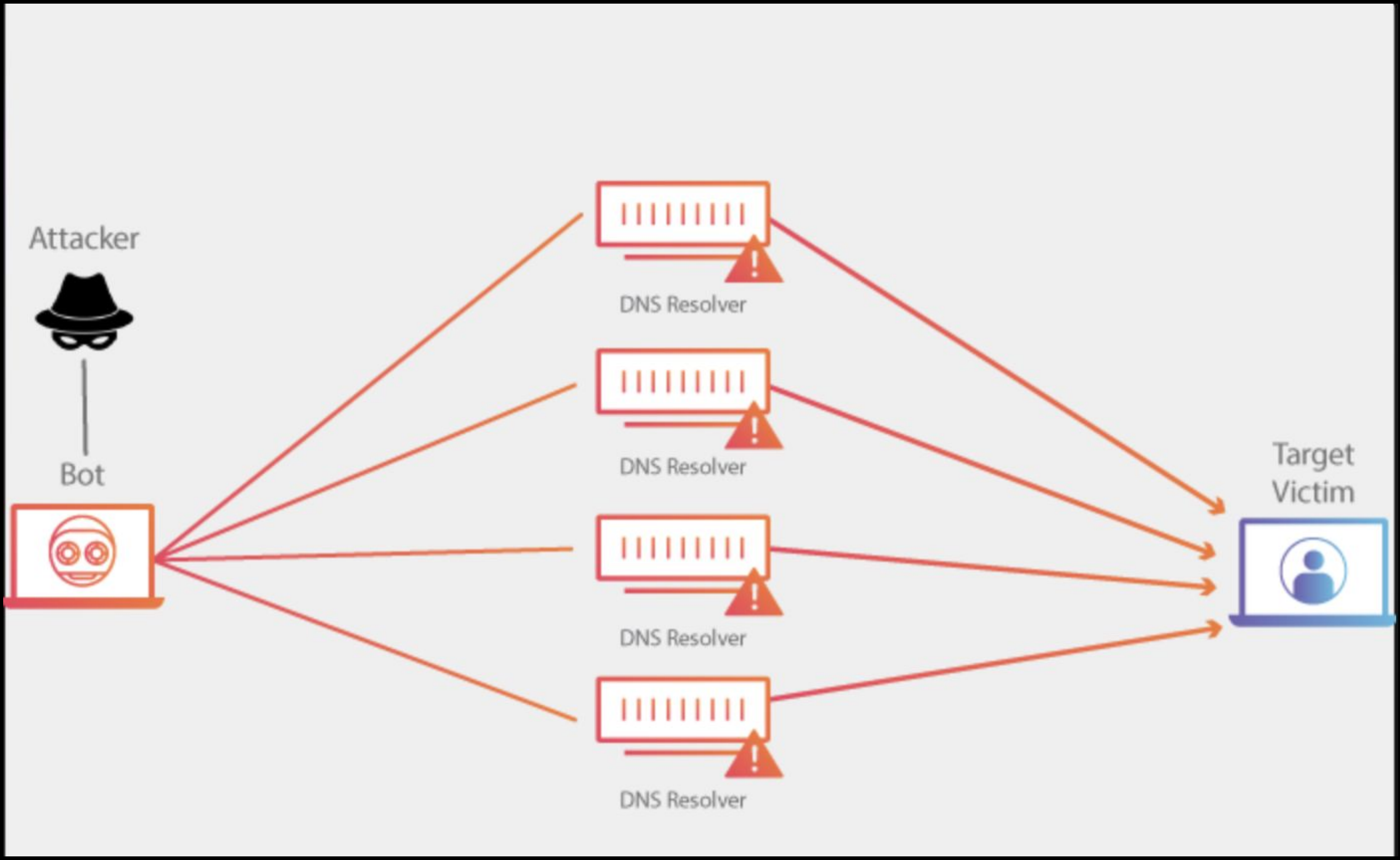
Blue Team Tools:

- **DNSSEC**: Ensures DNS records are cryptographically signed and verified, preventing spoofing.
- **DoH (DNS over HTTPS)** or **DoT (DNS over TLS):** Encrypts DNS traffic to protect it from tampering.
- **Splunk/Elastic Stack:** Monitors DNS queries and responses for irregularities.
- **Wireshark:** Analyzes network traffic and can detect spoofed DNS responses.

DNS: Threat Mitigation

1. DNS Spoofing (MiTM Attacks)
2. DNS Amplification (DoS & DoS)
3. DNS Cache Poisoning

DNS Amplification (DDoS)



DNS Amplification Mitigation

1. Set rate limits on DNS responses to prevent abuse from amplification attacks.

2. Use response rate limiting (RRL) on DNS servers to block large floods.

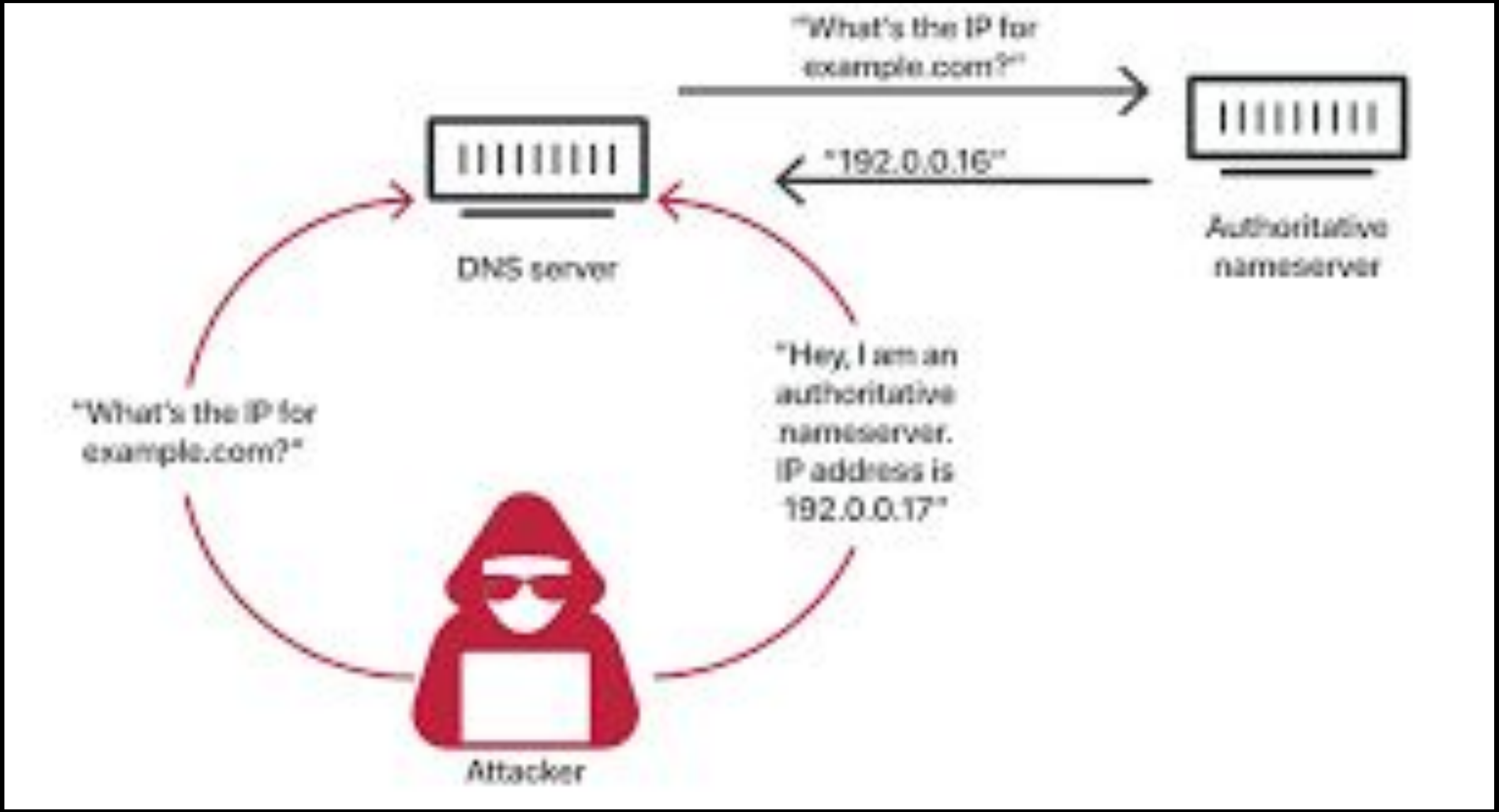
DNS Threat Mitigation

1. DNS Spoofing (MiTM Attacks)

2. DNS Amplification (DoS & DoS)

3. DNS Cache Poisoning

DNS Cache Poisoning


"What's the IP for example.com?"
"192.0.0.16"
DNS server
Authoritative nameserver
"What's the IP for example.com?"
"Hey, I am an authoritative nameserver. IP address is 192.0.0.17"
Attacker

DNS Cache Poisoning Mitigation

Red Team Tools:

- Metasploit **(DNS Amplification Modules)**: Uses vulnerable DNS servers to launch amplification attacks.
- Tools capable of launching DDoS attacks using DNS amplification techniques.
- dnsamp: Specifically designed for DNS amplification attacks.
- dnsspoof: Can poison the DNS cache by sending forged responses.
- Bettercap: Can manipulate DNS responses in transit to poison the cache.

Blue Team Tools:

- BIND/Unbound: These DNS servers support **Response Rate Limiting (RRL)** to mitigate amplification attacks.
- Fail2Ban: Can block IP addresses making abnormal or high volumes of requests.
- Firewall (IPTables/UFW): Filters and blocks malicious DNS traffic at the network level.
- Wireshark: To analyze network traffic and detect amplification patterns.

Summarizing DNS Mitigation

- Red Team Tools:
  - DNS Spoofing: dnsspoof, Ettercap, Bettercap, Responder.
  - DNS Amplification: Metasploit, LOIC/HOIC, dnsamp.
  - DNS Cache Poisoning: Metasploit, dnsspoof, Bettercap.
- Blue Team Tools:
  - DNSSEC: Secure DNS responses.
  - DoH/DoT: Encrypt DNS traffic.
  - Splunk: Monitor and detect suspicious DNS behavior.
  - Wireshark: Inspect DNS traffic in real time.
  - BIND/Unbound: DNS servers with built-in security features like RRL and DNSSEC.

FTP Threats

Threats:

- Plain-text credential transmission.
- Unauthorized data exfiltration via anonymous access.

FTP Tool Implementations

Red Team Tools:

- **Metasploit FTP exploits:** Often used to target outdated or misconfigured FTP servers.
- **Hydra/Medusa:** Brute-force FTP credentials.

Tools for Blue Team:

- **FTPS** (SSL/TLS) or **SFTP:** Ensure secure, encrypted file transfers.
- **Fail2Ban:** Block brute-force attempts on FTP login.
- **Splunk:** Monitor FTP logs for abnormal activities (e.g., mass file transfers).

Securing SMB

Threats:

SMB Relay Attacks

Exploits such as **EternalBlue**

SMB Tool Implementation

Red Team Tools:

- **Impacket (smbrelayx, secretsdump):** Used for SMB relay and hash dumping attacks.
- **Metasploit EternalBlue:** To exploit unpatched SMB vulnerabilities.

Some Blue Team Tools:

- **SMBv3 with encryption:** Enforce encrypted SMB communication.
- **BloodHound:** Map attack paths within the SMB environment.
- **Sysmon + Splunk:** Real-time monitoring for unusual SMB activities (e.g., file transfers).

Active Directory Hardening: Kerberos

Threats:

- **Kerberos Delegation** (Unconstrained, Constrained, and Resource-Based Constrained Delegation)
- Exploitation of **S4U2self** and **altservice** flags for lateral movement

Tool Implementations

Red Team Tools:

- **Rubeus:** For Kerberos ticket harvesting and S4U2self attacks.
- **Impacket (getST):** Exploits RBCD for lateral movement and privilege escalation.
- **Mimikatz:** For stealing Kerberos tickets and conducting DCSync attacks.

Blue Team Tools:

- **BloodHound:** Identify AD delegation vulnerabilities.
- **PowerView/SharpView:** Enumerate machines with unconstrained delegation.
- **Rubeus Detection:** Monitor for ticket requests related to Kerberos abuse.

DACL Hardening

Threats

Abuse of GenericAll and GenericWrite permissions on AD objects.

Tool Implementation

Red Team Tools:

- BloodHound: Maps AD ACL (Access Control List) relationships.
- PowerView: For enumeration of AD object permissions.
- Mimikatz: Can be used to dump credentials once privilege escalation is achieved.

Blue Team:

- PowerView/SharpView: Identify AD objects with risky permissions (GenericAll, GenericWrite).
- BloodHound: Track and map ACL abuse paths in AD.

Email Security

Threats:

- Phishing
- Email Spoofing
- Open SMTP Relays

Tool Implementations

Red Team Tools:

- **Gophish:** For phishing campaigns.
- **SET (Social Engineering Toolkit):** Used to craft and execute phishing attacks.
- **Spoofcheck:** For identifying vulnerable email domains.

Blue Team Tools

- **DMARC, SPF, DKIM:** Protect email domains against spoofing.
- **SpamAssassin:** Open-source tool for filtering out spam and phishing emails.
- **Splunk:** Real-time monitoring of email traffic for suspicious patterns.

Next Meetings

2024-10-29 • Next Tuesday

- Active Directory III with Ronan Boyarski

2024-10-31 • Next Thursday

- Snort with Michael Khalaf & Sagnik Chakraborty