



Sicurezza delle reti¹

Mattia Monga

Dip. di Informatica e Comunicazione
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2010/11

¹ © 2011 M. Monga. Creative Commons Attribuzione-Condividi allo stesso modo 2.5 Italia License.
<http://creativecommons.org/licenses/by-sa/2.5/it/>. Materiale derivato da © 2010 M. Cremonini.



Lezione VI: Analisi del traffico

Esercizi



- Aprire una connessione in ascolto sulla porta tcp: 7777
- Connettersi alla connessione precedente (localhost:7777)
- Monitorare lo scambio di pacchetti con tcpdump



Le tecniche di base (nmap)

NMAP: nmap.org

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO



- Aprire una connessione in ascolto sulla porta tcp: 7777
- Effettuare vari scan con nmap
- Monitorare lo scambio di pacchetti con tcpdump



While a fugitive in Mexico, Mr. X remotely infiltrates the Arctic Nuclear Fusion Research Facility's (ANFRF) lab subnet over the Interwebs. Virtually inside the facility (pivoting through a compromised system), he conducts some noisy network reconnaissance. Sadly, Mr. X is not yet very stealthy.

Unfortunately for Mr. X, the lab's network is instrumented to capture all traffic (with full content). His activities are discovered and analyzed... by you!

[<http://forensicscontest.com/2010/02/03/puzzle-4-the-curious-mr-x>]

- 1 Qual è il numero IP di Mr. X da cui effettua gli scan?
- 2 Che tipi di scan ha usato?
- 3 Che porte sono aperte sulla macchina target?