Welcome Cyber#1

Reader: reader.codaisseur.com

Slack: codaisseur-school.slack.com

Discord: https://discord.gg/qyehPh

Today’s schedule

19:00 - 20:00	☐ Ports
20:00 - 20:15	☐ Test YOUR modem
20:15 - 20:45	☐ UPnP
20:45 - 21:00	☐ Break
21:00 - 21:30	☐ Zenmap

Today:
Different modes...

DIY MODE = ON

&

Sit back and relax

Ports...

Entrance to a computer...

0 to 65535

Ports...

IMPLIES services

Ports...

FTP

SSH

TELNET

DNS

HTTPS

NTP

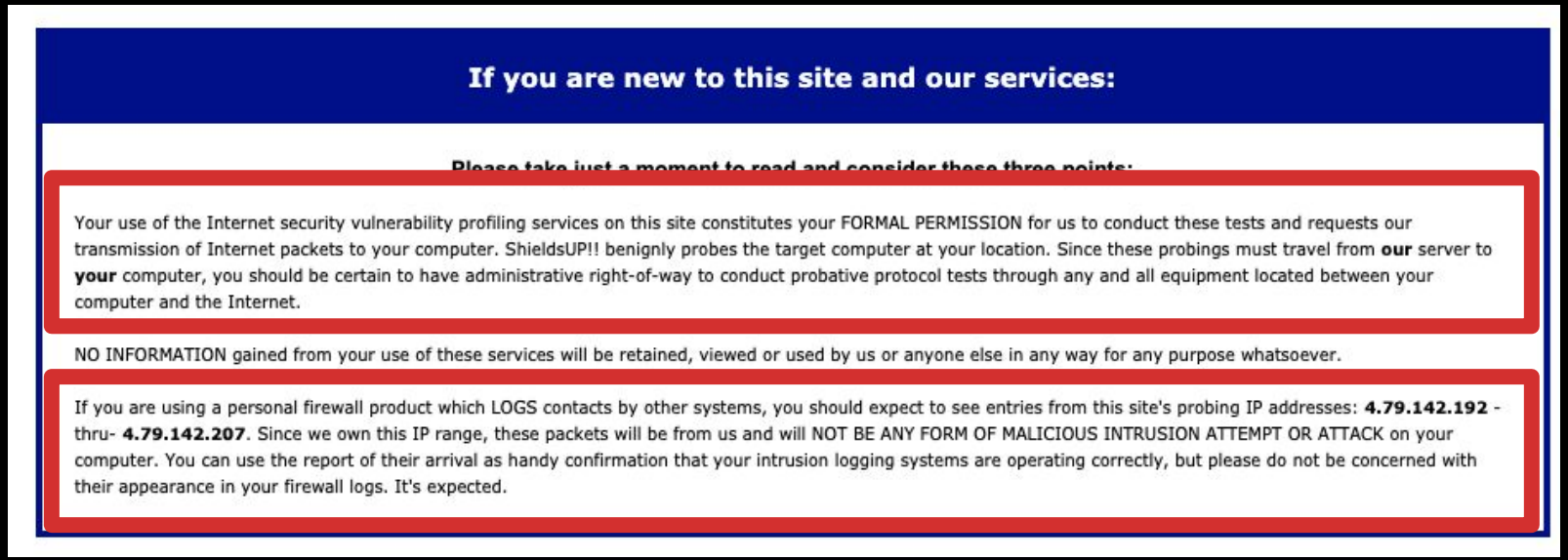
Ports...

OPEN - CLOSED - .....

Ports...

Port scanning

Serious!



If you are new to this site and our services:

Please take just a moment to read and consider these three points:

Your use of the Internet security vulnerability profiling services on this site constitutes your FORMAL PERMISSION for us to conduct these tests and requests our transmission of Internet packets to your computer. ShieldsUP!! benignly probes the target computer at your location. Since these probings must travel from **our** server to **your** computer, you should be certain to have administrative right-of-way to conduct probative protocol tests through any and all equipment located between your computer and the Internet.

NO INFORMATION gained from your use of these services will be retained, viewed or used by us or anyone else in any way for any purpose whatsoever.

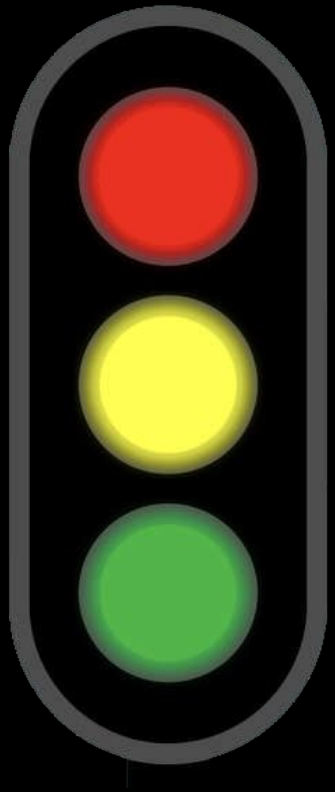
If you are using a personal firewall product which LOGS contacts by other systems, you should expect to see entries from this site's probing IP addresses: **4.79.142.192** - thru- **4.79.142.207**. Since we own this IP range, these packets will be from us and will NOT BE ANY FORM OF MALICIOUS INTRUSION ATTEMPT OR ATTACK on your computer. You can use the report of their arrival as handy confirmation that your intrusion logging systems are operating correctly, but please do not be concerned with their appearance in your firewall logs. It's expected.

DIY MODE = ON

GOTO:
https://www.grc.com/

Services -> ShieldsUP!

Sit back and relax



RED

ORANGE

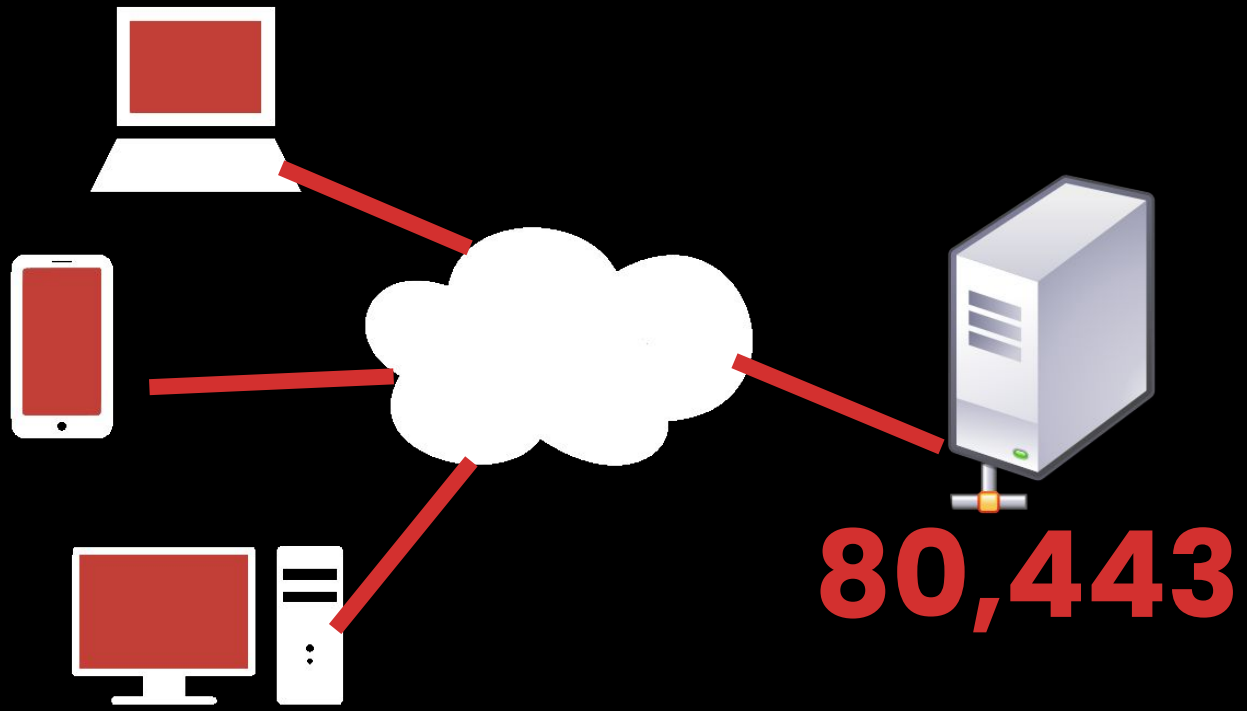
GREEN

OPEN

CLOSED

SILENT

WebServer...



WebServer...

80,443,
but why

WebServer...

80 = http = unsecure
443 = https = secure

WHY do we open port 80?

DIY MODE = ON

GOTO:

https://www.grc.com/

AND DO:

Universal Plug n'Play (UPnP)

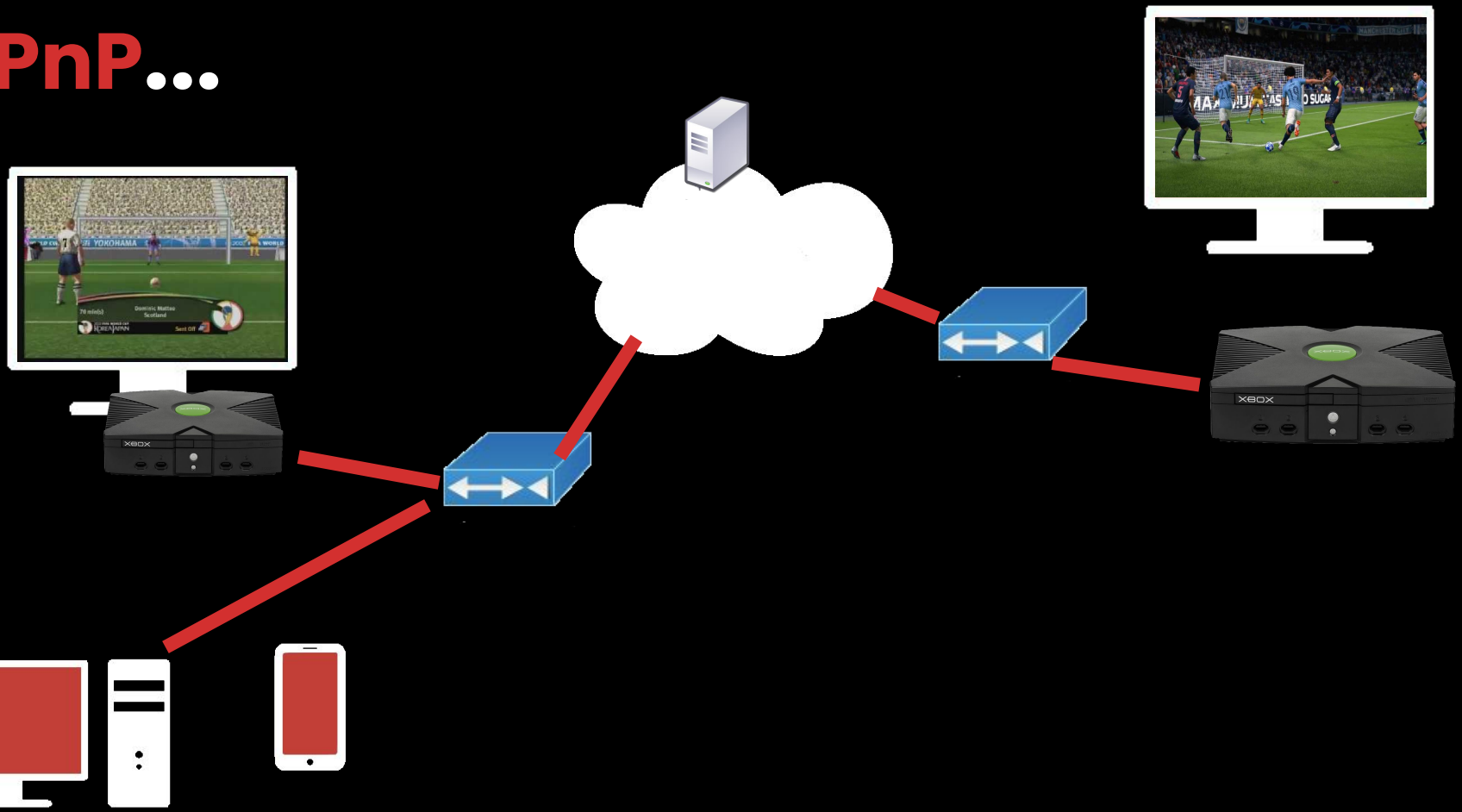
Internet Exposure Test

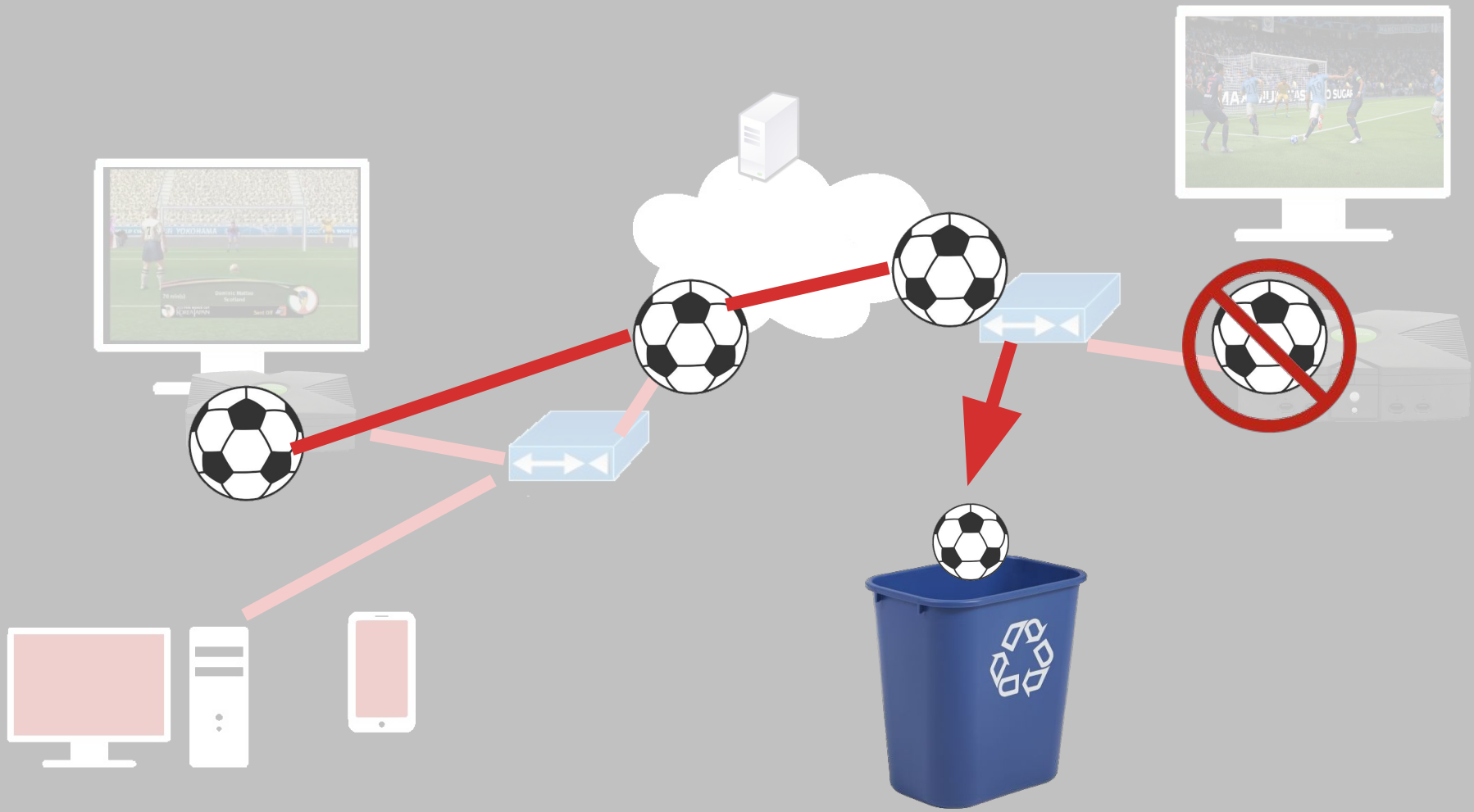
Sit back and relax

UPnP...

(Universal Plug and Play)

UPnP...





UPnP...

Opens ports
on
routers / modems

UPnP...

Internet cameras
Home automation
Game consoles
NAS
Printers
(smart)-tv's

Zenmap

Look for a host with many open ports

Network scanning...

1. Login into the kali box in the Codaisseur cloud
2. Open terminal and run zenmap
3. Scan the network
4. Find the vulnerable host

DIY MODE = ON

The End