A Next Generation DB Scanner

Nelson Brito
Security Researcher & Enthusiast

Agenda

- Introduction
- Motivation
- Microsoft SQL Server
- VSAM and ESAM
- Demonstration
- Questions and Answers

BSIDES LATAM

Introduction

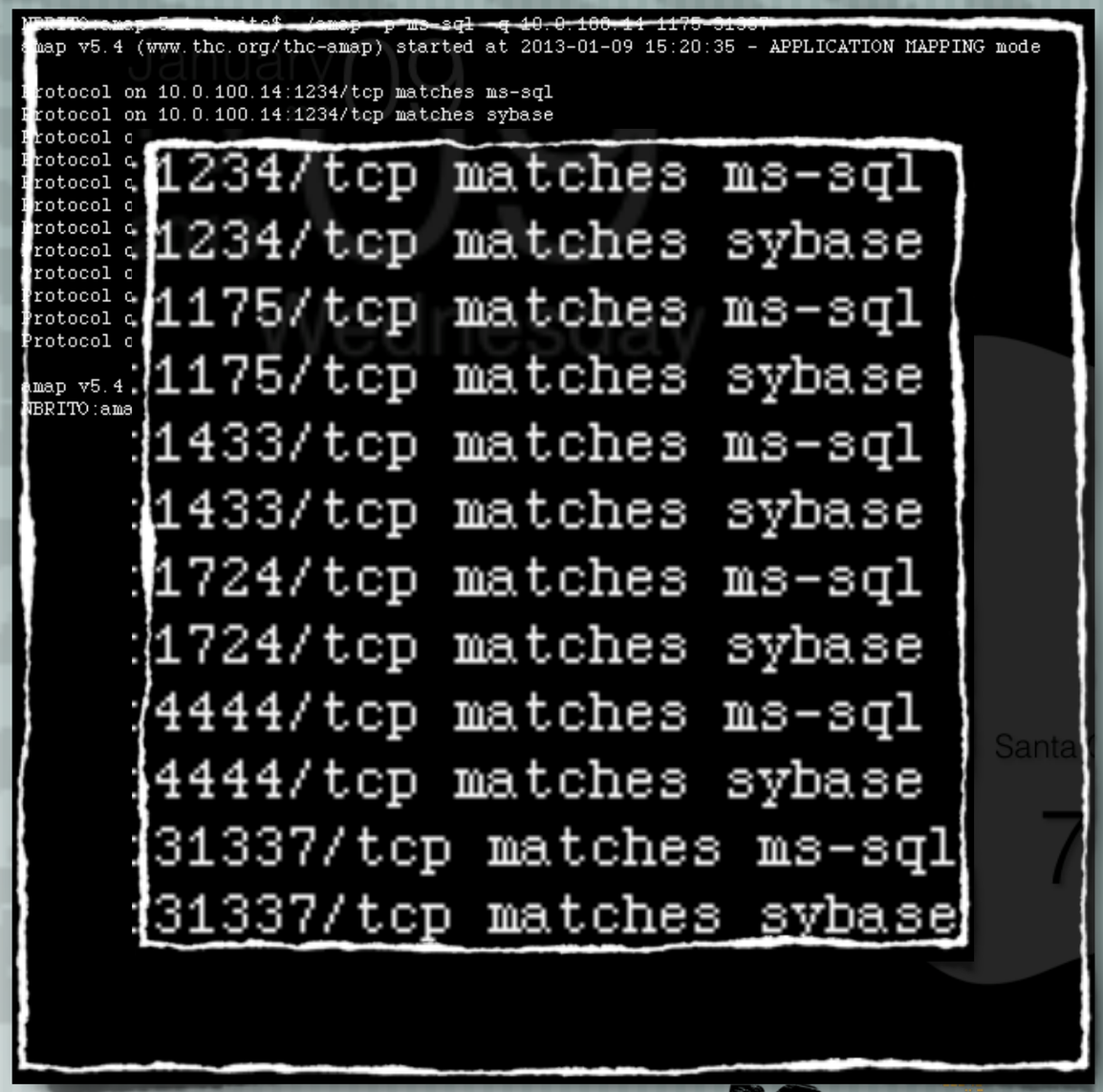
Fingerprinting Services

Banner Grabbing in the early ages, i.e., tools were only able to identify ASCII based services.

Then THC released the first next generation scanning tool, which goes beyond the Banner Grabbing...

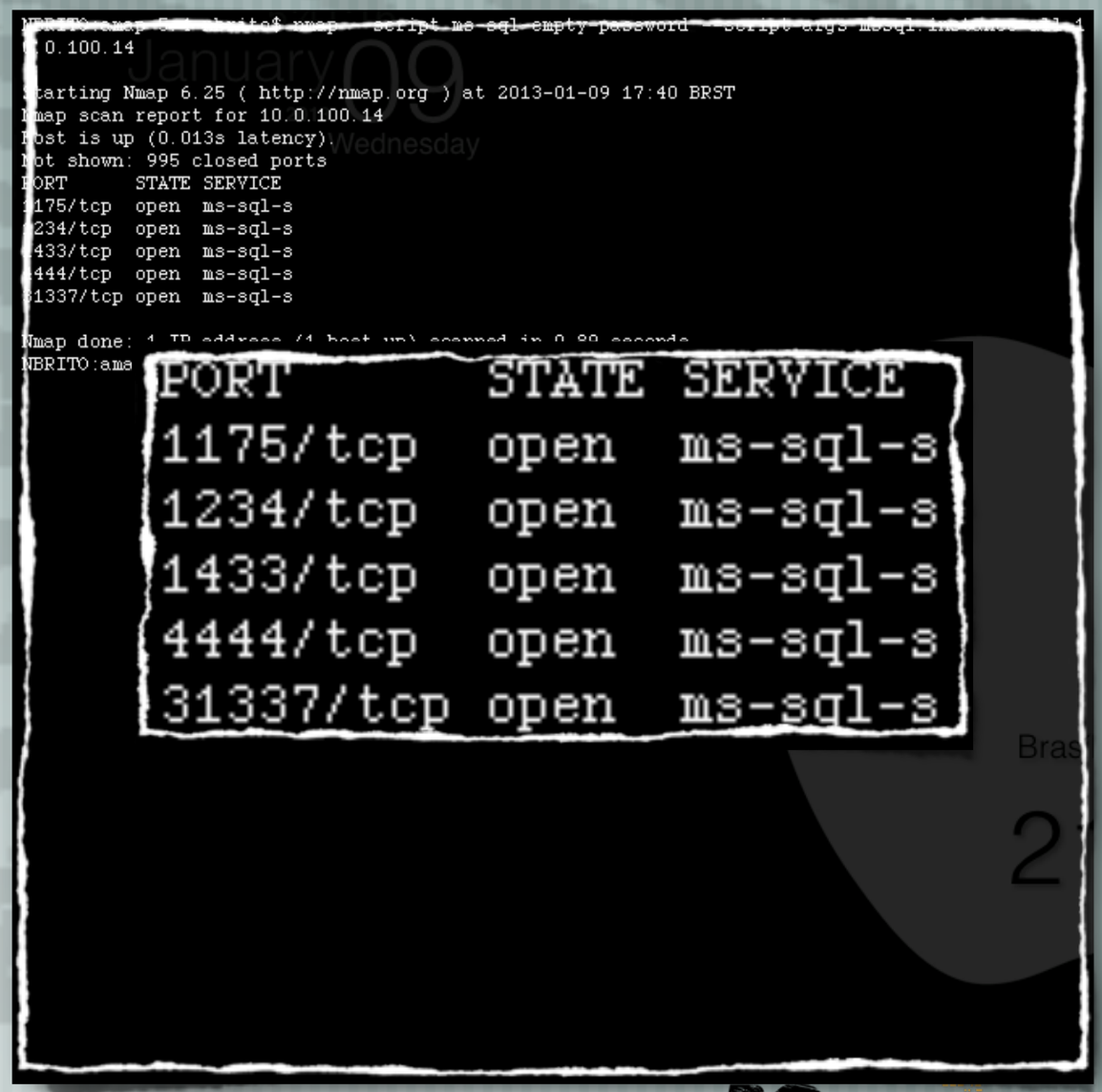
As described by van Hauser (THC):

- "Amap was the first next-generation scanning tool for pen-testers. It attempts to identify applications even if they are running on a different port than normal."
- "It also identifies non-ASCII based applications. This is achieved by sending trigger packets, and looking up the responses in a list of response strings."



Fingerprinting Services

- THC-AMAP v4.0 (July 2003) was the very first tool attempting to identify applications' version, even those non-ASCII and running in dynamic ports.
- NMap 3.50 (February 2004) has also included the ability to identify applications' version.
- Both of them do not perform an accurate identification of version, patch level and further...
  - I am not blaming the tools... They are great.
  - We will see what they are missing. WAIT!!!



Motivation

The [IN]s Problems

HIPAA

PCI-DSS

HITECH

FISMA

Sarbanes-Oxley

ISO/IEC 15408

ISO/IEC 27001

BSIDES LATAM

[V | P | D] Scanners

- [Vulnerability | Port] Scanners target hosts instead of the actual databases, i.e., they "usually" do not look for database instances and/or do not report an accurate version, as well as patch level.
- In the real world, one single host may have multiple databases, with multiple instances, multiple versions and multiple patch levels

- Database Scanners often require a valid and privileged user account to perform such task.
- Questions:
  - Does it work for a penetration test?
  - Does it work for an audit and vulnerability assessment?
  - Would you ask DBA's password to show how lame he is?

BSIDES LATAM

[V | P | D] Scanners

Dave Aitel <dave@immunityinc.com> February 6, 2013 6:07 PM
To: dailydave@lists.immunityinc.com Hide Details
[Dailydave] Catch22's in Vulnerability Management All Mail
Security: ✪Signed with unknown key (0xDA25B44B)

I love both our Qualys and Tenable friends, but I have to say, I worry about "authenticated scans". Perhaps my worry is unwarranted, but having a domain admin that is connecting to and trying to authenticate to every host on the network seems like a very bad idea.

For example:

- What if you do a NTLM proxy attack?
- What if you downgrade your accepted protocols to NTLMv1 and then crack the hash and now are domain admin for free?
- What if there is some vulnerability in the web apps or host box that supports these programs?
- When Qualys, for example, logs into MS SQL, and I have MITM on that network, why can't I just take over the connection and be admin from then on?

https://community.qualys.com/docs/DOC-4095
http://static.tenable.com/documentation/nessus_credential_checks.pdf

If these attacks work, it's a bit of a catch22. In order to achieve compliance, you must be out of compliance!

I assume people are using authenticated scans, because without it, you're generally getting lots of false positives to weed through, which is annoying (and for which we sell CANVAS plugins >).

-dave

Beyond the HOST

MSSQLSERVER

BSIDES LATAM

Beyond the HOST

MSSQLSERVER
(1433/TCP)

BillingDB
(1234/TCP)

CreditCardDB
(1175/TCP)

DBPayroll
(1337/TCP)

EvaluationDB
(1724/TCP)

FinancialDB
(2016/TCP)

BSIDES LATAM

Microsoft SQL Server

"SQL Server 2000 introduces the ability to host multiple instances [...] the multiple instances cannot all use the standard SQL Server session port. While the default instance listens on TCP port 1433, named instances listen on any port assigned to them."

"The SQL Server Resolution Service [...] provides a way for clients to query for the appropriate network endpoints to use for a particular instance of SQL Server."

Microsoft SQL Server version can be gathered and fingerprinted using:

- SQL Server Resolution Protocol (SSRP)
- Tabular Data Stream Protocol (TDS)

NOTE: No authentication and valuable information.

BSIDES LATAM

Beyond the TRUE & FALSE

- Information Security (just like the world for that matter) goes beyond white and black..... Or true and false!
  - There are “A thousand shades of gray”.

0
(FALSE)

1
(TRUE)

Beyond the TRUE & FALSE

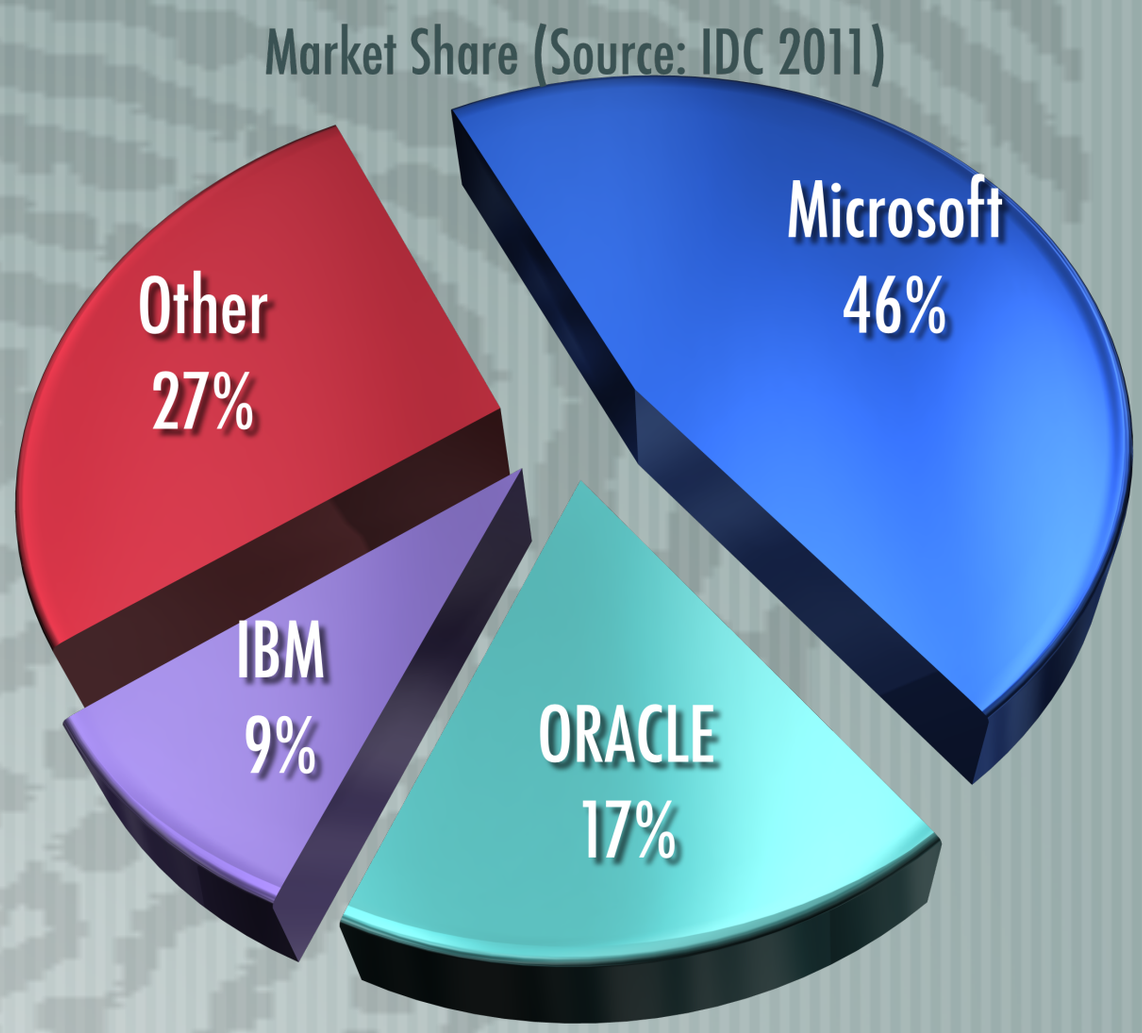
- Information Security (just like the world for that matter) goes beyond white and black..... Or true and false!
  - There are “A thousand shades of gray”.
  - Risk is not restricted to true and false.

0%	1% 2% [...] 98% 99%	100%

Microsoft SQL Server

Microsoft SQL Server

- Heavily used by Mission Critical Operations, Business Intelligence, Big Data, Data Warehouse, etc..
- Widely deployed in the Brazilian Market, as seen in Case Studies on Microsoft's website.
- Installed (by "default") with some Microsoft's Applications:
  - Microsoft Visual Studio, Microsoft Office, etc...



BSIDES LATAM

What if... Map the versions?

Microsoft SQL Server

What if... Map the versions?

Microsoft SQL Server

10

What if... Map the versions?

Microsoft SQL Server

10

2008

What if... Map the versions?

Microsoft SQL Server	
10	50
2008	

What if... Map the versions?

Microsoft SQL Server	
10	50
2008	R2

What if... Map the versions?

Microsoft SQL Server		
10	50	2550
2008	R2	

What if... Map the versions?

Microsoft SQL Server		
10	50	2550
2008	R2	SP1 GDR (MS12-070)

VSAM and ESAM

VSAM and ESAM

- VERSION Scoring Algorithm Mechanism:
  - Targets the database instances.
- EXPLOIT Scoring Algorithm Mechanism:
  - Targets the host, based on the previous VSAM results, i.e., the database instances.
- Powered by Exploit Next Generation++ Technology.

```
VSAM( 1):   16% Microsof
VSAM( 1):   16% Microsof
VSAM( 1):   16% Microsof
VSAM( 1):   16% Microsof
VSAM( 1):   16% Microsof
VSAM( 1):   16% Microsof
```

```
ESAM( 3):   33% KB307540
ESAM( 6):   66% KB317748
ESAM( 4):   33% MS00-092
ESAM( 5):   33% MS01-032
ESAM( 5):   33% MS01-041
ESAM( 6):   33% MS01-060
ESAM( 7):   66% MS02-007
ESAM( 9):   66% MS02-020
ESAM( 7):   66% MS02-030
ESAM( 7):   66% MS02-034
ESAM( 7):   66% MS02-038
ESAM( 9):   50% MS02-039
ESAM( 9):   66% MS02-043
ESAM( 8):   66% MS02-056
ESAM( 9):   66% MS02-061
ESAM( 8):   83% MS03-031
ESAM( 9):  100% MS08-040
ESAM(10):  100% MS09-004
ESAM( 5):   83% MS12-070
```

SIDES LATAM

Version	BillingDB	CreditCardDB	DBPayroll	Evaluation	FinancialDB	MSSQLSERVER	TOTAL
8.0.311				✓			16%
8.0.382					✓		16%
8.0.534		✓					16%
8.0.636			✓				16%
8.0.766						✓	16%
8.0.2039	✓						16%

Version	BillingDB	CreditCardDB	DBPayroll	Evaluation	FinancialDB	MSSQLSERVER	TOTAL
RTMa				✓			16%
SP1 Beta					✓		16%
SP2a		✓					16%
SP2+MS02-039		✓					16%
SP3a					✓		16%
SP4	✓						16%

Vulnerability	RTMa	SP1 Beta	SP2a	SP2+MS02-039	SP3a	SP4	TOTAL
KB307540	✓	✓					33%
KB317748	✓	✓	✓	✓			66%
MS00-092	✓	✓					33%
MS01-032	✓	✓					33%
MS01-041	✓	✓					33%
MS01-060	✓	✓					33%
MS02-007	✓	✓	✓	✓			66%
MS02-020	✓	✓	✓	✓			66%
MS02-030	✓	✓	✓	✓			66%
MS02-034	✓	✓	✓	✓			66%
MS02-038	✓	✓	✓	✓			66%
MS02-039	✓	✓	✓				50%
MS02-043	✓	✓	✓	✓			66%
MS02-056	✓	✓	✓	✓			66%
MS02-061	✓	✓	✓	✓			66%
MS03-031	✓	✓	✓	✓	✓		83%
MS08-040	✓	✓	✓	✓	✓	✓	100%
MS09-004	✓	✓	✓	✓	✓	✓	100%
MS12-070	✓	✓	✓	✓	✓		83%

Vulnerability	Evaluation	FinancialDB	CreditCardDB	DBPayroll	MSSQLSERVER	BillingDB	TOTAL
KB307540	✓	✓					33%
KB317748	✓	✓	✓	✓			66%
MS00-092	✓	✓					33%
MS01-032	✓	✓					33%
MS01-041	✓	✓					33%
MS01-060	✓	✓					33%
MS02-007	✓	✓	✓	✓			66%
MS02-020	✓	✓	✓	✓			66%
MS02-030	✓	✓	✓	✓			66%
MS02-034	✓	✓	✓	✓			66%
MS02-038	✓	✓	✓	✓			66%
MS02-039	✓	✓	✓				50%
MS02-043	✓	✓	✓	✓			66%
MS02-056	✓	✓	✓	✓			66%
MS02-061	✓	✓	✓	✓			66%
MS03-031	✓	✓	✓	✓	✓		83%
MS08-040	✓	✓	✓	✓	✓	✓	100%
MS09-004	✓	✓	✓	✓	✓	✓	100%
MS12-070	✓	✓	✓	✓	✓		83%

Demonstration

Touching the UNTOUCHABLE!

SQL Server 2000	SQL Server 2000	SQL Server 2000	SQL Server 2000	SQL Server 2008 R2	SQL Server 2014
					
10.100.100.11 1434/UDP 1433/TCP	10.100.100.12 1175/TCP 1234/TCP 1337/TCP 1434/UDP 1433/TCP 1724/TCP 2016/TCP	10.100.100.13 1175/TCP 1234/TCP 1337/TCP 1433/TCP 1434/UDP 1724/TCP 2016/TCP	10.100.100.14 1175/TCP 1234/TCP 1337/TCP 1433/TCP 1434/UDP 1724/TCP 2016/TCP	10.100.100.15 1337/TCP 1433/TCP 1434/UDP	10.100.100.16 1433/TCP 1434/UDP

BSIDES LATAM

Questions and Answers

Questions???

COUNTDOWN

Competencies		Results	
Residual Evidence Rate		0%	
Harmful Scanning Rate		0%	
Version/Vulnerability Detection Rate		99,99%	
HIPS/NIPS Blocking Rate		0%	
Traffic Behavior		Nonmalicious	
Database Credentials		NONE	
	Technique	Fingerprinting	Scanning (`-S`)
Packet Rate (Fingerprinting vs. Scanning)	Full (SSRP*/TDS)	((# of Instances x 2) + 1) x (# of Hosts)	((# of Instances x 2) + 1) x (# of Hosts)
	Pre-Login (`-P`) (SSRP**/TDS)	(# of Instances + 1) x (# of Hosts)	(# of Instances + 1) x (# of Hosts)
	Pre-Login*** (Default Instance)	# of Hosts	# of Hosts
	Brute Force (`-b`) (TDS Only)	(# of Ports) x (# of Hosts)	(# of Ports) x (# of Hosts)

Thank you!

http://about.me/nbrito