Passive LAN Information Gathering

Roy Duisters - 30 June 2011

Supervised by:
Michiel van Veen & Marc Smeets
KPMG IT Advisory

Outline

- Introduction
- Methods
- Protocol analysis
- Proof of concept
- Conclusion
- Questions

Picture source: chelseaclock.com

Introduction 1/2

- Passive LAN Information Gathering
  - Network reconnaissance
    - Lots of multicast/broadcast traffic can be passively observed
      - ARP, CDP, SMB, HSRP, etc.
    - Passive vs active
      - Conventional reconnaissance techniques can be detected
      - Passive information gathering lowers detection risk
  - Proof of concept

Introduction – Main research question 2/2

Main research question:

Which information can be obtained by listening passively in a corporate LAN environment and how can this information be combined, correlated and reported to create an "outline" of the network, to simplify and to prevent detection of the reconnaissance phase of a penetration test?

- *Highlights of the subquestions*
  - *Selecting the protocols*
  - *Analysis of these protocols*
  - *Combining and presenting the gathered information*

Methods 1/3

- Determine the information to gather
  - By first determining which information is generally gathered during the reconnaissance phase
    - The organization and its procedures
      - Organizational structure
      - ..
    - Security of the enterprise IT environment
      - Security plans and policies
      - Technical security measures
      - ..
    - Structure / architecture of the IT infrastructure
      - Hard- and software in use
      - Important IT components
      - ..

Methods 2/3

- Passively gathering the information
  - Only broadcast / multicast traffic observed on switched / bridged LANs

- Protocol sample
  - Selection criteria
    - Common usage in enterprise LAN environments
    - Possibility whether the protocol contains useful information
  - Each protocol has been given a ”score”, based the applicability to both criteria

Methods 3/3

- Protocol sample
  - The six protocols with the highest ”score” have been selected
    - mDNS, SMB Browser, DHCP, NBNS, STP, CDP
- Selected protocols were analysed on
  - Functionality
  - Protocol details
  - Usability for network profiling

Protocol Analysis – Two interesting protocols 1/5

- Server Message Block Browser
  - Functionality
    - Provides access to files/printers/etc.
    - Mainly used on Microsoft Windows networks
  - Interesting information for network profiling
    - Hosts / domains advertise themselves periodically
      - Containing the hostname, configured domain / workgroup, OS version, etc.
      - Flags indicate the services the system offers
        - NT workstation, print queue, SQL server, domain controller, etc.

Protocol Analysis – Two interesting protocols 2/5

- Cisco Discovery Protocol
  - Functionality
    - Shares network information between (mainly Cisco) devices
  - Interesting information for network profiling
    - Information about the connected network device
      - Platform, OS, capabilities, etc.
    - Information about the connected network
      - VLAN information (connected and voice)

Protocol Analysis – Combining data 3/5

- Combining the pieces of the puzzle
  - Map information to a single system
    - By source MAC or IP (depending on the protocol)
  - Map the systems to a single (L3) subnet
    - By the IP subnet
  - Map systems to a single (L2) network
    - By the source traffic capture
  - Difficulties
    - Protocols from multiple layers from the OSI model
    - No guarantee that information will be obtained

Picture source: Englishforeveryone.org

Protocol Analysis 4/5

- Generally gathered information (recap)
  - The organization and its procedures
    - E.g. naming procedures, physical locations
  - Security of the enterprise IT environment
    - E.g. security devices, password policies
  - Structure / architecture of the IT infrastructure
    - E.g. systems that store interesting data

Protocol Analysis 5/5

	mDNS	SMB Browser	DHCP	NBNS	STP	CDP
Organization and procedures	🟡	🟩	🟨	🟡	🟫	🟨
Security of the IT environment	🟥	🟥	🟥	🟥	🟥	🟨
Structure/ architecture	🟡	🟢	🟩	🟡	🟨	🟩

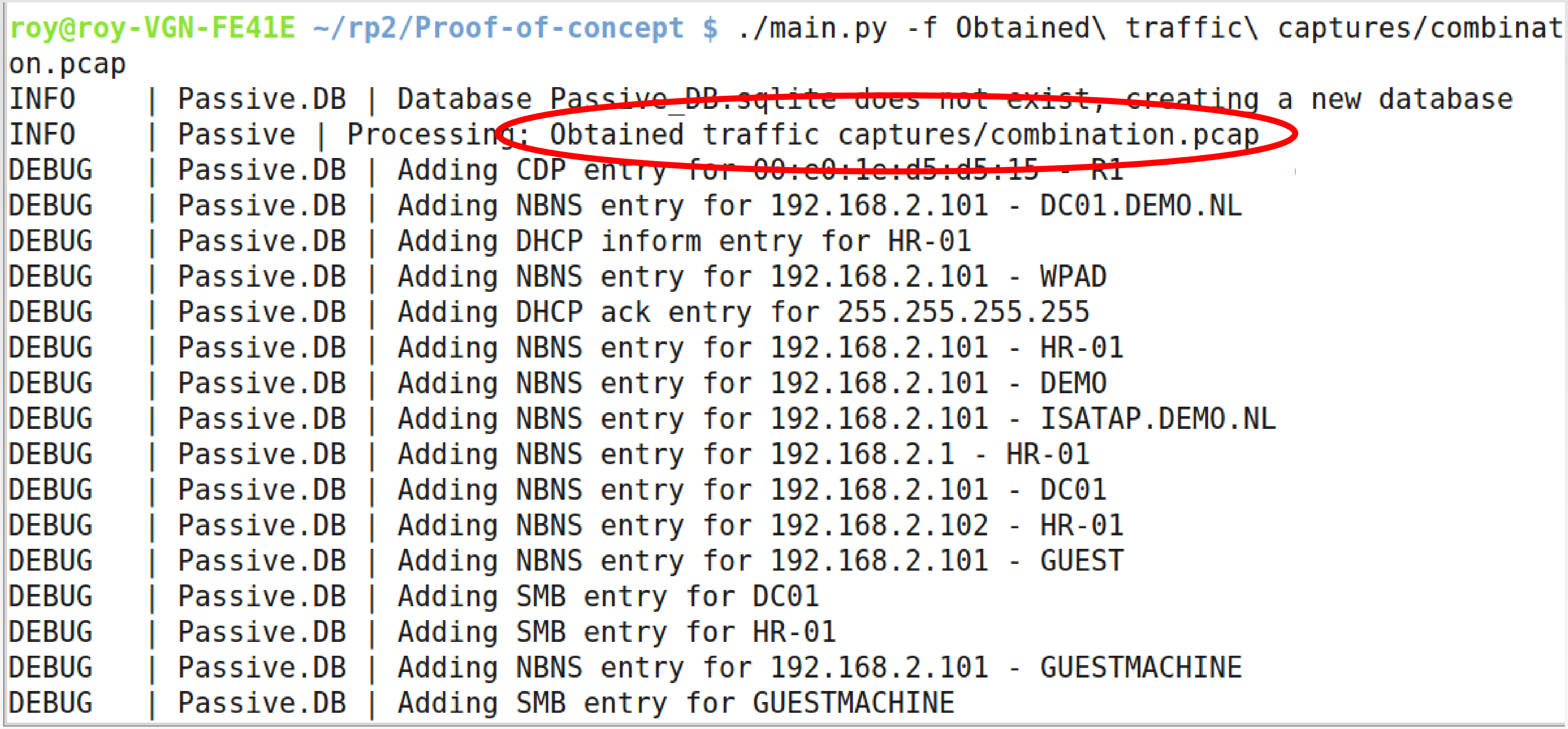
No information available ←→ Directly usable information

🟫 🟥 🟨 🟡 🟩 🟢

Proof of concept

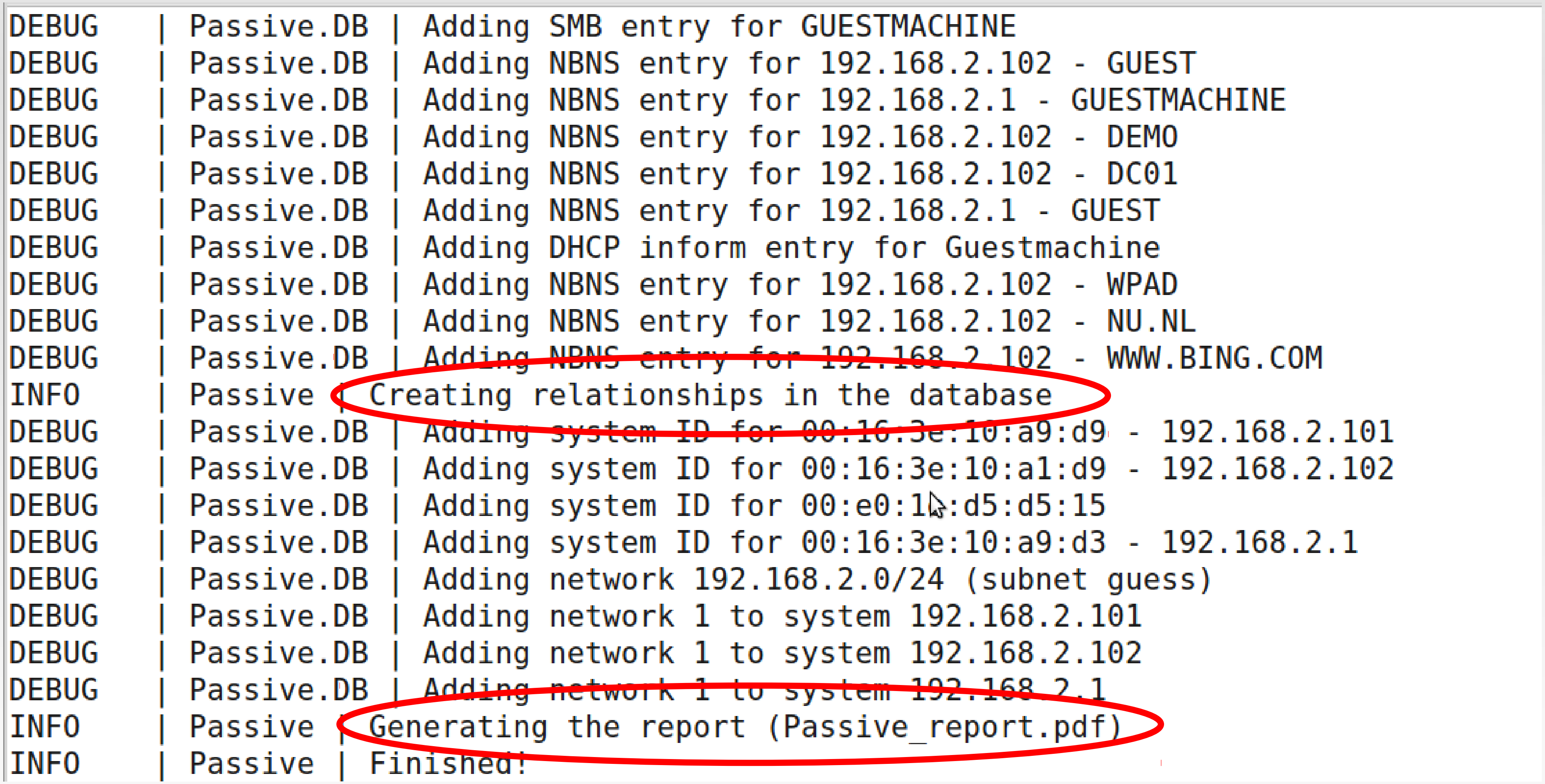
- Implementation of the previously described technique
  - Parses PCAP traffic captures
  - Gathers information from five protocols
    - Makes use of the Scapy library
  - Writes gathered information to a database
  - Creates relations between the data
  - Generates an example report

Proof of concept - Demo



```
roy@roy-VGN-FE41E ~/rp2/Proof-of-concept $ ./main.py -f Obtained\ traffic\ captures/combinat
on.pcap
INFO     | Passive.DB | Database Passive_DB.sqlite does not exist, creating a new database
INFO     | Passive | Processing: Obtained traffic captures/combination.pcap
DEBUG    | Passive.DB | Adding CDP entry for 00:e0:1e:d5:d5:15 - R1
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.101 - DC01.DEMO.NL
DEBUG    | Passive.DB | Adding DHCP inform entry for HR-01
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.101 - WPAD
DEBUG    | Passive.DB | Adding DHCP ack entry for 255.255.255.255
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.101 - HR-01
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.101 - DEMO
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.101 - ISATAP.DEMO.NL
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.1 - HR-01
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.101 - DC01
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.102 - HR-01
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.101 - GUEST
DEBUG    | Passive.DB | Adding SMB entry for DC01
DEBUG    | Passive.DB | Adding SMB entry for HR-01
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.101 - GUESTMACHINE
DEBUG    | Passive.DB | Adding SMB entry for GUESTMACHINE
```

Proof of concept - Demo



```
DEBUG    | Passive.DB | Adding SMB entry for GUESTMACHINE
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.102 - GUEST
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.1 - GUESTMACHINE
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.102 - DEMO
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.102 - DC01
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.1 - GUEST
DEBUG    | Passive.DB | Adding DHCP inform entry for Guestmachine
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.102 - WPAD
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.102 - NU.NL
DEBUG    | Passive.DB | Adding NBNS entry for 192.168.2.102 - WWW.BING.COM
INFO     | Passive | Creating relationships in the database
DEBUG    | Passive.DB | Adding system ID for 00:16:3e:10:a9:d9 - 192.168.2.101
DEBUG    | Passive.DB | Adding system ID for 00:16:3e:10:a1:d9 - 192.168.2.102
DEBUG    | Passive.DB | Adding system ID for 00:e0:1[illegible]:d5:d5:15
DEBUG    | Passive.DB | Adding system ID for 00:16:3e:10:a9:d3 - 192.168.2.1
DEBUG    | Passive.DB | Adding network 192.168.2.0/24 (subnet guess)
DEBUG    | Passive.DB | Adding network 1 to system 192.168.2.101
DEBUG    | Passive.DB | Adding network 1 to system 192.168.2.102
DEBUG    | Passive.DB | Adding network 1 to system 192.168.2.1
INFO     | Passive | Generating the report (Passive_report.pdf)
INFO     | Passive | Finished!
```

Proof of concept - Demo

The example PDF report

Conclusion

- Main research question

Which information can be obtained by listening passively in a corporate LAN environment and how can this information be combined, correlated and reported to create an "outline" of the network, to simplify and to prevent detection of the reconnaissance phase of a penetration test?

  - One can passively create a profile of the network
  - Outcome is highly dependent on the available protocols
  - A combination of methods is required to obtain all information

Questions

Thank you for your attention!

Questions?