Network attacks

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Hacking phases

1. Reconnaissance
2. Scanning
3. (enumeration)
4. **Gaining Access**
   a. **Network Attacks**
   b. System attacks
5. Maintaining access/escalating privileges
6. Clearing traces

ISSES
Co-funded by the Erasmus+ Programme of the European Union

MAC address

- “A media access control address (MAC address) **is a unique identifier assigned to a network interface controller (NIC)** for use as a network address in communications within a network segment.”
- “MAC addresses are primarily assigned by device manufacturers, and are therefore often referred to as the **burned-in address**, or as an **Ethernet hardware address**, hardware address”
- Is MAC unique?

ISSES

Co-funded by the Erasmus+ Programme of the European Union

MAC spoofing

```
pavle@pavle-ideapad:~$ macchanger -s wlp2s0
Current MAC:   70:c9:4e:[redacted] (unknown)
Permanent MAC: 70:c9:4e:[redacted] (unknown)
pavle@pavle-ideapad:~$ sudo ip link set dev wlp2s0 down
pavle@pavle-ideapad:~$ sudo macchanger -r wlp2s0
Current MAC:   70:c9:4e:[redacted] (unknown)
Permanent MAC: 70:c9:4e:[redacted] (unknown)
New MAC:       ee:a5:b6:62:d4:c6 (unknown)
pavle@pavle-ideapad:~$ sudo ip link set dev wlp2s0 up
pavle@pavle-ideapad:~$ ifconfig wlp2s0
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.109  netmask 255.255.255.0  broadcast 192.168.1.255
        ether ee:a5:b6:62:d4:c6  txqueuelen 1000  (Ethernet)
        RX packets 315963  bytes 425155682 (425.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 189688  bytes 22451111 (22.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pavle@pavle-ideapad:~$ sudo ip link set dev wlp2s0 down
pavle@pavle-ideapad:~$ sudo macchanger -p wlp2s0
Current MAC:   ee:a5:b6:62:d4:c6 (unknown)
Permanent MAC: 70:c9:4e:[redacted] (unknown)
New MAC:       70:c9:4e:[redacted] (unknown)
pavle@pavle-ideapad:~$ sudo ip link set dev wlp2s0 up
pavle@pavle-ideapad:~$ ifconfig wlp2s0
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.109  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 70:c9:4e:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 315975  bytes 425157258 (425.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 189691  bytes 22451596 (22.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Switched network sniffing

- Switches fill the MAC address table
- MAC flooding:
  - Fill the switch MAC table with fake MAC addresses (macof tool: https://kalilinuxtutorials.com/macof/)
  - When the table is full, switch starts to flood packets and acts like a hub
  - solution: **switch port security** – allow only single MAC address per port

ISSES
Co-funded by the Erasmus+ Programme of the European Union

ARP protocol

```
▸ Frame 118: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▾ Ethernet II, Src: LiteonTe_[redacted] (70:c9:[redacted]), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: LiteonTe_[redacted] (70:c9:[redacted])
    Type: ARP (0x0806)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: LiteonTe_[redacted] (70:c9:[redacted])
    Sender IP address: 192.168.1.109
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.103
```

```
▾ Ethernet II, Src: SamsungE_[redacted] (f4:0e:[redacted]), Dst: LiteonTe_[redacted] (70:c9:[redacted])
  ▸ Destination: LiteonTe_[redacted] (70:c9:[redacted])
  ▸ Source: SamsungE_[redacted] (f4:0e:[redacted])
    Type: ARP (0x0806)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: SamsungE_[redacted] (f4:0e[redacted])
    Sender IP address: 192.168.1.103
    Target MAC address: LiteonTe_[redacted] (70:c9:[redacted])
    Target IP address: 192.168.1.109
```

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

ARP table

```
pavle@pavle-ideapad:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.100            ether   d0:63:b4:00:59:40   C                     wlp2s0
_gateway                 ether   c0:c1:c0:c3:45:6f   C                     wlp2s0
192.168.1.103            ether   f4:0e:22:f4:15:83   C                     wlp2s0
192.168.1.101            ether   a4:50:46:11:5f:8f   C                     wlp2s0
```

ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

ARP poisoning

- ARP maps IP addresses to specific MAC addresses:
  - ARP query – (sent to MAC:FF:FF:FF:FF:FF:FF): What is the MAC address of the machine with IP address X?
  - ARP response from machine with IP address X – sends from the MAC address of X
- What if Y responds with MAC Y to the ARP query for IP X?
  - ARP spoofing – initiator gets the wrong MAC-IP mapping and sends packets destined to IP X to MAC Y.
- ARP poisoning tools: Ettercap, Cain & Abel
- IP DHCP snooping and ARP snooping for avoiding these attacks

ISSES
Co-funded by the Erasmus+ Programme of the European Union

DHCP protocol

- Dynamic Host Configuration Protocol

```
50 1275.0370591… 0.0.0.0          255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x5ef36f47
64 1277.8162619… 0.0.0.0          255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x5ef36f47
67 1278.8902579… 192.168.1.1      255.255.255.255    DHCP    590 DHCP Offer    - Transaction ID 0x5ef36f47
68 1278.8905763… 0.0.0.0          255.255.255.255    DHCP    342 DHCP Request  - Transaction ID 0x5ef36f47
69 1278.9032657… 192.168.1.1      255.255.255.255    DHCP    590 DHCP ACK      - Transaction ID 0x5ef36f47
```

```
▼ Option: (55) Parameter Request List
    Length: 16
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (28) Broadcast Address
    Parameter Request List Item: (2) Time Offset
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (12) Host Name
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (26) Interface MTU
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (42) Network Time Protocol Servers
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (252) Private/Proxy autodiscovery
```

```
▼ Option: (53) DHCP Message Type (ACK)
    Length: 1
    DHCP: ACK (5)
▼ Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 192.168.1.1
▼ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (86400s) 1 day
▼ Option: (1) Subnet Mask
    Length: 4
    Subnet Mask: 255.255.255.0
▼ Option: (3) Router
    Length: 4
    Router: 192.168.1.1
▼ Option: (6) Domain Name Server
    Length: 4
    Domain Name Server: 109.122.98.6
▶ Option: (255) End
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

DHCP starvation attack

- DoS type of attack
- Attacker sends fake requests with spoofed MAC addresses forcing DHCP server to lease all the IP addresses in the pool
- New users are not able to log in
- Tools: dhcpstarv, yersinia

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Rogue DHCP server attack

- Attacker starves the real DHCP server
- Attacker acts as a DHCP server, sending default gateway IP address and/or DNS IP address
- DHCP protection – DHCP snooping feature on network devices – allows DHCP traffic only from the configured/authorized DHCP server

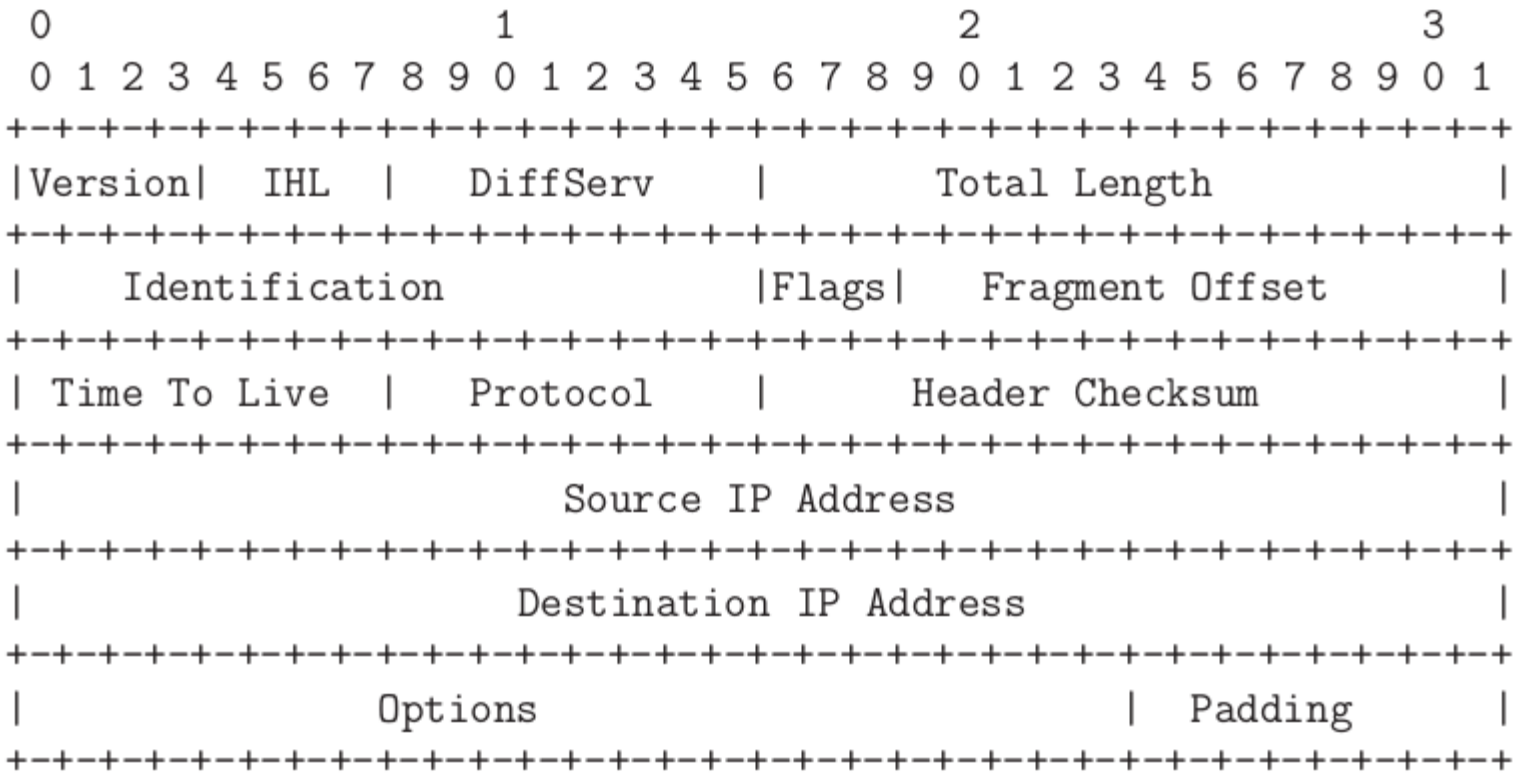
ISSES
Co-funded by the Erasmus+ Programme of the European Union

IP and TCP based attacks

ISSES

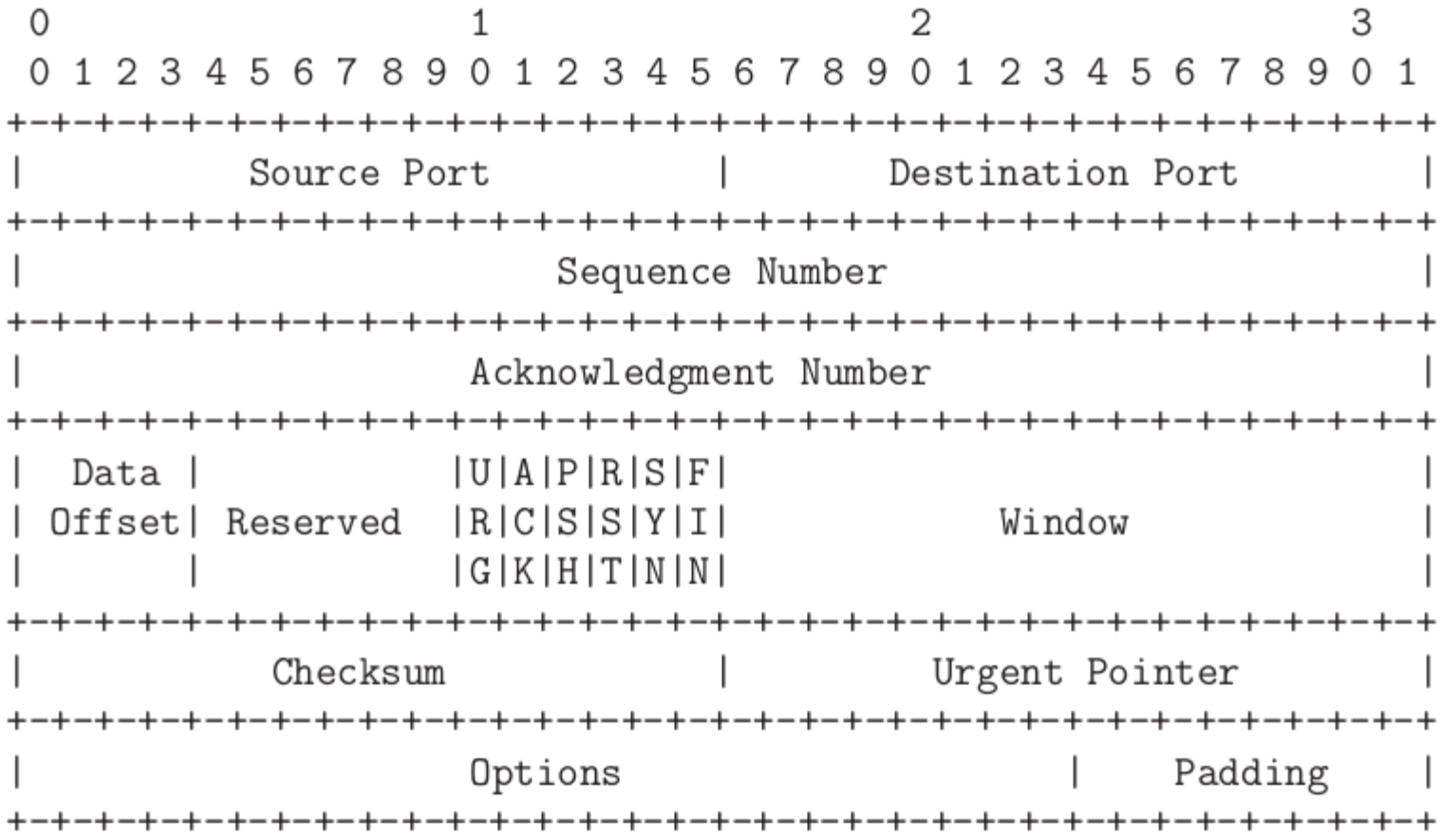
Co-funded by the
Erasmus+ Programme
of the European Union

IPv4



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

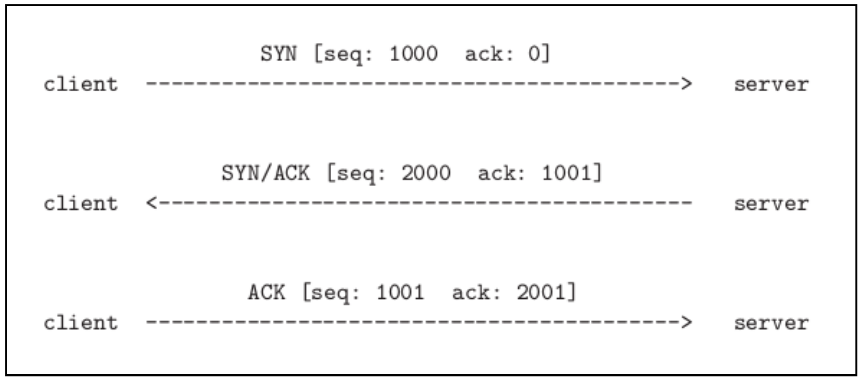
TCP



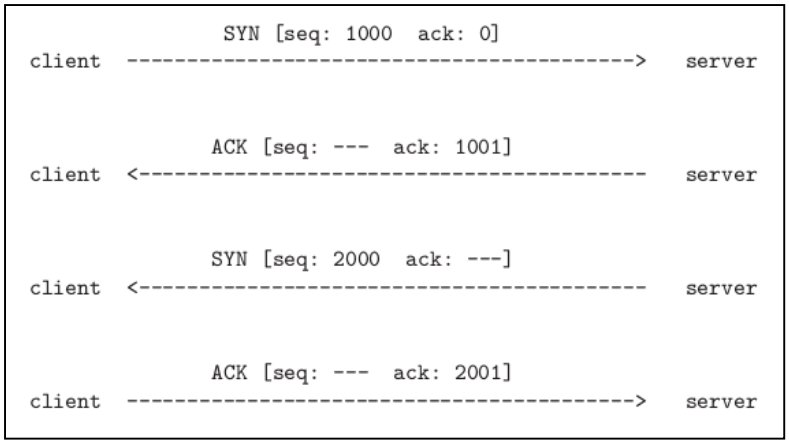
ISSES
Co-funded by the Erasmus+ Programme of the European Union

TCP handshake and split handshake

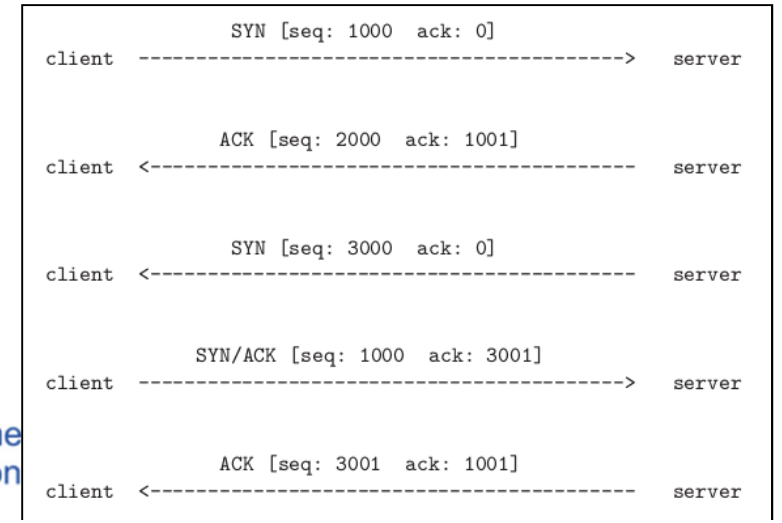
3-way handshake



Split handshake (RFC 793)



- Who sends SYN/ACK?
- Split handshake can trick the IDS/FW software on the client side



ISSES

Co-funded by the Erasmus+ Programme of the European Union

Shrew DoS attack (1)

- The retransmission decision for a TCP segment is based on logic that operates at two different timescales:
  - When traffic congestion is low, the timescale used for determining the frequency of retransmission is RTT (Round Trip Time), which is typically of the order of a few tens of milliseconds.
  - However, when congestion is high, the frequency of retransmission is determined by the much longer RTO (Retransmission Timeout), which is generally of the order of a full second.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Shrew DoS attack (2)

- TCP AIMD congestion control:
  - Upon ACK: CWND=CWND+a (e.g. a=1 SegmentSize)
  - No ACK in RTT: CWND=CWND*b (e.g. b=1/2)
  - No ACK in RTO – severe congestion CWND=1
- Initial value of RTO depends on RTT (RFC 2988).
- When RTT cannot be measured, the initial value for RTO value is set to 3s, minimum 1s.
- If no ACK is received within an RTO, the value of RTO doubles with each subsequent timeout.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Shrew DoS attack (3)

- Attacker creates a short burst which congests the link and causes regular TCP packets to be lost.
- Burst duration is approx. RTT. (so that it can't be measured)
- Next burst is after RTO (e.g. 1s)… (CWND=1)
- Next burst is after double RTO… (CWND=1)
- TCP sender stays in slow start state (CWND=1) while the average attacker traffic volume is low.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

SYN Flooding

- Attacker repeatedly sends SYN TCP segments to every port on the server using a fake IP address.
- The server responds to each such attempt with a SYN/ACK segment from each open port and with an RST segment from each closed port.
- Attacker never sends back the expected ACK segment.
- As soon as a connection for a given port gets timed out, another SYN request arrives for the same port from the attacker.
- When a connection for a given port at the server gets into this state of receiving a never-ending stream of SYN segment the intruder has a sort of perpetual half-open connection with the victim host.
- Server can protect its resources by rate limiting all incoming SYN packets.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

IP address spoofing

- IP source address spoofing refers to an intruder using one or more forged source IP addresses to launch, say, a TCP SYN flood attack on a host in another network.
- Solution ingress filtering: RFC 2827 – do not allow routers to send out packets if their source IP address does not fall in the range assigned to that network.
- Also if there is NAT between the attacker and a victim, IP spoofing is not possible

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

DNS based attacks

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

DNS cache poisoning

- Putting wrong (IP address, symbolic name) mapping into the DNS servers cache.
- The attacker has to know (by sniffing) or guess destination port (16bit) and Transaction ID (16bit) which is randomly generated
- The attacker has to plant fake responses before the proper answer comes to the server
- Due to the birthday paradox the attacker does not have to do the brute force of all Transaction IDs – few hundred Transaction IDs are sufficient
- The attacker can increase the TTL of the fake DNS entry

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

DNS query/response messages

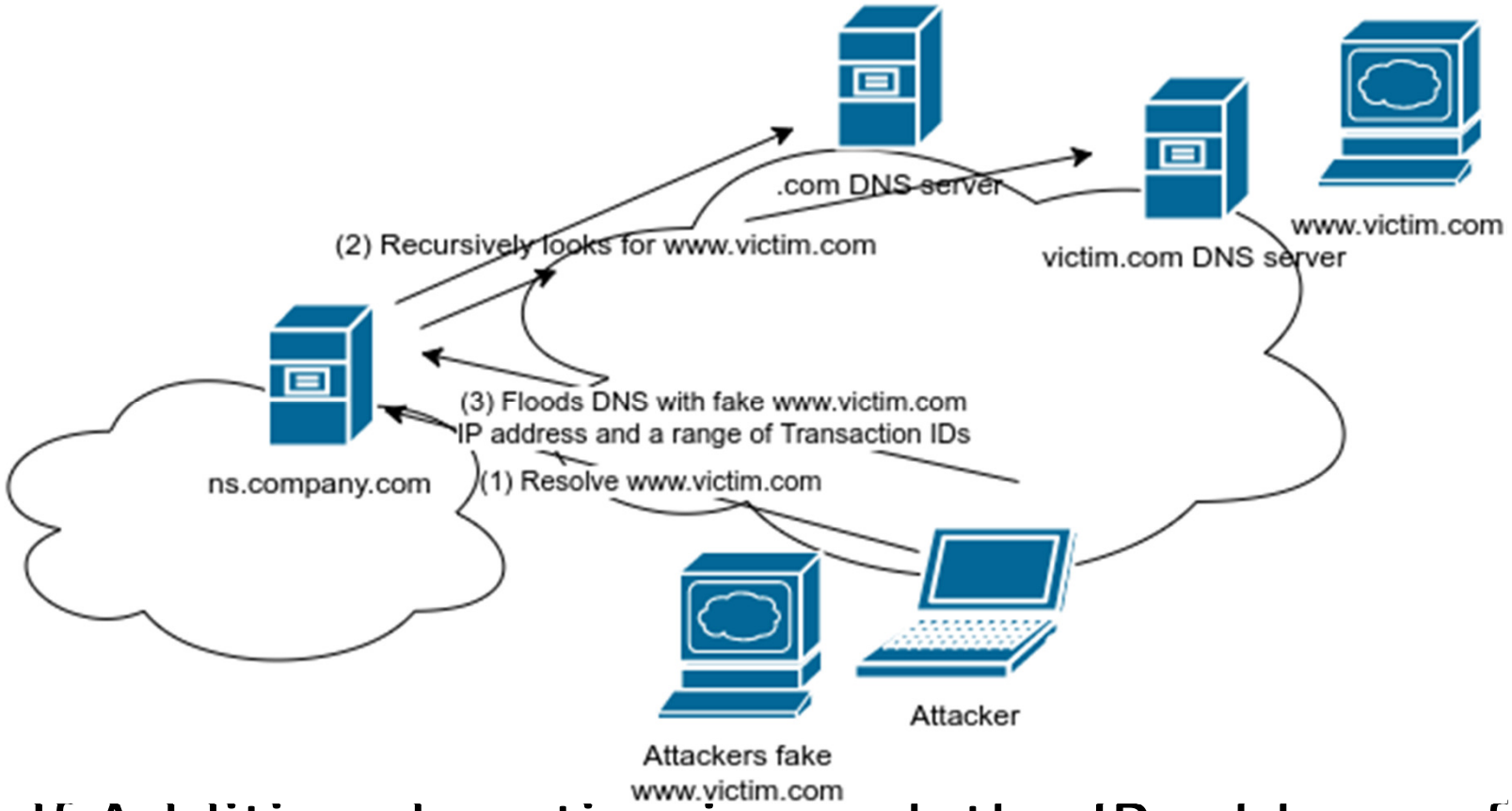
```
▸ Frame 24: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
▸ Ethernet II, Src: LiteonTe_d0:8b:bf (70:c9:4e:d0:8b:bf), Dst: Cisco-Li_b6:6f:53 (00:1c:10:b6:6f:53)
▸ Internet Protocol Version 4, Src: 192.168.1.112, Dst: 109.122.98.6
▸ User Datagram Protocol, Src Port: 58744, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xa911
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ startpage.com: type A, class IN
        Name: startpage.com
        [Name Length: 13]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Additional records
    ▸ <Root>: type OPT
    [Response In: 25]
```

```
▸ Frame 25: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface
▸ Ethernet II, Src: Cisco-Li_b6:6f:53 (00:1c:10:b6:6f:53), Dst: LiteonTe_d0:8b:bf (70:
▸ Internet Protocol Version 4, Src: 109.122.98.6, Dst: 192.168.1.112
▸ User Datagram Protocol, Src Port: 53, Dst Port: 58744
▾ Domain Name System (response)
    Transaction ID: 0xa911
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Answers
    ▾ startpage.com: type A, class IN, addr 145.131.132.68
        Name: startpage.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 30
        Data length: 4
        Address: 145.131.132.68
    ▸ startpage.com: type A, class IN, addr 145.131.132.84
    ▸ startpage.com: type A, class IN, addr 89.146.4.147
  ▾ Additional records
    ▸ <Root>: type OPT
    [Request In: 24]
    [Time: 0.034915497 seconds]
```

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

DNS cache poisoning



- If Additional section is used, the IP address of the victim.com DNS can be poisoned as well

ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

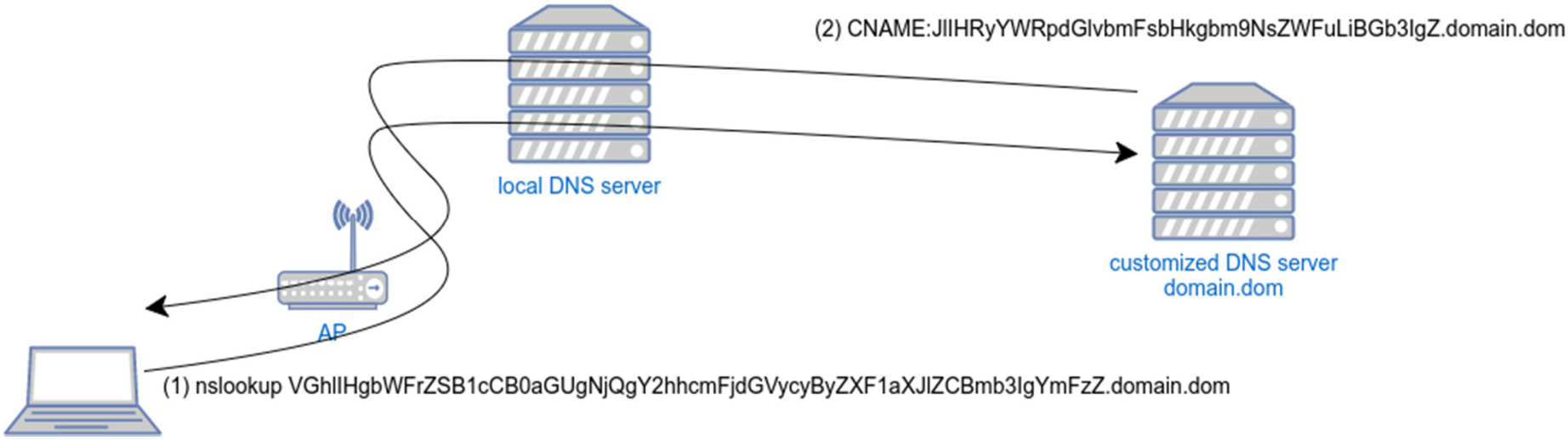
Kaminsky DNS poisoning attack

- DNS server accepts records which it has not asked for
- Attacker asks for the resolution of: 1.victim.com, 2.victim.com,…,x.victim.com which do not exist
- Attacker tries to poison the cache of these non-existant entries before the answer from ns.victim.com comes as before
- In the additional records of all these attempts it puts the fake IP address of the ns.victim.com
- Measures against: randomize port and Transaction ID numbers & bailiwick check
- Look at: https://www.youtube.com/watch?time_continue=940&v=qftKfFVHVuY&feature=emb_title

ISSES

Co-funded by the Erasmus+ Programme of the European Union

DNS tunneling/data exfiltration



- DNS traffic passes the firewall
- Use DNS to transport other traffic
- First use to bypass paid WiFi access
- Can be used for botnet C&C

ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

DNS tunneling tools

- High throughput tools:
  - DNScat: http://tadek.pietraszek.org/projects/DNScat/
  - DNS2TCP: https://www.aldeid.com/wiki/Dns2tcp
  - Iodine: https://code.kryo.se/iodine/
- Low throughput tools:
  - DNS messenger
  - MULTIGRAIN
  - Wekby

ISSES

Co-funded by the Erasmus+ Programme of the European Union

DNS fast fluxing

- A method to hide botnet
- Quickly change the IP address for a single symbolic name to hide the malicious servers.
- Used for phishing botnets
- Single flux: Quickly change DNS records
- Double flux: Bots are proxies towards the attackers server

ISSES
Co-funded by the Erasmus+ Programme of the European Union

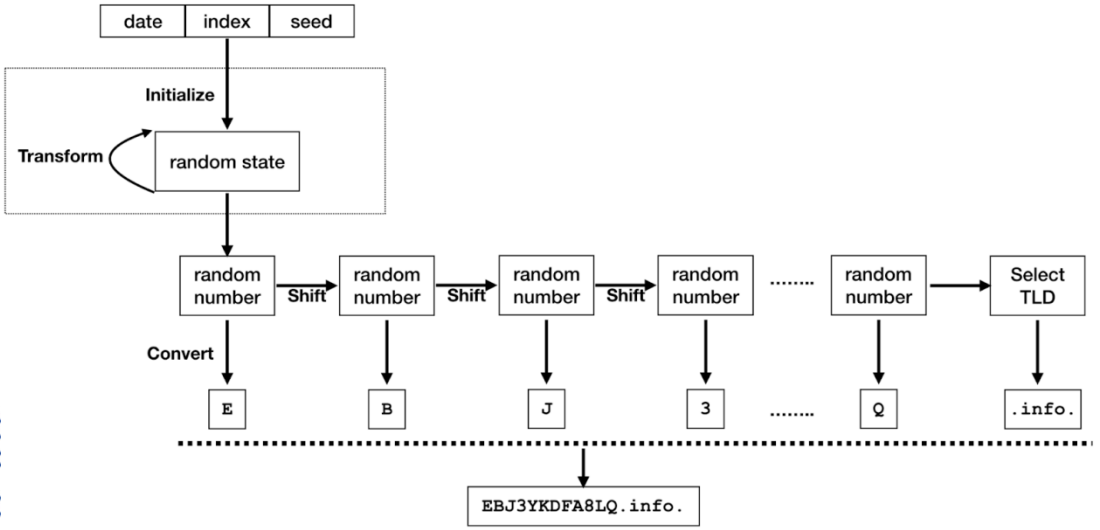
Domain generation algorithm

- No domain hardcoded into the bot malware source
- Domains for C&C dynamically created and changed periodically
- Seed for domain creation can be timestamp, message on a popular social network,…

Domain examples:

t3622c4773260c097e2e9b26705212ab85.ws
u83ccf36d9f02e9ea79a9d16c0336677e4.to
v02bec0c090508bc76b3ea81dfc2198a71.in
wa9e4628c334324e181e40f33f878c153f.hk
xdcc5481252db5f38d5fc18c9ad3b2f7fd.cn

Words made of the two word from a dictionary combination, etc.



ISSES
Co-funded b
Erasmus+ P
of the Europ