Network Protocols II

Luke Anderson

luke@lukeanderson.com.au

26th May 2017

University Of Sydney

THE UNIVERSITY OF SYDNEY

Overview

1. **Source Routing**
2. **Port Scanning and Fingerprinting**
3. **Firewalls**
4. **FTP Bounce Attacks**
5. **Traceroute**
6. **Firewalking**
7. **IP Security**
8. **Adrress Resolution Protocol**
9. **DNS**
10. **Infrastructure Attacks**
11. **Into the looking glass**

Source Routing

Source Routing

In both IPv4 and IPv6, sender is allowed to specify packet routes using **source routing** *(or "path addressing")*.

Strict source routing the sender specifies each hop that the packet takes through the network.

- IP Header: `SSRR`

Loose source routing the sender only specifies the group of hosts the packet must transfer through.

- IP Header: `LSRR`

This allows a remote attacker to facilitate non-blind attacks. Previously, they were only allowed to mount blind attacks because they never got a "reply packet".

Source Routing

- Source routing **can** be turned off in the kernel.
- Many kernels are configured to ignore source routing.
- Many firewalls and routers block source routed packets and may optionally trigger some alarms.

Port Scanning and Fingerprinting

Port Scanning

Port Scanning is the process of sending packets to all ports on a machine (or machines) to audit the available (open) services.

Example:

```
# nmap 192.168.0.1-255
Starting nmap V. 2.3BETA14 by fyodor@insecure.org ( www.insecure.org/
    nmap/ )
Interesting ports on cosmic.spectre.net (192.168.0.1):
Port    State   Protocol    Service
22      open    tcp         ssh
139     open    tcp         netbios-ssn

Interesting ports on orbital spectre.net (192.168.0.1):
Port    State   Protocol    Service
7       open    tcp         echo
9       open    tcp         discard
21      open    tcp         ftp
25      open    tcp         smtp
42      open    tcp         nameserver
53      open    tcp         domain
80      open    tcp         http

Nmap run completed -- 255 IP addresses (2 hosts up) scanned in 10
    seconds
```

OS Fingerprinting

OS Fingerprinting is the process of scanning machines using peculiarities in the IP stack to identify the vendor and operating system version.

```
# nmap -O 192.168.0.2

Starting nmap V. 2.3BETA14 by fyodor@insecure.org ( www.insecure.org/
     nmap/ )
Interesting ports on orbital.spectre.net (192.168.0.2):
Port    State   Protocol    Service
7       open    tcp         echo
9       open    tcp         discard
13      open    tcp         daytime

TCP Sequence Prediction:    Class=random positive increments
                            Difficulty=10629 (Worthy challenge)
Remote operating system guess: Windows 2000 RC1-RC3

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

Firewalls

Firewalls

A firewall is a packet filtering **gateway**, aiming to limit the number of services exposed on a connection.
Think of a wall with holes in it

Static Packet Filtering Gateway Look at a set of static rules known as **access control lists** (ACLs). Static packet filters are fast but weak. (And annoying to maintain)

Dynamic Packet Filtering Gateways Aims at being more intelligent about what packets to allow (**stateful inspection** of packet headers).

Application Level Gateways Atetempt to enhance the security further.

- In short: acts as a proxy (user authentication, no direct IP connections between inside and out).
- Doesn't support all services (so it isn't used as often).

FTP Bounce Attacks

FTP Bounce Attacks

FTP Servers can be used to launch **bounce attacks**.

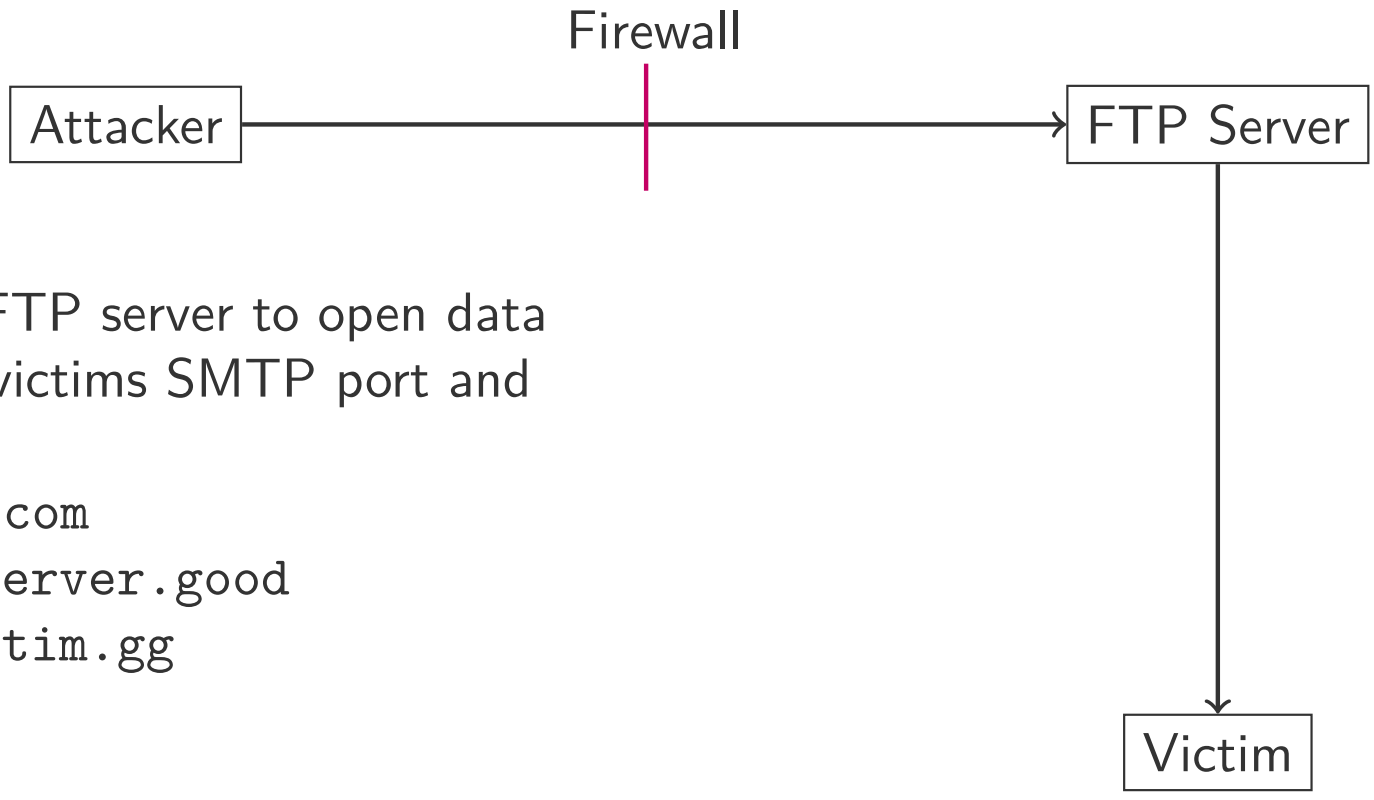
This is an example of an attack that a firewall *can't* help against.

Example

1. Attacker finds FTP server located behind a firewall - allowing write to a directory.
2. Attacker logs in, uploads a file containing SMTP commands for a spoofed mail message.
3. Attacker uses the `PORT` command to point to a victim's mail port.
4. Attacker uses the `RETR` to initiate the file transfer.
5. The FTP server will then connect to the victim's mail port, uploading valid mail commands.

https://en.wikipedia.org/wiki/List_of_FTP_commands

FTP Bounce Attacks



Attacker tells FTP server to open data connection to victims SMTP port and upload:

```
hello pizza.com
mail from: server.good
rcpt to: victim.gg
data
...
end
```

Victim gets (believable) email, spoofed

Traceroute

Traceroute

Traceroute is a network debugging utility designed to map out the pathway between hosts over IP by monotonically increasing the **time-to-live** (TTL) field in the IP header.

The TTL field is used to limit the number of hops a packet has through a network before it expires.

On expiry, an ICMP error message is generated (the time to live exceeded).

By increasing the TTL field, we will receive error messages for each hop, tracing the path taken to the destination.

Traceroute

```
1  # traceroute cassius.ee.usyd.edu.au
2  traceroute to cassius.ee.usyd.edu.au (129.78.13.49), 30 hops max, 40
       byte
3  packets
4  1 * * *
5  2 sydney-atm.vic-remote.bigpond.net.au (61.9.128.189) 34.477 ms 35.317
6  ms 32.934 ms
7  3 202.12.157.72 (202.12.157.72) 34.205 ms 36.603 ms 32.927 ms
8  4 fastethernet4-1-0.win4.Melbourne.telstra.net (139.130.61.117) 32.514
       ms
9  34.914 ms 35.385 ms
10 5 FastEthernet0-0-0.lon20.Melbourne.telstra.net (203.50.79.30) 34.258
       ms
11 32.954 ms 33.645 ms
12 6 optvs.lnk.telstra.net (139.130.6.26) 38.416 ms 34.988 ms 35.881 ms
13 7 GigEth1-0-0.sn2.optus.net.au (202.139.190.16) 47.587 ms 46.593 ms
14 48.402 ms
15 8 NSW-RNO-Dom.sn2.optus.net.au (202.139.18.114) 51.023 ms 58.395 ms
16 49.161 ms
17 9 usyd-atm-chippendale.nswrno.net.au (203.15.123.36) 81.577 ms 91.889
       ms
18 91.788 ms
19 10 su-ti.gw.usyd.edu.au (129.78.226.241) 85.420 ms 78.939 ms 91.274 ms
20 11 * * *
21 12 * * *
22 13 cassius.ee.usyd.edu.au (129.78.13.49) 94.850 ms 100.272 ms *
```

Firewalking

Firewalking

Firewalking is the process of determining the **access control lists** of packet filtering gateways (firewalks, routing...) similar to traceroute.

- Works by sending packets with a **TTL** one greater than targeted gateway.
- If the gateway allows traffic, it will forward the packets to the next hop where it will expire and we will get a message back.
- If the gateway doesn't allow traffic it will most likely drop and no response will come back.
- Through scanning, ACLs for the gateways and firewalls can be determined.

IP Security

IPSec

IPSec is the working group on security aiming at securing IPv4 and IPv6.
Two main features:

1. Authentication Header (AH)
   - Authentication and Integrity
2. Encapsulated Security Payload (ESP)
   - For confidentiality and sometimes authentication/integrity

Packets can use AH and/or ESP.
IPsec doesn't protect against.

- Traffic Analysis.
- Non-Repudiation.
- Denial-of-Service.

IPsec is used to set up **virtual private networks (VPNs)**

Authentication Header

The **Authentication Header (AH)** provides authentication (and possibly integrity) only.

Transport Mode Is applicable only to host implementations and provides protection for upper layer protocols, in addition to selected IP header fields.

Tunnel Mode Is where it protects the entire inner IP packet, including the entire IP header.

The authentication algorithm used is defined by a security association. Suitable authentication algorithms include:

- Keyed Message Authentication Codes (MACs) based on symmetric encryption algorithms.
- One way hash functions (e.g. MD5 or SHA-1).

Encapsulating Security Payload

The **Encapsulating Security Payload (ESP)** provides confidentiality for packets.

Similar to the AH, it can be used in both transport (between two hosts) or tunnel (IP tunnel between gateways) modes.

ESP is algorithm independent. Common ciphers used include 3DES, DES, CAST128 and Blowfish.

Security Association

The Authentication Header defines **Security Association** to use for a particular link (oor connection UDP/TCP).

- Authentication algorithm and mode.
- Authentication key(s).
- Encryption algorithm and mode.
- Encryption key(s).
- Presence / absence of a crypto synchronization/IV.
- Lifetime of a key or when key change should occur.
- Lifetime of the security association.
- Source address of the security association.
- Sensitivity level (SECRET/CLASSIFIED).

Issue: **Key distribution and Management**

IKE/IKE v2

"**Internet Key Exchange**"

Protocol used to set up Security Association in IPSec.

Uses X.509 certificates for authentication which are pre-shared or distributed using DNS (DNSSEC) and Diffie-Hellman to set up a shared secret. Runs as IKE daemon in user space.

Adrress Resolution Protocol

Address Resolution Protocol

Address Resolution Protocol (ARP) is used to map IP addresses to hardware addresses.

A table called the **ARP cache** is used to store the MAC address and its corresponding IP address.

When a packet is sent to a node on a network:

1. Goes to the router.
2. Queries the ARP for the MAC address matching the destination IP.
3. ARP lookup returns the MAC from the cache.
    - If it finds the address - ARP program provides it.
    - If no entry found, ARP broadcasts a special packet to all nodes.
        - The machine recognises the IP and responds with its MAC.
        - The ARP cache is updated.

Spoofing ARP

ARP is one of the simplest, but most fundamental protocols on the Internet.

Lack of strong authentication means that manipulating ARP is trivial, allows for powerful attacks to be accomplished, including many higher, more secure protocols (ssh, ssl...)

- Poisoning the ARP cache of targets.
- MAC flooding.
- Man-in-the-Middle.
- Connection hijacking.
- Denial-of-Service.
- Cloning.

ARP Attacks

As time passes, networks are migrating towards being **fully switched**. Each host is on a separate cable, so the number of machines sharing a connection are minimised.

Implications:

- Increases network performance.
- Increases security: sniffing link will only give trafffic for one host, not all on the network.

ARP Attacks

ARP facilitates Mallory to trivially launch man-in-the-middle attacks against Alice and Bob:

- Mallory poisons the ARP cache of Alice and Bob.
- Alice associates Bob's IP with Mallory's MAC.
- Bob associates Alice's IP with Mallory's MAC.
- All of Alice and Bob's traffic will now pass through Mallory.

This works even if the network is fully switched!

What if Bob is a gateway or router?

All the traffic flowing through that router is now Mallorys.

She is able to see everything!

Other ARP Attacks

MAC Flooding
Where an attacker sends spoofed ARP replies at a high rate to the switch - eventually overflowing the port/MAC table. Most switches then revert to "*full broadcast*" mode.

Denial-of-Service
ARP caches are updated with non-existent MAC addresses, causing valid frames to be dropped.

Connection hijacking

Cloning

Preventing ARP Spoofing

ARP Spoofing is very difficult to prevent:

- Enable MAC binding at a switch.
- Implementing static ARP tables.

MAC binding makes it so that once an address is assigned to an adapter it cannot be changed without authorisation.

Static ARP management is only realistically achieved in a very small network. In a large, dynamic network, it would be impossible to manage the task to keep the entries updated.

`arpwatch` for Unix based systems monitor changes in the ARP cache and alert admins to the change.

DNS

DNS

Many of the earlier problems we have discussed are a result of authentication through source IP address (and spoofing).

Many other applications also extend trust to other hosts based on their names (known as name addresses).

e.g. `elec5616.com`

The **Domain Name Service (DNS)** performs the mapping between IP address and name address.

Attacks on DNS

Similar to ARP, DNS by default does not have any form of authentication.

The ability to subvert DNS through hacking the nameserver or poisoning the cache leads to many potential attacks:

- `r*` commands, NFS (file sharing), /etc/hosts.equiv and other transitive trust relationships.
- Impersonation attacks (e.g. webserver).
- Denial-of-Service.

DNSSEC

Suite of IETF extensions to secure DNS using digital signatures, which include:

- Origin of authentication of DNS data.
- Authenticated denial of existence.
- Data integrity (not availability or confidentiality!)

.

The DNSSEC-bis is a subsequent improvement for scalability.

However, although DNSSEC has been available for years, it still has low adoption rate.

Why?
Would you sacrifice traffic loss in the event of a small error?

DNSSEC

New DNS record types:

- RRSIG
- DNSKEY
- DS
- NSEC
- NSEC3
- NSEC3PARAM

Each lookup returns RRSIG DNS record, a digital signature that can be verified via public key in DNSKEY. DS Record is used in authentication of DNSKEYs using the chain of trust. NSEC and NSEC3 records are used for robust resistance.

DNSSEC

Example:

```
1 fedoraproject.org.  46  IN  RRSIG   AAAA 5 2 60 20170620150112
      20170521150112 7725 fedoraproject.org.
      kFn2QXx6KFbEBkjw2qpZgklAH7cuMyVtpyyR9iB/WmXDoEIVlbZ5ucvq iJPAHiLp/
      TDM8miFSftRu5FpKEUrZQjwHRg1Hd1kovl/YQM3AOpbMmko ukZ7/
      kiUDedKFnvwmSoYWipp5sI80bXrSG414BiaigYz2Cn+7BHXZ6zf yGQ=
2 fedoraproject.org.  46  IN  RRSIG   A 5 2 60 20170620150112
      20170521150112 7725 fedoraproject.org. tcWndX34Xom8DnKJF9+
      rcf0OMaiuJYN0YzH8IJvbgzP5QP7TddQ8/MaT ta7Zr/
      NOBxoqzFJoIfYG9Nt92E1wfGsZT5YSMLQbi/uLcFOss/J4Susn
      IfcZ7cpQLlmAm2RKWBpMxr7+kal1EApU5Tz536zD2YCMn9Dkta3zCWqv B7k=
3 fedoraproject.org.  86386   IN  RRSIG   NSEC 5 2 86400 20170620150112
      20170521150112 7725 fedoraproject.org. i8xbJU+4
      POERYspzwDt9v5uKQkzEwNu9t1RIIdchByAmDzKbvXCehH/9
      yyQLN1jAONkzNmzjvTUiTu6MpmfQblojVLUgIOGeVadfhSqG46xobX9U 9
      uAaK12FbSSmbWPLXwIbxmyxWMvPWtzQH/gBqMpyho1f4UKznBdM1ujt 7kQ=
4 fedoraproject.org.  286 IN  RRSIG   DNSKEY 5 2 300 20170620150112
      20170521150112 7725 fedoraproject.org.
      bAu4GOlsTMQuutwtpBi5V5Jik3gNDSbNt+dcrvrMMBXuoy818XWAaKVv /Te75/
      Li2wiC8fAgnlwj/Ujs0CYlMQQr6rByiK2kqP63p63t/X4dFAfb lbOhm8kRA4t+
      DIooJm7AjBLUIP2HxdOlsMgtjHtLodHYWQu4vuEnHE/u 0/o=
```

Infrastructure Attacks

Infrastructure Attacks

The **Internet Control Message Protocol (ICMP)** is used to communicate error messages and network conditions across IP.

Like other infrastructure protocols, strong authentication is absent.

- ICMP Redirect messages can be spoofed, "redirecting" traffic (doesn't work anymore).
- ICMP error messages can be spoofed, telling targets a host victim is unavailable.

Most firewalls block ICMP into and out of the network.

Since "**ping**" uses ICMP echo, this means that sometimes all ICMP is allowed to pass (else, ping is broken).

Other Infrastructure Attacks

Likewise, other protocols (RIP, EGPR, BGP, OSPF) are open to attacks.

Common attacks with domain names involve subverting the process of domain name registrars (e.g. social engineering Verisign) in order to change root nameserver records!

Into the looking glass

It's going to get worse!

- Stealthy, anonymous, encrypted, one-way communications are difficult to detect/trace.
- Collaboration: botnets assembled from IoT devices and smart appliances!
- Darknet ("ubernets").
- Mobility ever increasing.
- Automated agents pretending to be humans (already present with Chatbots).
- Software to confuse biometric forensics.

With all of this, we are still expecting major attacks on the telecom/mobile network... any day.

What we need to do

- Rebuild the Internet from the ground up using secure building blocks.
- Build strong authentication into protocols, pretty much every component.
- Add audit trails and authentication for packets.
- Out-of-band network control.
- Stronger languages, better programming practices, better quality control.
- Secure default configs out of the box.

Essentially - everyone needs to play their part.