Network Sniffing and Packet Analysis Using Wireshark

Combined **null** and **OWASP** meet
Bangalore
1101/0011/1010

tamaghna.basu@gmail.com
tamahawk-techguru.blogspot.com
twitter.com/titanlambda

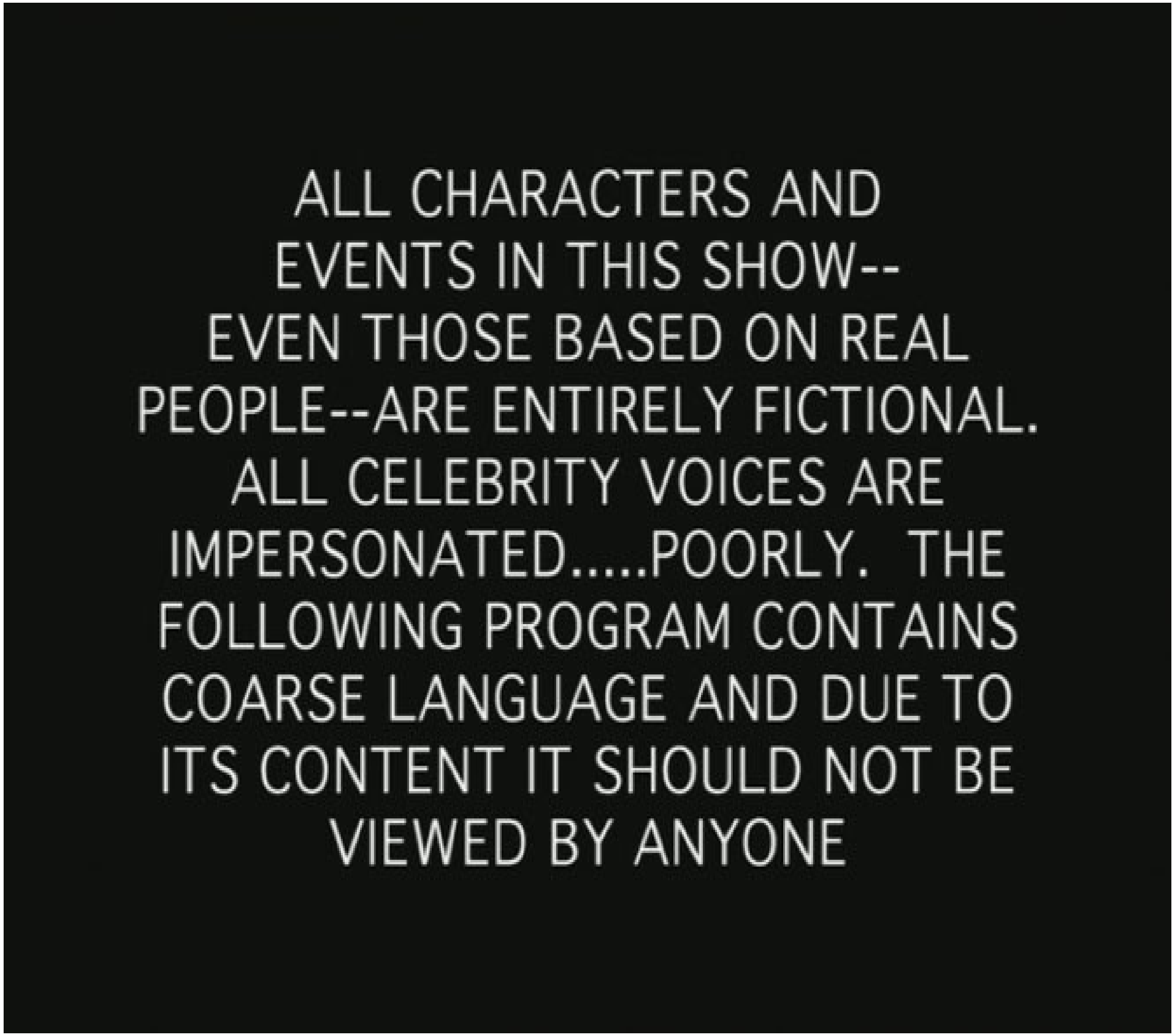
- Difficult to put all these things together

- Existing sessions – 100 – 150 slides

- Time Constraint

Topics

- Why?
- What?
- How ?
  - Basic sniffing techniques
  - Intro to wireshark
  - Closure look at protocols
  - Case Studies



ALL CHARACTERS AND
EVENTS IN THIS SHOW--
EVEN THOSE BASED ON REAL
PEOPLE--ARE ENTIRELY FICTIONAL.
ALL CELEBRITY VOICES ARE
IMPERSONATED.....POORLY. THE
FOLLOWING PROGRAM CONTAINS
COARSE LANGUAGE AND DUE TO
ITS CONTENT IT SHOULD NOT BE
VIEWED BY ANYONE

Prerequisite:

- Patience
- Patience
- Patience

AND

Or
May
be…

Why sniffing/packet analysis

- Why you?
- Why Me?
- Why Others?

Purpose of sniffing and packet analysis

- A million different things can go wrong with a computer network, from a simple spyware infection to a complex router configuration error.

- Packet level is the most basic level where nothing is hidden.

- Understand the network, who is on a network, whom your computer is talking to, What is the network usage, any suspicious communication (DOS , botnet, Intrusion attempt etc)

- Find unsecured and bloated applications – FTP sends cleartext authentication data

- One phase of computer forensic - could reveal data otherwise hidden somewhere in a 150 GB HDD.

What is this?

- Also known as packet sniffing, protocol analysis etc.

- Three Phases -
  - Collection – promiscuous mode
  - Conversion – UI based tools are better
  - Analysis – Protocol level, setting rules etc

- Get various data like text content, files, clear text authentication details etc.

- Tools
  - Sniffer – wireshark, cain and abel, tcpdump (commnd line tool), networkminer
  - Packet Analysis – wireshark, networkminer, xplico etc

Sniffing Techniques

- Promiscuous mode
- Hub environment
- Switch environment
  - Port mirroring
  - Hubbing out the target network/machine
  - ARP cache poisoning /ARP spoofing

Wireshark: History

Gerald Combs, a computer science graduate of the University of Missouri at Kansas City, originally developed it out of necessity.

The very first version of Combs’ application, called Ethereal, was released in 1998 under the GNU Public License (GPL).

Eight years after releasing Ethereal, Combs left his job and rebranded the project as Wireshark in mid-2006.

Wireshark: Features

- GPL
- Available in all platform
- Both live and offline analysis
- Understands almost all protocols, if not, add it – open source
- Filter/search packets, Expert's comment, Follow TCP Stream, Flow Graph etc
- Plenty of tutorials/documentation available
- Get sample captured packets for study - http://wiki.wireshark.org/SampleCaptures

- **Demo: Let's start eating. Feed your brain. :)**

Starters: Protocol diagnosis

- ARP
- DHCP
- HTTP/TCP
- DNS
- FTP
- Telnet
- ICMP
- SMTP

Deserts: Case Studies

- FTP Crack
- Blaster worm
- OS fingerprinting
- Port Scanning
- ICMP Covert Channel
- Browser Hijacking - spyware

Mouth Freshner: Honeynet Challenge

- Challenge 1
  - Problem Statement
  - Analysis
  - Tools used
  - Solution

MainCourse????

“Tell me and I forget. Show me and I remember. Involve me and I understand.” - chinese proverb

Thank you for witnessing this historical moment...

Answers and Discussions?

tamaghna.basu@gmail.com
tamahawk-techguru.blogspot.com
twitter.com/titanlambda