50005 - Networks and Communications - Lecture 7

Oliver Killane

18/04/22

WireShark

Lecture Recording

Lecture recording is available here

Definition: Credential Resuse/Stuffing

Using previously leaked/found eail-passoword combinations on other services. Useful when users reuse passwords for mutliple services.

Definition: Network Monitoring / Packet Sniffing

Listening on a network and reading packets where you (your **NIC**) are not the intended recipient.

Definition: Code/SQL Injection

Executing code on a system by passing it through normal data collection.

e.g if text entered in a website is directly substituted into a database query, by writing SQL ocde in the text entry, we can alter (or add another query) to the query generated.

Definition: Session/Cookie Hijacking

Using the cookie/authentication token form another user's session to get authenticated.

Definition: Wardriving

Identifying and compomising unsecured wireless networks.

e.g installing spyware on usecured home routers.

Definition: Wireshark

Wireshark is a network protocol analyser. It allows users to capture, analyse & deconstruct packets to analyse traffic on a network.

WireShark Modes

Promiscuous Mode

- Works for Wired and wireless.
- **NIC** does not drop packets, retains all received packets.
- When wireless, only listens on the connected network.
- Some **NIC**s ignore this (considered *impolite* and easily abused).

Monitor Mode

- Only works on wireless networks.
- **NIC** listens on all networks in range/that it can receive from.
- Wifi networks secured with authentication (e.g password) will appear scrambled (encryption).
- Most **NICs** do not support this, may require new drivers or a special **NIC**.
- **WinPcap** (windows) does not support though **AirPcap** and **Npcap** on linux do.

Sniffing Ethics

When monitoring a network, it needs to be a netywork you have permission to monitor (either wired or wireless)

Lecture Recording

Lecture recording is available here

WireShark Packet Capture

Location	Can Capture
Hub	Local traffic, Broadcast/Multicast, (Promiscuous Mode) Entire Network.
Switch	Local Traffic, Broadcast/Multicast, (Promiscuous Mode) Network connected to the same switch port.
WLAN	Local Traffic, Broadcast/Multicast, (Promiscuous Mode) Entire WLAN, (Monitor Mode) All wireless packets physically receivable/in range.

We can provide wireshark with authentication to allow it to decrypt packets on for protected networks (e.g provide the RSA key for SSL, or password for WPA/WEP).

WireShark Display Filters

Can hide or select packets based on contents, destination & source address and more. And can build up complex filters.

Example: WireShark Capture Filter

```
1 http.request.method == GET &&
2 http contains "password" &&
3 (ip.src != 10.43.54.65 || ip.dst != 10.43.54.65)
```

More Examples and filter building tutorial.

NMAP

Definition: NMAP

A network scanning tool which uses sends raw **IP** packets and monitors responses & determine the services provided by the network and its hosts.

It can be used to detect vulnerable hosts on a network.

We can scan networks using the gui, or by using the command line utility:

```
# Quick scan without checking ports
nmap -sn <ip address>

# Scan a range of ports on a host
nmap -p <start port>-<end port> <ip address>

# Scan all ports on a host
nmap -p- <ip address>

# Scan without discovery (even if the host wont respond to a ping, we can still check
    ↪ its ports)
nmap -Pn <ip address>
```