TDC 375
Network Protocols

Miscellanea
Network Management

- SNMP
- NETCONF
- syslog
- NTP
- AAA (authentication, authorization, accounting)
- Counters, flows, graphs and tools
- Documentation and maps
Scanning the Internet

- nmap/zmap versus custom tools
- How to make TCP service scanning stateless
  - Initial SYN scan with follow up app check
  - post-process pcap or real-time data extraction
- Embedded scan signatures and fingerprints
- How do you probe the entire IPv4 Internet? IPv6?
- Do you white list prefixes?
- Responding to and limiting complaints
Tor

- An anonymity-enhancing relay network
- Clients connect to an entry or bridge
- Retrieve a relay node directory
- Build a path, only client knows the full path
- Leverages proxy, X.509 and SSL/TLS technology
- Challenges and issues
- Related technologies
SDN and OpenFlow

• What exactly is SDN?
• OpenFlow as an implementation of SDN, kind of
• Much of this derives from academic interest
• What problem does these things solve?
• Is this what people want:
  • Open network hardware
  • More flexible packet processing capabilities
  • Isolation of control plane from data plane
Secret Handshake Clubs

- FIRST.org
- nsp-security
- Ops-trust
- REN-ISAC
- Other malware / spam / security related
- “The Underground”
Rent to PWN

A "rented" skimming set is merely the same set but you do not get the Encryption key.

You send us the tracks immediately after getting them, we decode, cash out approx half the cost of the rental units are €900.

After 1 use, it is yours, as we will have made more than enough money to cover our costs.
$$$ MAKE MONEY FAST $$$

<i>A</i> i have access to accounts ranging from a few hundred thousand to several million that i have the ability to wire from

<i>A</i> but i've been talking to people high up in banking and they've basically told me no wire above $50,000 will probably go through so i'd be looking at wiring below that amount
IPv6 Skiddies

A> I DDOS PPL ALL THE TIME IN HERE
A> im gonna have to refrain you from openly ddos ppl in this chan
A> ipv6
A> so none u fucks can get me

B> had ipv6
B> i got a few roots with ipv6
B> udp6.pl
B> will pwn you
B> you cannot refrain me from anything
Bling

A> Yo is this your company that sells these fake watches?
...
A> Hook me up w/ a cc once in awhile
...
A> 3/4k a day?
A> Get me in on this
A> I'd quit bots 2 make 4k$ a day
Spam in the Market Place

RULES: @/+v verify first, | For cashout join #Cashout | Report/View rippers #rippers –/- For Help join #help –/- For WesternUnion Join #WesternUnion Notice: Only English

A> selling php maler send to inbox yahoo/gmail, paypal unverified balance 100$, blocked egols, cc, payment egold

A> selling php mailer send to inbox yahoo/gmail, hackhost+cpanel, inbox, fresh cc, paypal unverify, r57+c99 shell, payment egold
The Ugly and Unmentionables

The Internet Underground is like the traditional criminal underground. All sorts of things can be bought (weapons), sold (drugs), traded (credit cards), obtained (passports) and found ([REMOVED]) there.