



## Penetration Test Report

---

*Anonymised*

*15/11/2011*

**CONFIDENTIAL**

**Non-Disclosure Statement:** All information obtained during a ProCheckUp assessment about our customer's systems and assets including, but not limited to, its procedures and systems, is deemed privileged information and not for public dissemination. ProCheckUp Ltd pledge their commitment that this information will remain strictly confidential. This information will not be disclosed or discussed to any third party without the express written consent of the customer. ProCheckUp Ltd is fully committed to maintaining the highest level of ethical standards in its business practice.

**Legal Notice:** It is impossible to test for 100% security. This report does not constitute and should not be construed as a guarantee of the target's security.

ID	Author	Date	Account Manager
AN151111	Security Consultant	15/11/2011	Account Manager

Table of Contents

Non-Disclosure Statement & Legal Notice ..... 5
Non-Disclosure Statement..... 5
Legal Notice ..... 5
How to use this report ..... 6
Management Summary ..... 6
Summary of Findings ..... 6
Test Results..... 6
Severity Scale ..... 6
Document Control ..... 7
1 Management Summary ..... 9
2 Technical Results ..... 11
2.1 Reconnaissance Phase ..... 11
2.1.2 Network sniffing ..... 11
2.1.3 NetBIOS Name Service & Session Enumeration ..... 12
2.1.5 Service Discovery ..... 14
2.2 Exploitation Phase..... 15
2.2.1 Network Devices ..... 15
2.2.2 Windows Vulnerabilities ..... 15
2.2.3 Password Policy ..... 17
2.2.4 Remote Control Services ..... 18
2.2.5 Linux Vulnerabilities..... 19
2.3 Overview of Findings..... 20
3. Test Results..... 21
3.1. Network Devices - EthernetBoard OkiLAN 8100e ..... 21
10.10.10.1 ..... 21
10.10.10.2 ..... 21
10.10.10.3 ..... 21
●●●● VxWorks Debug Service Enabled ..... 21
3.2. Windows infrastructure..... 22
3.2.1. Domain Controllers – Domain ‘Anonymised1’ – Windows 2008 Server R2 ..... 22
10.10.10.70..... 22
10.10.10.71 ..... 22
●●●● Lack of password complexity requirements ..... 22
●●●● Domain Administrator password cracked..... 23
●●●● LAN Manager (LanMan) supported..... 24
●●●● NetBIOS leaks sensitive information through the use of null sessions ..... 25
3.2.2. Additional Servers – Domain ‘Anonymised1’ – Windows 2003 Server R2 ..... 26
10.10.10.47 ..... 26
10.10.10.49 ..... 26

10.10.10.50.....	26
10.10.10.51.....	26
●●●●● Remote Desktop Protocol Server Private Key Disclosure Vulnerability.....	26
10.10.10.210.....	27
10.10.10.143.....	27
●●●●● Local Administrator password cracked.....	27
10.10.10.110.....	28
10.10.10.111.....	28
●●●●● Apache Tomcat Manager Common Administrative Credentials.....	28
10.10.10.15.....	30
10.10.10.16.....	30
10.10.10.19.....	30
●●●●● CA BrightStor ARCserve Backup for Windows Remote Buffer Overflow.....	30
10.10.10.11.....	31
10.10.10.94.....	31
●●●●● Microsoft Windows SMB Shares Unprivileged Access.....	31
10.10.10.79 – Windows 2000 Server.....	32
●●●●● Microsoft IIS Remote Command Execution.....	32
10.10.10.201 – Windows 2003 Server R2.....	33
●●●●● Web server supports unnecessary methods.....	33
10.10.10.9 – Windows 2003 Server R2.....	34
●●●●● Passwords stored in clear-text.....	34
10.10.10.57 – Windows 2003 Server R2.....	35
●●●●● Symantec Backup Exec Authentication Bypass.....	35
3.3. Linux Servers – Ubuntu 11.04.....	36
10.10.10.77.....	36
●●●●● Sensitive files found.....	36
3.4. Remote Control Services – VNC, Dameware Mini Remote control, Remote Desktop.....	38
10.10.10.78 – VNC 4.1.....	38
10.10.10.215 - Dameware Mini Remote control.....	38
10.10.10.127 - Remote Desktop.....	38
10.10.10.90 – VNC 4.1.....	38
●●●●● Password reuse.....	38
●●●●● VNC Authentication Bypass.....	39
3.4. Appendix –Port Scans.....	40
3.4.1. Network Devices.....	40
10.10.10.1.....	40
10.10.10.2.....	40
10.10.10.3.....	40
3.4.2. Windows infrastructure - Domain Controllers - Domain 'Anonymised1'.....	41

10.10.10.70 .....	41
10.10.10.71 .....	42
3.4.3. Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ .....	43
10.10.10.47 .....	43
10.10.10.49 .....	44
10.10.10.50 .....	45
10.10.10.51 .....	46
10.10.10.210 .....	47
10.10.10.143 .....	48
10.10.10.110 .....	49
10.10.10.111 .....	50
10.10.10.15 .....	51
10.10.10.16 .....	52
10.10.10.19 .....	53
10.10.10.11 .....	54
10.10.10.94 .....	55
10.10.10.79 .....	56
10.10.10.201 .....	57
10.10.10.9 .....	58
10.10.10.57 .....	59
3.4.4. Linux Servers – Ubuntu 11.04 .....	60
10.10.10.77 .....	60
3.4.5. Apple Workstations – Mac OSX 10.7.2 (Lion) .....	61
10.10.10.78 .....	61
10.10.10.90 .....	61
3.4.6. Windows Workstations – Windows XP Professional Service Pack 3 .....	62
10.10.10.215 .....	62
10.10.10.127 .....	62

## Non-Disclosure Statement & Legal Notice

### Non-Disclosure Statement

This report has been made for *Anonymised*. All information obtained during a ProCheckUp assessment about our customer's systems and assets including (but not limited to) its procedures and systems, is deemed privileged information and not for public dissemination. ProCheckUp Ltd severally pledge their commitment that this information will remain strictly confidential. This information will not be disclosed or discussed to any third party without the express written consent of the customer. ProCheckUp Ltd is fully committed to maintaining the highest level of ethical standards in its business practice.

### Legal Notice

It is impossible to test an Internet connection for 100% security. This report does not constitute and should not be construed as a guarantee of the target's security.

## How to use this report

### Management Summary

The management summary highlights the main findings from the report and provides an indication as to the level of security of the target environment.

### Summary of Findings

This section shows a summary of the issues found on each target accompanied by a bar chart to demonstrate the number of vulnerabilities found on each target and their severity.

The vulnerabilities are counted by their type and not instances of the same vulnerability. For example, Cross-Site Scripting is classed as a single vulnerability even though multiple pages may have the same issue.

### Test Results

This section lists the open ports found for each target and contains the low to serious vulnerabilities.

Each vulnerability includes an indication of its impact, a description, results and how it can be resolved.

Whenever possible, an exploit for the identified vulnerability will be supplied.

### Severity Scale

Vulnerabilities are supplied with ratings next to them giving an indication of their severity and are rated on a scale of one to five using the icons below.

The rating that is applied to a vulnerability is based on the information gathered during the testing and the threat to that specific environment under review.

A rating of five means that the vulnerability will enable an attacker to break into the server, a rating of one therefore is of low severity, possibly disclosing information that cannot be hidden. (e.g. port 25 on a mail server.)

A more detailed description containing examples of the ratings can be seen below:

Severity	Description
	Level 1 vulnerabilities expose information such as open ports.
	Level 2 vulnerabilities expose a small amount of sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks against a host.
	Level 3 vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level of vulnerability could result in potential misuse of the host by intruders. Examples of Level 3 vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules or security mechanisms and unauthorized use of services such as mail relaying.
	Level 4 vulnerabilities provide intruders with remote user access, but not remote administrator or root user capabilities. Level 4 vulnerabilities provide hackers partial access to file-systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information qualify as Level 4 vulnerabilities.
	Level 5 vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers full file-system read and write capabilities, and remote execution of commands as a root or administrator user. The presence of backdoors and Trojans qualify as Level 5 vulnerabilities.

## Document Control

Date	Action	Author
23 <sup>rd</sup> November 2011	Report Generated	Security Consultant A
24 <sup>th</sup> November 2011	Technical QA	Security Consultant B
25 <sup>th</sup> November 2011	Report QA	Account Manager

*This Page Intentionally Left Blank*



# 1 Management Summary

*Anonymised* is a leading UK company with offices in *Anonymised*. *Anonymised* employs approximately 150 people and provides corporate, commercial, public sector and private clients throughout the UK and abroad with a full range of *anonymised* services.

Between the 15th and 18th November 2011 a security assessment was performed by ProCheckUp against computer systems belonging to *Anonymised* across a number of locations. The testing was performed from *Anonymised* and was targeted against numerous network components within the *Anonymised's* environment.

The scope of the test was to highlight vulnerabilities that could be utilised by a malicious user with no privileges to subvert the environment, escalate privileges and gain access to sensitive information.

Overall the security of the network was found to be **low** and the ProCheckUp test highlighted a number of vulnerabilities of varying levels.

The testing process was conducted in phases to simulate different attacks and attackers that could potentially pose a threat to the *Anonymised's* business and network. All testing was conducted in line with ProCheckUp's penetration testing methodology.

The objective of the testing was to analyse the list of systems provided, enumerate and exploit security vulnerabilities. Both the scope and impact of these vulnerabilities were identified and the findings are presented within the Technical Results (Section 2, page 11) and the Test Results (Section 3, page 21) of this report. The exploitation of security vulnerabilities by an attacker can expose an organisation to a number of IT related risks. A summary of those exposed by the systems that were tested are summarised below: -

- It was discovered that the **confidentiality** of all data stored within the *Anonymised's* environment could be compromised by an internal attack. Such an attack would require no more than RJ45 network access.
- The **integrity** of data stored within numerous databases and host systems could also be compromised. This was initially possible through successful access to the systems which was gained via a compromised administrative account. In addition, the integrity of stored data could be compromised through the exploitation of missing security patches.
- The level of access obtained could be used to shutdown systems, delete data and perform other actions that could seriously affect data **availability**. Additionally, large parts of the network infrastructure were compromised and many of the vulnerabilities identified could be used to seriously affect network availability.

Testing revealed that a number of significant security vulnerabilities were present in *Anonymised's* systems. Exploitation of these vulnerabilities by an attacker would allow highly privileged access to be gained to a large number of business critical applications including document stores, financial systems and critical administrative hosts. As such, the organisation is currently exposed to an excessive level of IT related risk and could face fiscal loss as well as potentially being in breach of the Data Protection Act 1998.

The vulnerabilities were present due to a number of weaknesses in the configuration of computer systems. The types of vulnerabilities identified during testing are not unique to *Anonymised* and can be addressed. Rather than simply identifying each instance of a vulnerability and rectifying that instance, it is important that a policy is put in place to ensure that any future system builds do not also suffer from similar weaknesses. In particular it is recommended that policies are put in place with regards to the following:

- **Password Policy** – Passwords for several different systems and technologies were found to not conform to a strong policy. Most critically, some members of the highly privileged “Domain Administrators” Windows group were found to have weak passwords, including passwords set to “password” and passwords which were the same as the usernames. This would allow an attacker to gain full administrative access to all Windows systems and so allow them to compromise all of *Anonymised’s* critical data. A number of weak and default passwords were also identified across other technologies, including:
  - Microsoft Windows 2000 / 2003 / 2008 Server systems
  - Microsoft Windows XP Professional
  - Ubuntu Linux Systems
  - OSX Lion Systems
- **Security Patching** – A number of systems had not been patched with all the relevant security updates. The systems could therefore be compromised using publicly available exploit code which could result in highly privileged unauthorised access. Most critically, domain controllers were found to be missing a significant patch that would allow an attacker to compromise them and subsequently the entire domain. The Windows desktops tested also appeared to be generally well patched; however, the level of patching did vary widely and this could present an attacker with opportunities to compromise well patched systems on the network through trust relationships.
- **Lack of password complexity requirements** – It was found that *Anonymised’s* domain controllers allow the user to choose or change to insecure passwords, suggesting that there is no password complexity policy being enforced. Additionally, it was also found that users are allowed to have the same password as their username, which is not in line with good security practice and should be corrected as a matter of urgency.
- **Password reuse** - The same passwords are being shared by different remote control services within *Anonymised’s* network, allowing a malicious user to logically jump from system to system bypassing the filtering policies implemented once knowledge of *Anonymised’s* network topology has been gathered. This also should be corrected as a matter of urgency.
- **Exposed services** - Policies on which services are permitted to run on the network should be defined along with any additional security measures that should be implemented with their use.
- **Host Configuration Security (Systems hardening)** – A standard base operating system security build is fundamental in ensuring that a defence in depth approach is adopted throughout a network infrastructure. A verified hardened build for all desktops, servers, web servers and all relevant systems is an important part of any defence against many of the common vulnerabilities exploited during the attack phase of the penetration test. These standard builds should also include all the security configuration settings for web servers and database servers. A suitable system hardening process should be defined and documented. All future system builds should follow this process.

In summary, the security of the internal networks was not of an appropriate standard and enabled unauthorised access to be gained to a large number of critical systems and the data held within them. Although good security practice was evident in many of the tested areas, it is nevertheless recommended that the issues highlighted in this report are addressed in a timely manner to ensure that the overall level of security supported by the organisation’s systems is maintained at an appropriate level.

## 2 Technical Results

This section covers the two main phases of the engagement; the reconnaissance and exploitation phases. These phases are further separated into the testing techniques used and the technologies that were discovered which disclosed valuable information or lead to a full compromise of the host.

### 2.1 Reconnaissance Phase

On connecting the test equipment to the network, a DHCP service was available to gain IP addresses. This revealed information that allowed potential critical targets to be discovered. The DHCP server and other host and network information can be seen in the output below:-

```
[itsme@gh0st ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr AA:BB:CC:00:00:00
          inet addr:10.10.10.222  Bcast:10.10.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8403 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2394 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:869574 (849.1 KiB)  TX bytes:212937 (207.9 KiB)
```

In an Active Directory environment, hosts that provide the DNS service, typically act as domain controllers. Therefore, host information such as this could be invaluable to an attacker:

```
[itsme@gh0st ~]# cat /etc/resolv.conf | tee domain-check
search anonymised.local.co.uk
nameserver 10.10.10.71
nameserver 10.10.10.72
```

The following techniques and discoveries enabled information to be gathered and used for the attack phase:-

#### 2.1.2 Network sniffing

Network sniffing can be accomplished with the use of a technique called ARP poisoning. This technique corrupts the ARP tables of the hosts targeted for sniffing so that network traffic is relayed through the attacker's machine. Effective sniffing was achieved on the network by targeting two hosts considered likely to generate a fair amount of traffic containing information regarding other networks and potentially user credentials. The two targets were a workstation with a user logged on (this was discovered using NetBIOS) and one of the local backup switches (10.10.10.3).

Longer periods of sniffing and relocating to various points in the network could potentially allow the disclosure of account credentials and sensitive information. Leakage of such information is accomplished if the infrastructure is using clear text protocols. The use of clear text protocols to transmit sensitive data was widespread on the network.

Several techniques can prevent the use of ARP poisoning. An effective technique is to use static ARP entries. However, the creation and maintenance of all the necessary tables would cause a large administration overhead. Additionally, 802.1x Authentication on the network can also be used as part of a mitigation strategy. Software can be used to monitor ARP poisoning attacks such as 'Cain' for Windows systems or 'ARPWatch' for \*nix like systems. 'ARPWatch' builds a table of ARP tables and monitors them for changes (known as 'flip-flops'). However, this is a detection method only and does not prevent the attack from occurring.

### 2.1.3 NetBIOS Name Service & Session Enumeration

The NetBIOS Name Service (NBNS) has traditionally served as the distributed naming system for Microsoft Windows-based networks. In order to discover specific information regarding the Windows domains and systems in use, a number of NetBIOS sweeps were also conducted. This led to the discovery of the core *Anonymised's* Windows domain controllers and other key systems. Below is an example of this output showing the NetBIOS names and IP addresses for the domain controllers discovered during testing:

```
Get list of DCs in domain 'local.XXXXXX.co.uk' from '\\Dc2.local.XXXXXXXXX.co.uk '.
```

```
Dc1.local.XXXXXXXXX.co.uk [PDC] [DS] Site: XXXXXXXXXXX => 10.10.10.71
Dc2.local.XXXXXXXXX.co.uk [DS] Site: XXXXXXXXXXX => 10.10.10.72
```

The command completed successfully

The domain controllers could be identified using the Windows `'net view /domain:Anonymised'` command. An extract of the machines enumerated in the *Anonymised* domain is shown below:-

Server Name	Remark
\\XXXXAV	
\\XXXXXXXXBACKUP	
\\XXXXXXXXFINANCE	
\\XXXXXXXXXX	DC01
\\XXXXXXXXXX	DC02
\\XXXXXIIIS	Development IIS Server
\\XXXXXXXXEX01	
\\XXXXXXXXEX04	
\\XXXXXXXX-S1	
\\XXXXXXXX-S2	
\\XXXXXXX	
\\XXXXXMS02	
\\XXXXXMS01	
\\XXXXFAX01	
\\XXXXDFS01	Development File Server
\\XXXXFP05	
\\XXXXMS01	

Once these Microsoft systems had been located it was possible to recover information from them using Null sessions. The domain controllers could be queried for all domain user accounts and the password policy by using NULL sessions. These are anonymous connections to the default "IPC\$" share which by default enable access to a large amount of system information including usernames, group memberships and security policies such as the password policy. The password policy reveals to an attacker valuable information such as the number of unsuccessful attempts allowed before the user account was locked out, whether password complexity was enabled and other useful information.

```
Minimum password length: 6
Password history length: 5
Maximum password age (days): 30
Password must meet complexity requirements: Disabled
Minimum password age (days): 2
Forced logoff time (seconds): Not set
Locked account time (seconds): 3600
Time between failed logon (seconds): 1800
Number of invalid logon before locked out (seconds): 5
```

The information gathered by these attack vectors is illustrated in Section 3.2.1. Up to 2317 user accounts were discovered with the use of various tools such as 'GetAcct', an extract of these accounts is listed below:-

User Name
Sales
streamline
zurichteam
anne.harlow
Maggie.White
5283
carmen.thompson
5347
2840
6294
1128
5238
profund2
paulr
benh
SmallP
QUADRA_1
ChristineC
tasks
RiskData
5420
8029
5323
5244

It is recommended that NULL sessions be restricted to prevent this type of enumeration. NULL sessions can be also disabled by either setting the relevant registry key or setting the policy if it is not a business requirement. How these settings are changed depends upon the operating system in use.

## 2.1.5 Service Discovery

With information gleaned from the previous steps, port scanning was conducted to locate key services running on the known live hosts and also to locate all services running on critical hosts, such as the domain controllers. Below is outcome of the TCP port scan of the backup domain controller 10.10.10.71:

Interesting TCP ports on 10.10.10.70:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2008 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1030/tcp	open	msrpc	Microsoft Windows RPC
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	
3269/tcp	open	tcpwrapped	(unavailable)

This enabled key services across the network to be targeted for attack and key systems to be assessed for weak services that could lead to their compromise.

## 2.2 Exploitation Phase

The exploitation process was conducted in phases to simulate different attacks and attackers that could potentially pose a threat to the *Anonymised* business and network. During the exploitation phases a variety of techniques were employed to identify the services operating on different hosts and network devices. Port scanning, vulnerability scanning and the use of various tools and techniques were carried out in order to quickly identify running services and their potential exposed vulnerabilities. Once this was accomplished an exploitation of the identified vulnerabilities was then attempted.

This section contains separate discussions of the individual services found to offer an attacker the ability to compromise a host, or where it is considered that their security should be reviewed and possibly addressed.

### 2.2.1 Network Devices

VxWorks WDB Debug Agent was found to be enabled and running on *Anonymised's* network switches. Using this service, it was possible to read any memory zone which revealed hard-coded administration credentials. An attacker can use this flaw to take complete control of the affected device. The screenshots on page 21 show how it was possible to perform a memory dump on host 10.10.10.3. Such memory dump was then read by the attacker using a hex editor in a later stage of the test, revealing such user credentials.

### 2.2.2 Windows Vulnerabilities

The patching level across the *Anonymised's* Windows infrastructure was varied across the different hosts and their different operating systems (OS).

The Windows hosts tested were a representative sample of hosts seen across the *Anonymised* environment and were found to have varying patch levels. It was possible to remotely compromise a number of the Windows servers seen within the *Anonymised's* network. This was possible due to missing Microsoft security patches that had not been applied to the development/production servers. The contained vulnerabilities have been in existence for some time, and one from the year 2000. A representative sample of the nature and severity of the vulnerabilities seen across the Windows hosts reviewed is given below:-

- 1) Domain Controllers **10.0.2.10** and **10.0.2.11** were seen to allow a weak password policy which did not enforce the use of strong passwords.
- 2) It was found that legacy authentication is still being used on the 'Anonymised1' domain to store user passwords that are less than 15 characters in size. This is probably allowed due to legacy/backwards compatibility conditions, however there are a number of security flaws associated with this method that are due to weaknesses in its implementation and lead to the compromise of the company's Windows infrastructure. These weaknesses make it easier to perform a successful brute force attack, which does not require a degree of expertise in penetration testing methodologies.
- 3) The NetBIOS protocol, which is a native Windows protocol, provides attackers with sensitive information about the *Anonymised's* domain without requiring authentication. Usernames, Domains and shared resources enumeration is possible for the company's domain using such NetBIOS NULL sessions.
- 4) The remote version of Remote Desktop Protocol Server (Terminal Service) on the company's domain is vulnerable to a Man-in-the-middle attack. An attacker may cause the client to connect to a server under their control and send the client a public key to which they possess the private key and therefore, decrypt communications between client and server and obtain sensitive information. It was possible to retrieve Domain administration credentials using hacking tools available on the Internet.

- 5) It is possible to gain access to the Manager Web application for the remote Tomcat server using a known set of credentials. A remote attacker can leverage this issue to install a malicious application on the affected server and run code with Tomcat's privileges as SYSTEM, which is the highest non-human user on Windows systems. Allowing default credentials represent a high risk for *Anonymised*, and it should be resolved without delay.
- 6) Several servers are running a backup solution called BrightStor ARCserve for Windows. The remote version of this software has multiple buffer overflow vulnerabilities. The consultant, by sending a specially crafted packet, could remotely execute administration commands on the remote host.
- 7) 10.10.10.79 was found to be vulnerable to a vulnerability dated from the year 2000, widely known as Microsoft IIS Remote Command Execution. The consultant also could execute arbitrary code on the remote host without being authenticated against the system.
- 8) Hosts 10.10.10.9 and 10.10.10.77 were found to be storing passwords in clear-text. These passwords were used to get access to other servers/workstations.
- 9) Host 10.10.10.57 is running a version of Symantec Backup Exec which is prone to a vulnerability that allows an attacker to bypass authentication and gain unauthorized access to the affected system/application. Attackers with authorized network access can exploit this issue to bypass the logon process.

All Windows hosts can be automatically patched using a centralised patching solution. When considering the schedule for effective security patching, Windows servers should be treated differently to Windows workstations. Downtime and scheduled outage should be co-ordinated with the Change Control function within the organisation to ensure patching can be performed regularly and within strictly controlled business parameters.

In general varied patching levels and security profiles were observed across the Windows servers within the *Anonymised* environment. During discussion this was attributed to an inability to effectively schedule downtime in agreement with the business for the hosts to be patched. The increased risk of compromise by missing security patches should be factored into any business decision to postpone patching of systems within the *Anonymised* environment. Effective patching across the *Anonymised* environment is vital to maintaining the security of *Anonymised's* data and should be resourced appropriately.



### 2.2.3 Password Policy

The password policy configured for the domain was found to be weak. After analysis of the password policy in the Active Directory which was obtained previously, it was evident that the current policy does not enforce any password complexity and enforces a minimum of six characters.

Once the domain users were enumerated with techniques discussed, dictionary attacks were launched taking into consideration the account lockout policy. Consequently a large number of weak passwords were recovered, some of which were in the "Domain Administrators" group and so allowed full administrative access to be gained over the entire domain. It should be noted that the user account "db2admin" from the "Domain Administrators" group was found to have its password set as "db2admin". With a high privilege access to the domain, this enabled all the password hashes for the *Anonymised* domain to be obtained. Rainbow tables were then used to enable the passwords to be cracked in less time than a standard brute force attack. Rainbow tables greatly reduce the time required to crack a number of hashing algorithms, through a time and memory trade off principle. More information can be found at:

[http://en.wikipedia.org/wiki/Rainbow\\_table](http://en.wikipedia.org/wiki/Rainbow_table)

The password hashes that were obtained indicated that the domain controller supported LanMan (LM) encryption. LanMan (LM) has a number of cryptographic weaknesses and flaws. This includes the splitting of the password into two 7 character blocks and the hashing of each of these blocks separately. LM hashes are sometimes supported where compatibility with legacy systems is a requirement; however, NTLM hashes are much stronger and should always be used where compatibility requirements allow. It is recommended that the use of LM hashes should be restricted with NTLMv2 being supported as the only authentication mechanism on all Microsoft Windows systems.

In addition, a strong password policy should be enforced on all network devices and architectures across the *Anonymised's* infrastructure. During testing, it was found that network devices and databases were using either default or very weak passwords.

A password policy should be enforced on all types of accounts, especially privileged accounts such as administrative accounts and users should be educated on choosing secure passwords and safeguarding them.

The following is an example of a secure password policy:

- minimum length requirement of 8 characters
- upper and lower case characters must be used
- at least 2 digits should be part of the password

## 2.2.4 Remote Control Services

Various software packages were found to be used by *Anonymised* network. The remote control software in use includes:-

- Virtual Network Computing (VNC)
- Terminal Services (RDP)
- Dameware Mini Remote Control

VNC appeared to be the software used by the *Anonymised*'s IT department to remotely support workstations. During testing, it was found that the installed version of VNC was susceptible to authentication-bypass vulnerability, due to a flaw in the authentication process. As a result it was possible to connect remotely to a number of hosts of the *Anonymised*'s infrastructure. In addition to that, it was found that the hosts which were operating VNC were protected with a password which was reused on all the VNC servers and that it was previously retrieved during the test.

Terminal services were operating on the majority of Windows servers. This service was available on critical hosts including domain controllers. Access to Terminal Services was not restricted to administrative IP addresses only, and therefore, any host connected to the network would be allowed to establish a RDP connection. As Terminal Services are used for administration of critical hosts, it is recommended that this service be reviewed to ensure that remote access is actually required, or whether administrative functions could be controlled from the local host. Should remote access be required, an Access Control List (ACL) should be applied specifying those hosts which are authorised to access the service. Access to Terminal Services could also be limited by user accounts. Implementing this control in combination with the ACL (recommended above) would further secure access to hosts.

### 2.2.5 Linux Vulnerabilities

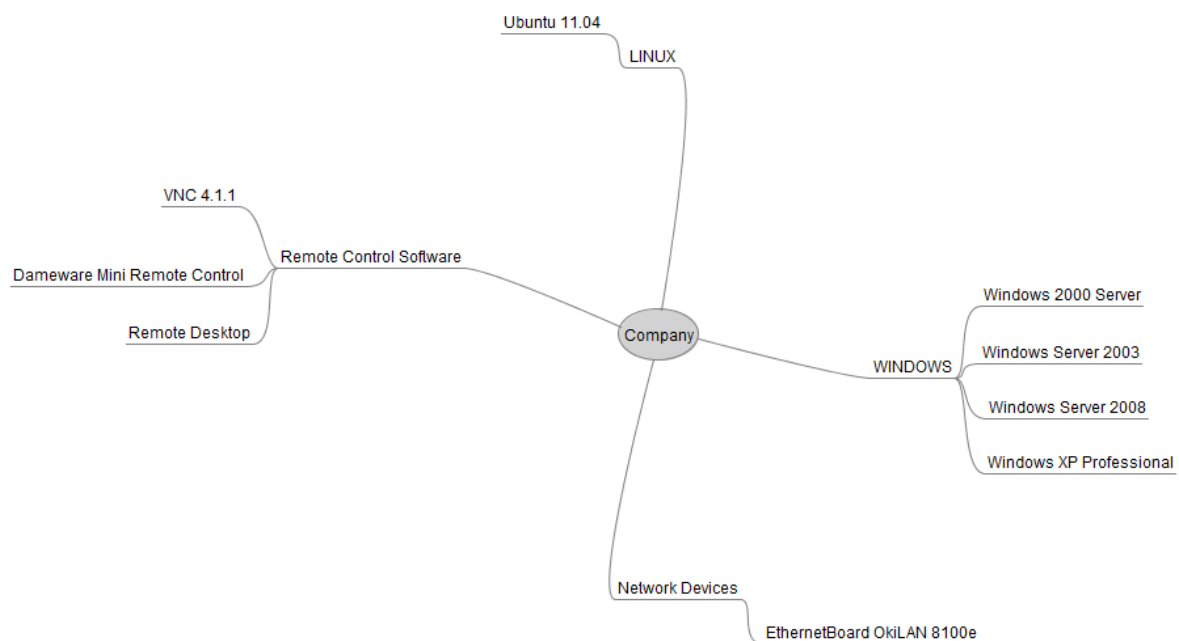
The Ubuntu Linux server 10.10.10.77 was found to be publicly exposing sensitive information such as usernames and password hashes, which were trivially retrieved and cracked. From this machine and as the user with highest privilege “root” it was possible to get access to the production network, by connecting to host “Spike”. Access was then granted to such network without any password authentication. Spike’s super-user access was not prompted to enter a password, as such access was granted via a public/private key scheme found in one of the publicly available directories withing the Ubuntu Linux host 10.10.10.77. Please note that Anonymised’s production network was out of scope, and this is only explained to highlight that an attacker would be able to compromise the whole company’s internal infrastructure as well as its Internet presence as a consequence of this vulnerability.

## 2.3 Overview of Findings

Total control of the entire network was achieved due to a weak password policy implemented on the *Anonymised's* domain, to password reuse and to missing security patches on several servers and workstations. These vulnerabilities allowed retrieving the complete password files for the heterogeneous network which were cracked during the test, granting administrative access to most machines within the network.

With Domain Administrator and 'super-user' 'root' password hashes obtained, it means that any machine within the network is trivially exploitable. User details, passwords and files could be erased or altered; impersonation of other users on the network would also be possible. It should be noted that administrative level access essentially means that any machine which is part of the network is vulnerable to an immediate attack.

Figure 1: Conceptual diagram of *Anonymised's* internal infrastructure.



In summary, a number of security vulnerabilities were identified in the infrastructure owned and operated by *Anonymised*. These expose the company to an excessively high risk level. It is strongly recommended that the issues highlighted in this report be addressed as soon as possible to ensure that security controls are maintained at an appropriate level.

It is recommended that hosts are built to a secure and homogenous configuration standard. This should involve a secure configuration document being created for each system or platform in use. These documents should provide steps and guidelines in order to secure such hosts. This will ensure they hosts are in optimum state before going into a production environment. It is recommended that *Anonymised's* infrastructure affected by these vulnerabilities should have the necessary changes applied as outlined in this report.

### 3. Test Results

#### 3.1. Network Devices - EthernetBoard OkiLAN 8100e

10.10.10.1

10.10.10.2

10.10.10.3

●●●●● **VxWorks Debug Service Enabled**

<b>VxWorks WDB 17185</b>  <b>(UDP)</b>	<p>A VxWorks WDB Debug Agent is running on this host. Using this service, it is possible to read or write any memory zone or execute arbitrary code on the host. An attacker can use this flaw to take complete control of the affected device.</p> <p><b>Results</b></p> <p>The following screenshots show how it was possible to perform a memory dump on host 10.10.10.3. Such memory dump was then read by the attacker using a hex editor in a later stage of the test, revealing sensitive information such as user credentials.</p> <p>Example 1: Memory dump of host 10.10.10.3 to the attacker’s machine:</p> <pre style="background-color: #000; color: #0f0; padding: 5px;"> [*] [ 31 % ] Downloaded 0x0500d46c of 0x10000000 bytes [*] [ 31 % ] Downloaded 0x05013dd0 of 0x10000000 bytes [*] [ 31 % ] Downloaded 0x0501a734 of 0x10000000 bytes [*] [ 31 % ] Downloaded 0x05021098 of 0x10000000 bytes [*] [ 31 % ] Downloaded 0x050279fc of 0x10000000 bytes [*] [ 31 % ] Downloaded 0x0502e360 of 0x10000000 bytes [*] [ 31 % ] Downloaded 0x05034738 of 0x10000000 bytes [*] [ 31 % ] Downloaded 0x0503b09c of 0x10000000 bytes                     </pre> <p>Example 2: Hashed password found for user ‘marcus’:</p> <table border="1" style="width: 100%; border-collapse: collapse; font-family: monospace;"> <tr><td>038A4260</td><td>75 6C 74 4C 69 73 74 00 00 00 00 00 00 00 00 00 00 00 36</td><td>ultList.....6</td></tr> <tr><td>038A4270</td><td>6D 61 72 63 75 73 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>marcus.....</td></tr> <tr><td>038A4280</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>.....</td></tr> <tr><td>038A4290</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>.....</td></tr> <tr><td>038A42A0</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 62 34</td><td>.....5b4</td></tr> <tr><td>038A42B0</td><td>31 [REDACTED] 62</td><td>[REDACTED]</td></tr> <tr><td>038A42C0</td><td>39 [REDACTED] 00</td><td>[REDACTED]</td></tr> <tr><td>038A42D0</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>.....</td></tr> </table> <p>Example 3: Hashed password found for user ‘admin’:</p> <table border="1" style="width: 100%; border-collapse: collapse; font-family: monospace;"> <tr><td>038A3ED0</td><td>00 00 00 00 00 00 00 00 00 00 61 64 6D 69 6E 00 00 00 00</td><td>.....admin..</td></tr> <tr><td>038A3EE0</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>.....</td></tr> <tr><td>038A3EF0</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>.....</td></tr> <tr><td>038A3F00</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>.....</td></tr> <tr><td>038A3F10</td><td>00 00 00 00 00 00 65 65 62 63 34 63 33 63 33 62 31</td><td>.....eebc4c3c3b</td></tr> <tr><td>038A3F20</td><td>35 [REDACTED] 65</td><td>[REDACTED]</td></tr> <tr><td>038A3F30</td><td>63 [REDACTED] 00</td><td>[REDACTED]</td></tr> </table> <p><b>Recommendation</b></p> <p><b>Disable the debug agent running on port 17185/udp. Upgrade the device’s firmware to its latest version available. Contact the device's vendor for a patch.</b></p>	038A4260	75 6C 74 4C 69 73 74 00 00 00 00 00 00 00 00 00 00 00 36	ultList.....6	038A4270	6D 61 72 63 75 73 00 00 00 00 00 00 00 00 00 00 00 00 00	marcus.....	038A4280	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	038A4290	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	038A42A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 62 34	.....5b4	038A42B0	31 [REDACTED] 62	[REDACTED]	038A42C0	39 [REDACTED] 00	[REDACTED]	038A42D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	038A3ED0	00 00 00 00 00 00 00 00 00 00 61 64 6D 69 6E 00 00 00 00	.....admin..	038A3EE0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	038A3EF0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	038A3F00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	038A3F10	00 00 00 00 00 00 65 65 62 63 34 63 33 63 33 62 31	.....eebc4c3c3b	038A3F20	35 [REDACTED] 65	[REDACTED]	038A3F30	63 [REDACTED] 00	[REDACTED]
038A4260	75 6C 74 4C 69 73 74 00 00 00 00 00 00 00 00 00 00 00 36	ultList.....6																																												
038A4270	6D 61 72 63 75 73 00 00 00 00 00 00 00 00 00 00 00 00 00	marcus.....																																												
038A4280	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....																																												
038A4290	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....																																												
038A42A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 62 34	.....5b4																																												
038A42B0	31 [REDACTED] 62	[REDACTED]																																												
038A42C0	39 [REDACTED] 00	[REDACTED]																																												
038A42D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....																																												
038A3ED0	00 00 00 00 00 00 00 00 00 00 61 64 6D 69 6E 00 00 00 00	.....admin..																																												
038A3EE0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....																																												
038A3EF0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....																																												
038A3F00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....																																												
038A3F10	00 00 00 00 00 00 65 65 62 63 34 63 33 63 33 62 31	.....eebc4c3c3b																																												
038A3F20	35 [REDACTED] 65	[REDACTED]																																												
038A3F30	63 [REDACTED] 00	[REDACTED]																																												

## 3.2. Windows infrastructure

### 3.2.1. Domain Controllers – Domain ‘Anonymised1’ – Windows 2008 Server R2

10.10.10.70

10.10.10.71

#### ●●●●● Lack of password complexity requirements

Domain controllers allow the user to choose or change to insecure passwords, suggesting that there is no password complexity policy being enforced. Additionally, it was also found that the password for user ‘db2admin’ on domain controllers 10.10.10.70 and 10.10.10.71 was set to ‘db2admin’. Such user was found to belong to the domain administrators group. This is not in line with good security practise and should be corrected as a matter of urgency.

#### Results

On the domain ‘Anonymised1’, users can have insecure passwords such as:

- Passwords using sequential digits (i.e.: ‘Profund456’, ‘Planar64’, ‘Bristol123’)
- Passwords equal to username (i.e.: username db2admin, password ‘db2admin’)
- Repeated / predictable digits (i.e.: XXXXX2, XXXXX22, XXXXX23)
- Dictionary words (i.e.: quark, XXXXX, research, riskdata, password)

The following screenshot is an example of the passwords in use on the XXXXXX domain:

User Name	LM Password	<8	Password
Sales	P		P
streamline	P		P
zurichteam	P		P
	P		P
	P		P
5283	P		P
	P		P
5347	P		P
2840	P		P
6294	P		P
1128	P		P
5238	P		P
profund2	P	x	p
paulr	P		P
benh	P		P
SmallP	P		P
QUADRA_1	C	x	q
ChristineC	R		R
tasks	R		r
RiskData	R		r
5420	S		S
8029	S		S
5323	S		S
5244	S		S

#### Recommendation

**Enforce a secure password complexity on all types of accounts, especially privileged accounts such as administrative accounts.**

- **The following is an example of a secure password policy:**
- **Minimum length requirement of 8 characters**
- **Upper and lower case characters must be used**
- **At least 2 digits should be part of the password**

Domain Controllers – Domain ‘Anonymised1’ – Continued...

### ●●●●● Domain Administrator password cracked

Due to the fact that domain controllers allow the user to choose or change to insecure passwords as explained previously, the domain administrator password hash for the ‘Anonymised1’ domain was retrieved. It was possible to crack such hashes during the penetration test.

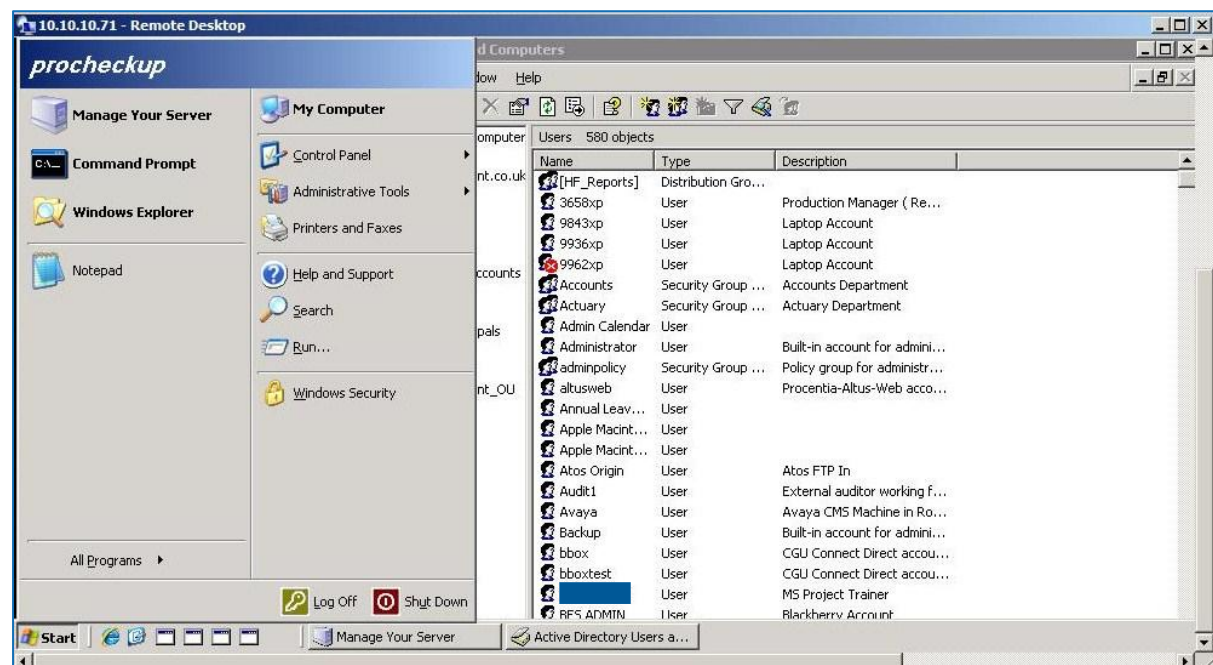
#### Results

Administrator password hash for the ‘Anonymised1’ domain:

Administrator:500:BOC60B894[REDACTED]520433290805C:::

Password in clear text: CO[REDACTED]-

Additionally, it was possible to create the domain administrator “procheckup” with unrestricted access on the ‘Anonymised1’ domain. The following screenshot shows access granted to Domain Controller XXXXXXXXXXXX (10.10.10.71) as such high privilege user:



#### Recommendation

**Change the administrator password to a hard-to-crack string. Ideally the password should be at least 8 characters long and combine lower and upper case characters, with digits or special symbols.**

Domain Controllers – Domain ‘Anonymised1’ – Continued...

**LAN Manager (LanMan) supported**

It was found that LAN Manager (LanMan) is being used on the ‘Anonymised1’ domain to store user passwords that are less than 15 characters in size. These passwords are hashed and are known as Lan Manager (LM) hashes. There are a number of security flaws associated with this method that are due to weaknesses in its implementation. This includes the splitting of the password into two 7 character blocks and the hashing of each of these blocks separately. In addition, all lower case letters are changed to upper case before the password is hashed. These weaknesses make it easier to perform a successful brute force attack.

To address the weaknesses in LM hashes, NT Lan Manager (NTLM) was created to provide a stronger hashing protocol. This was later superseded by NTLMv2 that uses a challenge-response approach.

**Results**

It was identified during testing that hosts on the ‘Anonymised1’ domain stored the password as LanMan hashes. The following is a proof of concept that shows the LM hashing implementation on domain ‘Anonymised1’:

	LanMan	NTLM	
7432:1610:5A426EEF123		C999F63D8DEE	::
6176:1613:0F2A4C49393		:243C01B6A3A	:::
9622:1617:B061F12E74C		935144EE4DF5	:
9891:1619:409324A96F1		A75D8781AC0A	:
9926:1624:760F09D5A4D		09B44B86F1B3	:
3509:1626:E52CAC67419		:8FD992DD15C	:::
9851:1628:81374D19DB8		:667007C56CE4	:
6294:1629:98799ADB78E		6:DCE78AFBF7D	:::
9945:1632:7922F507FFB		7A19DEC1D5F5	:
9843:1637:DDF80F3F2DE		9:B6F9033BC09	:
7596:1638:81867B7F883		34A0E0A11600A	:
9834:1641:F6BD219CD7C		:0E65D7677A6C	:::
9946:1642:E4833763F6C		C298C37CC433	:
3100:1643:347CC100217		5565F4F82A59	:
1228:1644:29420448F42		:E080D1E5A734	:
9947:1646:3E096D06EA8		0:4A854DED40C	:::
9963:1649:C171DD27411		2:6B4D07901AA	:::
1242:1652:DFA346DBFC9		:F3E6D6018018	:
9854:1653:43E15967E6E		ED2425958FC1	:
2860:1655:46FE10EA298		B2BEF1E76B6D	:
3640:1656:E52CAC67419		:64F12CDDAA8	:::
2480:1657:1D68628F493		:60DF4EFC966C	:
7273:1663:46086521173		A7EE8F86C8B0	:::

**Recommendation**

- It is recommended that the use of LM hashes be disabled.
- NTLMv2 should be used as the only authentication mechanism on all Microsoft Windows systems and should be enabled as default.
- This can be achieved by implementing the NoLMHash Policy using Group Policy.

See the knowledge base article <http://support.microsoft.com/?kbid=299656> for further information.



Domain Controllers – Domain ‘Anonymised1’ – Continued...

**NetBIOS leaks sensitive information through the use of null sessions**

**NetBIOS 137-139**  
(TCP & UDP)

NetBIOS provides attackers with sensitive information about your domain without requiring authentication. Usernames, Domains and shared resources enumeration is possible for the ‘Anonymised1’ domain using NetBIOS NULL sessions.

**Results**

Information such as User id, Name, Account type, Password Age, Privilege and SID was retrieved through the use of null sessions as shown on the following picture:

	A	B	C	D	F	G
1	User id	Name	Full name	Comment	Password age	Privilege
2	500	Administrator	Administrator	Built-in account for administering the computer/domain	2106days 6h 54m 57s	Administrator
16	1001	ServiceAccount	Service Account		2658days 6h 34m 6s	Administrator
23	1033	PFCUser	PFCUser	PATROL Account	4367days 17h 27m 58s	Administrator
31	1610	7432			24days 21h 32m 49s	Administrator
53	1656	3640			11days 3h 15m 9s	Administrator
63	1673	421			19days 2h 39m 13s	Administrator
73	1688	9911			0days 2h 45m 34s	Administrator
92	1718	3658			6days 2h 19m 6s	Administrator
125	1995	SunServices	SunServices	Account to run Sun Services	4280days 0h 32m 35s	Administrator
136	2031	Backup		Built-in account for administering the computer/domain	4241days 18h 10m 24s	Administrator
145	2052	PSLBatch	Profund Batch User	Profund Batch User (used by service to logon)	158days 22h 24m 37s	Administrator
221	2212	fns	fns		1153days 20h 9m 38s	Administrator

**Recommendation** Restrict anonymous connections/NULL sessions by setting the ‘RestrictAnonymous’ registry key accordingly to the ideal domain configuration  
[http://technet.microsoft.com/en-us/library/cc783167\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc783167(WS.10).aspx)

### 3.2.2. Additional Servers – Domain ‘Anonymised1’ – Windows 2003 Server R2

10.10.10.47

10.10.10.49

10.10.10.50

10.10.10.51

<span style="color: red;">●●●●</span> Remote Desktop Protocol Server Private Key Disclosure Vulnerability	
<p><b>RDP</b> <b>3389</b>  (TCP)</p>	<p>The remote version of Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man in the middle attack. An attacker may cause the client to connect to a server under their control and send the client a public key to which they possess the private key and therefore, decrypt communications between client and server and obtain sensitive information.</p> <p>During the test it was possible to intercept credentials of user ‘john.doe’, who appeared to be a domain administrator, leading to the compromise of the entire domain ‘Anonymised1’.</p> <p>3402 usernames with their associated password hashes were retrieved from domain controller 10.10.10.71.</p> <p><b>Results</b></p> <p>The following network packet was intercepted and decrypted by the ProCheckup consultant during the penetration test:</p> <ul style="list-style-type: none"> <li>- RDP client version: RDPv5</li> <li>- Downgrading client protocol version to RDPv4...</li> <li>- RDP client version: RDPv4</li> <li>- Client decrypted packet: 425 bytes total, 398 bytes decrypted</li> </ul> <pre> 0000 03 00 01 a9 02 f0 80 64 00 03 03 eb 70 81 9a 48 .....d....p..H 0010 00 00 00 00 f4 1a e1 f9 72 89 ef 1b 09 08 09 08 bb .....r..... [REDACTED] G.....A.n [REDACTED] .o.n.y.m.i.s.e.d [REDACTED] ...j.o.h.n.d.o.e [REDACTED] .X.X.X.X..M.O.1 [REDACTED] .X.X.X.X.X.X.X.X 0070 00 34 00 00 00 00 00 00 00 02 00 14 00 31 00 30 .4.....1.0                     </pre> <p><b>Recommendation</b></p> <p><b>Force the use of SSL as a transport layer for this service.</b></p> <p><a href="http://technet.microsoft.com/en-us/library/cc770833(WS.10).aspx">http://technet.microsoft.com/en-us/library/cc770833(WS.10).aspx</a>  <a href="http://www.securityfocus.com/bid/13818/">(http://www.securityfocus.com/bid/13818/)</a></p>

Additional Servers – Domain 'Anonymised1' – Continued...

10.10.10.210

10.10.10.143

### Local Administrator password cracked

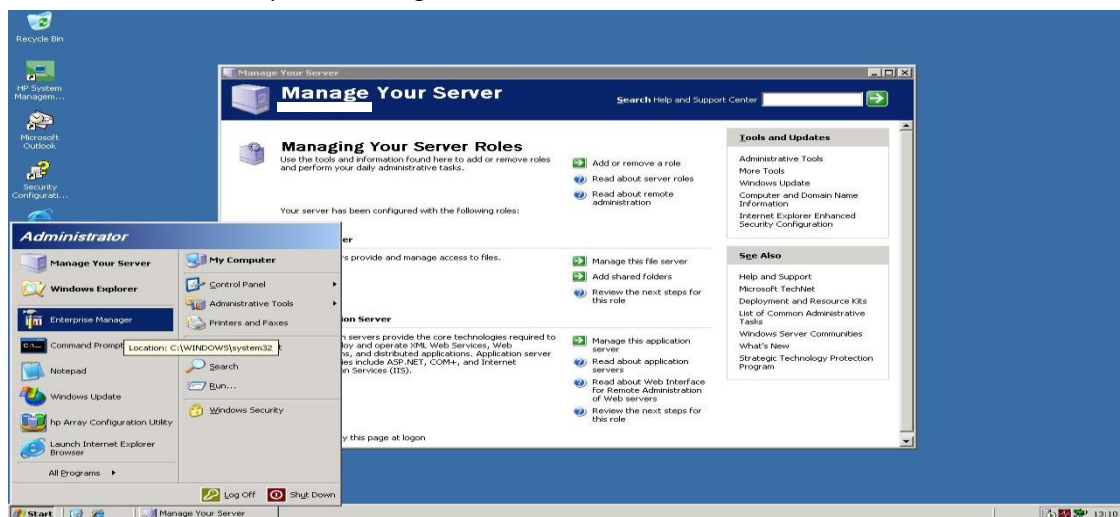
It was discovered that password for the local Administrator on servers 10.10.10.210 and 10.10.10.143 was set to 'letmein'. This is not in line with good security practise and should be resolved without delay.

#### Results

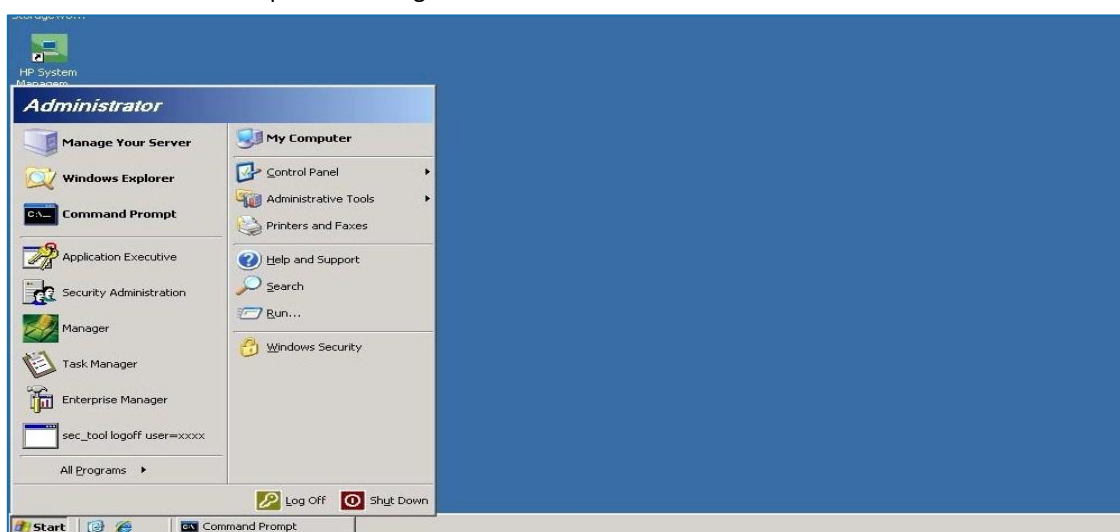
It was possible to log on as user Administrator on 10.10.10.210 and 10.10.10.143 within the servers' workgroup. The example below shows access granted to both machines from the consultant's machine through Terminal Services (RDP) using the following set of credentials:

- **Username:** Administrator
- **Password:** letmein

Example 1: Access granted to 10.10.10.210 as local Administrator



Example 2: Access granted to 10.10.10.143 as local Administrator



#### Recommendation

**Change the administrator password to a hard-to-crack string. Ideally the password should be at least 8 characters long and combine lower and upper case characters, with digits or special symbols.**

Additional Servers – Domain ‘Anonymised1’ – Continued...

10.10.10.110

10.10.10.111

●●●●● **Apache Tomcat Manager Common Administrative Credentials**

**HTTP 8080 (TCP)**

It is possible to gain access to the Manager web application for the remote Tomcat server using a known set of credentials. A remote attacker can leverage this issue to install a malicious application on the affected server and run code with Tomcat's privileges as SYSTEM on Windows systems. This is not in line with good security practice and should be resolved without delay.

**Results**

It is possible to log into the Tomcat Manager on the following URL :


`http://10.10.10.110:8080/manager/html`

The following credentials allowed access to the machine as highest privileged non-human user ‘SYSTEM’, as shown on the following screenshot :

Username: admin  
Password: <blank>

Tomcat Web Application Manager					
Message:		OK			
<b>Manager</b>					
<a href="#">List Applications</a>		<a href="#">HTML Manager Help</a>		<a href="#">Manager Help</a>	
<b>Applications</b>					
Path	Display Name	Running	Sessions	Commands	
/	Welcome to Tomcat	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a>	
/host-manager	Tomcat Manager Application	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a>	
/licenses	Leighton Licenses Application	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a>	
/manager	Tomcat Manager Application	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a>	
/tomcat-docs	Tomcat Documentation	true	1	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a>	

It was also possible to compromise the server at an OS level, which allowed the attacker to spawn a command prompt as user ‘SYSTEM’. The following screenshot exemplifies the attack:

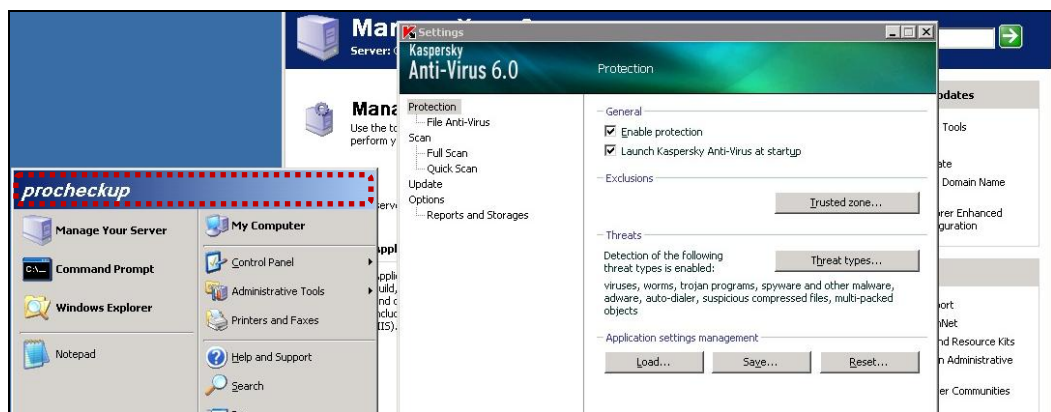


```

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Apache\Tomcat>whoami
whoami
nt authority\system
  
```

The user ‘Procheckup was then created as local Administrator, which allowed the attacker to log on to the machine through Terminal Server, as shown on the following screenshot:



It was also possible to obtain password hashes for an Enterprise Administrator of the 'Anonymised1' domain; however they were not cracked during the test due to time constraints. The password hashes retrieved are the following:

```

be001:60CC3B0 [REDACTED] F6B5B6:anonymised1
jonathan.test [REDACTED] 76DDB25B0C7D7B:anonymised1
c049:BF85EB00 [REDACTED] 8E952:anonymised1
user1:0C0C6A6 [REDACTED] 02340C:anonymised1
steve.test:33 [REDACTED] 64033D69095:anonymised1
be001:8D9A819 [REDACTED] 46A6BF:anonymised1
marcus:A6E980 [REDACTED] 903C804:anonymised1
marcus.test:B [REDACTED] F58B92263EC6:anonymised1
    
```

Please note that cracked password hash for user 'marcus' grants access to the 'Anonymised1' domain as Domain Administrator, as shown on the following 'net group' output:

```

Group name      Enterprise Admins
Comment          Designated administrators of the enterprise

Members

-----
_Template_GTS_Admin  Adminlstrat0r      marcus
    
```

**Recommendation**

**Disable the service if it is not being used. If the service is required, then edit the associated 'tomcat-users.xml' file and enforce a strong password policy on every set of credentials.**

Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.15**

**10.10.10.16**

**10.10.10.19**

<span style="color: red;">●●●●●</span> CA BrightStor ARCserve Backup for Windows Remote Buffer Overflow	
<b>Various Ports</b>	<p>Several servers are running BrightStor ARCserve for Windows. The remote version of this software has multiple buffer overflow vulnerabilities. An attacker, by sending a specially crafted packet, may be able to execute code on the remote host.</p> <p><b>Results</b></p> <p>The vulnerability affects the following network ports:</p> <p><b>DCE-RPC:</b> 6502-6504/tcp  <b>CA_License_Service:</b> 10203-10204/tcp  <b>Portmapper:</b> 111/tcp</p> <p><b>Proof of concept</b></p> <p>By sending a specially crafted packet to the RPC server on TCP port 6504, an unauthenticated remote attacker may be able to execute code on the remote host with SYSTEM privileges, as show in the example below:</p> <p><b>‘ipconfig’ command executed remotely on ‘PHOBOS’ (10.10.10.15):</b></p> <pre>Windows 2000 IP Configuration Host Name . . . . . : phobos Primary DNS Suffix . . . . . : local.anonymised.co.uk Node Type . . . . . : Hybrid IP Routing Enabled. . . . . : No WINS Proxy Enabled. . . . . : No DNS Suffix Search List. . . . . : local.anonymised.co.uk Ethernet adapter Local Area Connection: Connection-specific DNS Suffix . : Description . . . . . : HP NC7771 Gigabit Server Adapter Physical Address. . . . . : 00-10-18-10-05-2A DHCP Enabled. . . . . . . . . . : No IP Address. . . . . : 10.10.10.15 Subnet Mask . . . . . : 255.255.255.0 Default Gateway . . . . . . . . . . : 10.10.10.254 DNS Servers . . . . . : 10.10.10.72 10.10.10.71 Primary WINS Server . . . . . : 10.10.10.72 Secondary WINS Server . . . . . : 10.10.10.71</pre> <p><b>Recommendation</b></p> <p><b>Apply service pack 2 for Arcserve 11.5 or install the security patch.</b>  <a href="http://www.securityfocus.com/bid/21502">http://www.securityfocus.com/bid/21502</a></p>

Additional Servers – Domain 'Anonymised1' – Continued...

**10.10.10.11****10.10.10.94**

<span style="color: red;">●●●●○</span> Microsoft Windows SMB Shares Unprivileged Access	
<b>CIFS</b> <b>445</b>  <b>(TCP)</b>	<p>The remote machine has one or more Windows shares that can be accessed through the network with the given credentials. Depending on the share rights, it may allow an attacker to read/write confidential data.</p> <p><b>Results</b></p> <p>The following share can be accessed as non-existent user 'ijczjdac' on host 10.10.10.11:</p> <p><b>Ghost (readable,writable)</b></p> <pre> .. Admin cacls.txt Finance FULFILL GHOST.INI Ghost75.exe GHOSTERR.TXT GHOSTEXP.ENV GHOSTEXP.EXE Gilsans london newsid.exe ntfs.sys Ops Scheme SQLSecuritycheck.reg Travel           </pre> <p>The following share can be accessed as non-existent user 'qgeqrrbl' on host 10.10.10.94:</p> <p><b>Comms (readable,writable)</b></p> <pre> .. .DS_Store Branding (readable,writable) .. .com.apple.timemachine.supported .DS_Store Image library           </pre> <p><b>Recommendation</b></p> <p><b>To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.</b></p>

Additional Servers – Domain 'Anonymised1' – Continued...

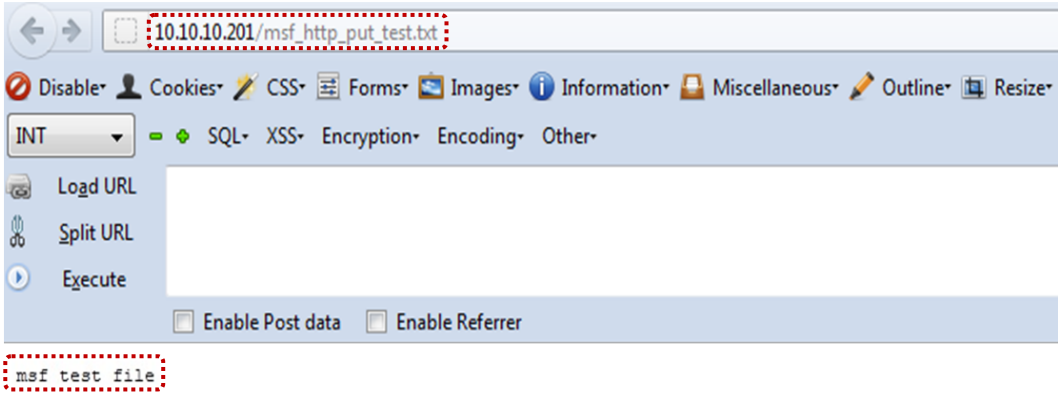
**10.10.10.79 – Windows 2000 Server**

Microsoft IIS Remote Command Execution	
<b>HTTP</b> <b>80</b>  <b>(TCP)</b>	<p>The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote host. An attacker does not need to be authenticated to exploit this flaw.</p> <p><b>Results</b></p> <p>Requesting the URL: <code>http:// 10.10.10.79/scripts/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\+/OG</code> produces the following server response:</p> <pre> <b>HTTP/1.1 200 OK</b> Server: Microsoft-IIS/5.0 Date: Mon, 22 Aug 2011 10:37:31 GMT X-Powered-By: ASP.NET Connection: close Content-Type: application/octet-stream <b>Volume in drive C is Local Disk Volume Serial Number is 18E0-09BD Directory of c:\</b> 17/03/2008 23:08 &lt;DIR&gt; Magnetic North 17/03/2008 21:35 &lt;DIR&gt; SQL2KSP4 25/05/2011 09:32 &lt;DIR&gt; Program Files 11/10/2004 17:00 &lt;DIR&gt; ASFRoot 11/11/2010 14:49 &lt;DIR&gt; backups 18/06/2010 12:30 &lt;DIR&gt; Documents and Settings 22/04/2008 10:15 &lt;DIR&gt; MNTMLOGS 17/03/2008 21:35 &lt;DIR&gt; mntemp 23/09/2010 17:04 &lt;DIR&gt; WINNT 02/03/2005 17:41 &lt;DIR&gt; upgrade 13/10/2006 02:12 &lt;DIR&gt; CPQSYSTEM 26/10/2005 12:26 &lt;DIR&gt; PerfLogs 27/09/2007 13:37 &lt;DIR&gt; pml support 11/07/2005 19:55 &lt;DIR&gt; compaq 11/10/2004 16:44 &lt;DIR&gt; Inetpub 30/09/2004 14:42 &lt;DIR&gt; hptapedrvrs 24/10/2009 10:54 &lt;DIR&gt; mnlogs 12/10/2006 20:58 &lt;DIR&gt; hp 08/07/2009 12:57 &lt;DIR&gt; log backup 17/03/2008 22:16 0 CaclsTempDirE.txt 21/02/2006 11:23 630,784 chatlnk.exe 18/07/2005 14:21 561,152 chatlink.exe 17/03/2008 22:16 84 CaclsTempDirB.txt 17/03/2008 22:16 83 CaclsProdGenAspNet.txt 17/03/2008 22:16 235,527 CaclsTempDirF.txt 17/03/2008 22:16 576 CaclsTempDirD.txt 17/03/2008 22:16 82 CaclsManGenAspNet.txt 17/03/2008 22:16 0 CaclsTempDirC.txt 13/10/2006 09:05 504,272 cp006349.exe 17/03/2008 22:16 0 CaclsTempDirA.txt 10/11/2004 17:44 158,494 javasetup.log 12/09/2006 14:28 202 keycode.txt 12/09/2006 12:32 2,009 Licence Issue.txt 17/03/2008 22:16 0 CaclsProdGenNetSvc.txt 20/08/2011 01:23 147,028 LOG.LOG 17/03/2008 22:16 0 CaclsManGenNetSvc.txt 15/11/2004 17:51 26,112 dnis.xls 17/03/2008 20:09 14,901 blueprint.xml 20/08/2011 00:57 0 dbg.tcpip.client.txt 17/03/2008 22:16 0 CaclsAlarmTPNetSvc.txt 31/10/2006 15:10 1,024 .rnd 17/03/2008 22:48 21,875 MNConfig20080317212351.12D8.log 27/09/2010 12:21 15,808,372 MNDebugLog.zip 14/09/2006 11:40 25,735,860 MNDebugLog_Optimise_09-14- 2006_114014.zip 17/03/2008 22:16 58 CaclsAlarmTPAspNet.txt 17/03/2008 22:16 52,729 mnsetup.log 17/11/2004 15:02 74,737 ethereal.log 05/06/2006 17:45 6,336,000 Alarms_tlog_200606050000.TRN 17/03/2008 19:34 28,442 MNConfig20080317184229.1198.log 61 File(s) 80,668,965 bytes 19 Dir(s) 59,414,880,256 bytes free </pre> <p><b>Recommendation</b></p> <p><b>Ensure that the latest security patches are applied to the server. Further information can be found on the following links:</b></p> <p><a href="http://www.microsoft.com/technet/security/bulletin/ms01-026.msp">http://www.microsoft.com/technet/security/bulletin/ms01-026.msp</a>  <a href="http://www.microsoft.com/technet/security/bulletin/ms01-044.msp">http://www.microsoft.com/technet/security/bulletin/ms01-044.msp</a></p>



Additional Servers – Domain 'Anonymised1' – Continued...

### 10.10.10.201 – Windows 2003 Server R2

Web server supports unnecessary methods	
<p><b>HTTP 80</b></p> <p><b>(TCP)</b></p>	<p>The HTTP methods 'PUT' and 'DELETE' were found to be enabled on the server under test. This is not in line with best security practise.</p> <p>'PUT' allows an attacker to upload arbitrary web pages on the server. If the server is configured to support scripts like ASP or PHP, it will allow the attacker to execute code with the privileges of the web server.</p> <p>'DELETE' allows an attacker to delete arbitrary content from the web server.</p> <p>Only 'HEAD', 'GET' and 'POST' are required for the correct functionality of a web server. All other HTTP methods should be disallowed for security reasons.</p> <p><b>Results</b></p> <p>The following screenshot shows how a .txt file was uploaded to server 10.10.10.201 using the HTTP 'PUT' method:</p> <p><code>http://10.10.10.201/msf_http_put_test.txt</code></p>  <p><b>Recommendation</b></p> <p><b>Disable 'PUT' and 'DELETE'. Production environments typically only need 'HEAD', 'GET' and 'POST'.</b></p>

Additional Servers – Domain 'Anonymised1' – Continued...

### 10.10.10.9 – Windows 2003 Server R2

**●●●●○ Passwords stored in clear-text**

The following files containing passwords have been found on 10.10.10.9. Having unnecessary files can create additional security risks.

**Results**

- 'RefUpdateDataPassword.txt'  
spreadsheet = **refupdate**  
zipfile = **lehman**
- 'Passwords.txt'  
Spreadsheet = **cr0mwell**  
zips = **harr1et**
- 'PASSWORDS.txt'  
zip = **benstat2009**  
spreadsheets = **cr0mwell**
- 'PASSWORD.txt'  
**cr0mwell**  
as in Oliver but the letter o is a zero.

**Recommendation**  
**Delete any unnecessary directories or restrict them to internal administrative interfaces.**

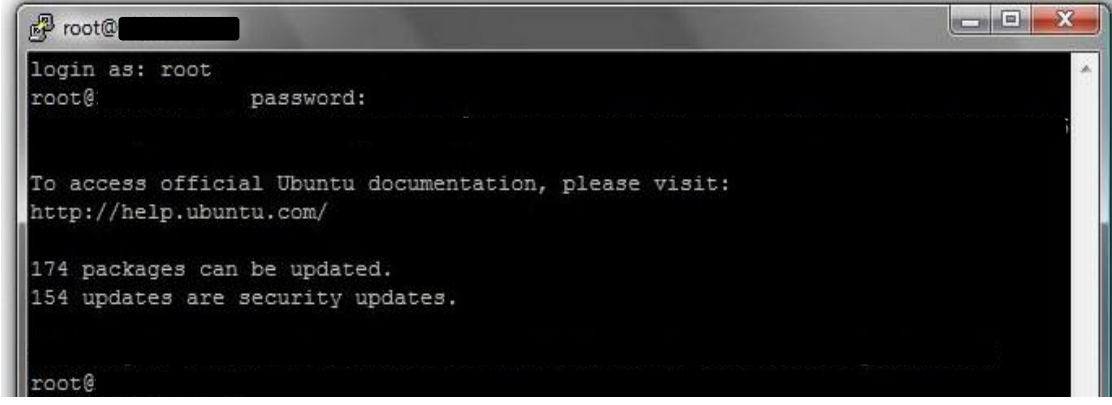
Additional Servers – Domain ‘Anonymised1’ – Continued...

10.10.10.57 – Windows 2003 Server R2

Symantec Backup Exec Authentication Bypass	
<p><b>BackupExec</b> <b>10000</b>  <b>(TCP)</b></p>	<p>The version of Symantec Backup Exec is prone to a vulnerability that allows an attacker to bypass authentication and gain unauthorized access to the affected application. Attackers with authorized network access can exploit this issue to bypass the logon process using the remote agents.</p> <p><a href="http://securityresponse.symantec.com/avcenter/security/Content/2008.11.19.html">http://securityresponse.symantec.com/avcenter/security/Content/2008.11.19.html</a></p> <p>Successfully exploits may allow attackers to retrieve or delete files on the targeted computer. As a proof of concept the c:\boot.ini file was retrieved from such domain controller, as shown below:</p> <p><b>Results</b></p> <pre> VOL=C: FILESYSTEMS=C:\WINDOWS\system32\config\system [boot loader] timeout=30 default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS [operating systems] multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Standard" /fastdetect /NoExecute=OptOut </pre> <p><b>Recommendation</b></p> <p><b>Ensure that a consistent server patching policy is applied for the company's network.</b></p>

### 3.3. Linux Servers – Ubuntu 11.04

10.10.10.77

●●●● Sensitive files found	
<p><b>HTTP</b> <b>80</b></p> <p><b>(TCP)</b></p>	<p>The following files have been found within 10.10.10.77. These files were found to be publicly within organizational infrastructure available and contained sensitive information such as usernames and password hashes which were trivially cracked.</p> <p>Having unnecessary directories can create additional security risks. This is not in line with good security practice and should be corrected without delay.</p> <p><b>Results</b></p> <p><b>http://10.10.10.77/conf</b></p> <p>Password hash retrieved from password.txt:</p> <ul style="list-style-type: none"> <li>• Password hash extracted from “am-staging.dave”: rootpw --iscrypted \$1\$P.eus1q7\$n.XXX1KRXXXX8eY.GXXXX0</li> <li>• Password hashes extracted from “grants.sql” file: dba_local *EFC1EXXXXXXXXXXXXXXXXXXXXXXXXXXXX51C47D098C dba_glynn *7AC1BXXXXXXXXXXXXXXXXXXXXXXXXXXXX6B69EC97B0 mryall *E1225XXXXXXXXXXXXXXXXXXXXXXXXXXXXE84ABE6ACC juys *DACDDXXXXXXXXXXXXXXXXXXXXXXXXXXXXF5C47E2D06 qa_thedome *C4B41XXXXXXXXXXXXXXXXXXXXXXXXXXXX32C4B6AE0F cnguyen *B7965XXXXXXXXXXXXXXXXXXXXXXXXXXXXBFDD37226C panuser *27CFD4XXXXXXXXXXXXXXXXXXXXXXXXXXXXDD8F35EAC4</li> <li>• Password hashes extracted from file “pan.passwd”: techops:4rXXXXXXXX/1fmI dev:5FsXXXXXXXX86</li> <li>• Passwords cracked from Loghost’s /etc/shadow file: drag99 (root) drag99 (panuser) drag99 (a.buskin) chronic (a.godlstein) testing (j.pednekar)</li> </ul> <p>The following screenshot shows how access to linux01 was gained as superuser “root”:</p> 

From this machine and as root, it was possible to get access to “Spike” without any password authentication, as Spike’s root user is not prompted to enter a password but access is granted via a public/private key scheme which was found in linux01. Please note that Spike has access to the production environment.

The line below from Spike’s /etc/shadow file shows how the root user is not prompted for a password such machine:

```
root:*NP*:13830:0:99999:7:::
```

The following illustrates how access was granted to Spike from linux01 by simply SSH to it as the logged in user:

```
root@linux01:~# ssh spike
Last login: Wed Jan 26 10:27:18 2011 from mustang
#####
#           I am spike - Product Image Maker.           #
#                   images live in:                   #
# /disk/image_resizer/images/readonly/processed #
#                   Scripts are in RCS!                 #
# Please remember to ci -l after making changes #
#                   #                                   #
# To remove and flush images, please run:             #
# /disk/image_resizer/images/remove_images.sh #
#####

spike ~ # whoami; id
root
uid=0(root)
```

#### Recommendation

**Delete any unnecessary directories or restrict them to internal administrative interfaces.**

**Ensure that strong authentication is used on critical/production servers.**

### 3.4. Remote Control Services – VNC, Dameware Mini Remote control, Remote Desktop

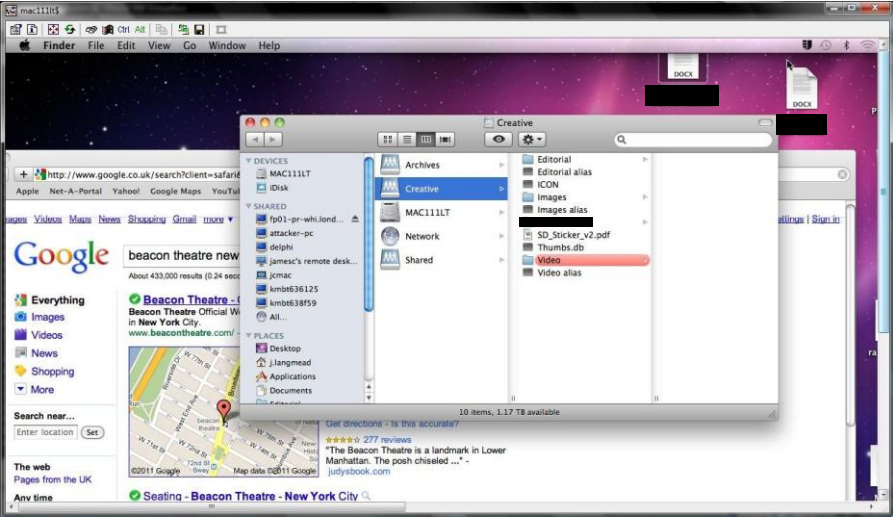
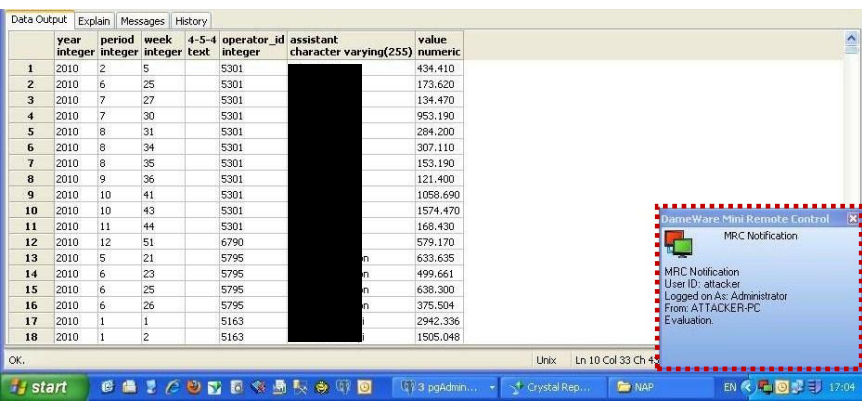
10.10.10.78 – VNC 4.1

10.10.10.215 - Dameware Mini Remote control

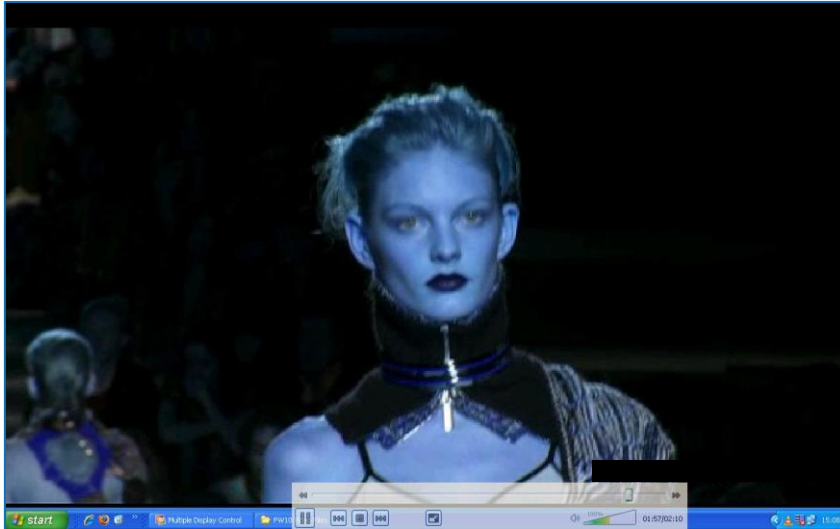
10.10.10.127 - Remote Desktop

10.10.10.90 – VNC 4.1

●●●●●
**Password reuse**

<p><b>VNC</b> <b>5900</b></p>	<p>It was found that the same passwords are being shared by different remote control services within the company’s network; this is not in line with good security practise and should be corrected as a matter of urgency.</p>
<p><b>DMRC</b> <b>6129</b></p>	<p><b>Results</b></p> <p>The following passwords were found to be used on different services such as VNC, Dameware Mini Remote Control and Remote Desktop:</p>
<p><b>RDP</b> <b>3389</b></p>	<ul style="list-style-type: none"> <li>• drag99</li> <li>• Pass@w0rd</li> <li>• MACADMIN</li> <li>• Letmein</li> </ul>
<p><b>(TCP)</b></p>	<p><b>Access granted to 10.10.10.78 through Mac OS X’s VNC server with password “MACADMIN”</b></p> 
	<p><b>Access granted to 10.10.10.215 through Dameware Mini Remote control with password “Letmein”</b></p> 

Access granted to 10.10.10.127 through Remote Desktop as local Administrator with password "drag99"



### Recommendation

**Enforce a secure password complexity on all types of accounts, especially privileged accounts such as administrative accounts. Do not reuse passwords.**

## VNC Authentication Bypass

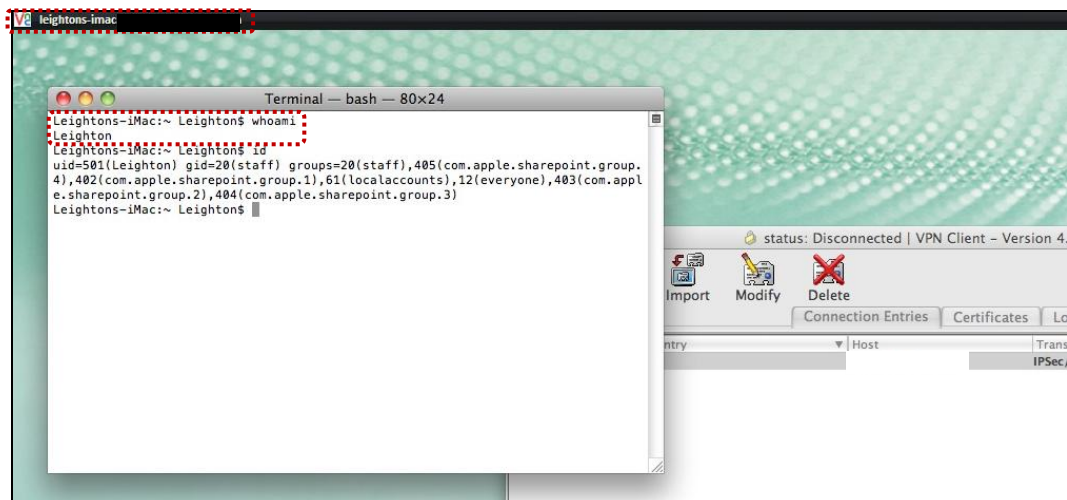
VNC  
5900

(TCP)

The VNC server installed on 10.10.10.90 host allows an attacker to connect to the remote host as no authentication is required to access this service. This should be corrected as a matter of urgency as a malicious VNC client can cause a VNC server to allow it to connect without any authentication regardless of the authentication settings configured in the server by sending an authentication request "secTypeNone" to the VNC server, leading to compromise of servers and workstations from which the network can be attacked.

### Results

It was possible to impersonate user 'Leighton' as the compromised machine was found to be unlocked. The following screenshot shows granted access to such machine from the company's internal network:



### Recommendation

**Upgrade VNC to the latest version available.**

## 3.4. Appendix –Port Scans

### 3.4.1. Network Devices

#### 10.10.10.1

```
Interesting UDP ports on 10.10.10.1:  
PORT      STATE      SERVICE  
17185/udp open|filtered vxworks_wdb
```

#### 10.10.10.2

```
Interesting UDP ports on 10.10.10.2:  
PORT      STATE      SERVICE  
17185/udp open|filtered vxworks_wdb
```

#### 10.10.10.3

```
Interesting TCP & UDP ports on 10.10.10.3:  
PORT      STATE      SERVICE  
17185/udp open|filtered vxworks_wdb  
23/tcp    tcpwrapped telnet (unavailable)
```



### 3.4.2. Windows infrastructure - Domain Controllers - Domain 'Anonymised1'

#### 10.10.10.70

Interesting TCP ports on 10.10.10.70:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2008 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1030/tcp	open	msrpc	Microsoft Windows RPC
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	
3269/tcp	open	tcpwrapped	(unavailable)

Interesting UDP ports on 10.10.10.70:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1030/udp	open filtered	unknown
1034/udp	open filtered	activesync-notify
1039/udp	open filtered	unknown
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Domain Controllers - Domain 'Anonymised1' – Continued...

**10.10.10.71**

Interesting TCP ports on 10.10.10.71:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2008 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1030/tcp	open	msrpc	Microsoft Windows RPC
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	
3269/tcp	open	tcpwrapped	(unavailable)

Interesting UDP ports on 10.10.10.71:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1030/udp	open filtered	unknown
1034/udp	open filtered	activesync-notify
1039/udp	open filtered	unknown
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike

### 3.4.3. Windows infrastructure - Additional Servers – Domain ‘Anonymised1’

#### 10.10.10.47

Interesting TCP ports on 10.10.10.47:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	

Interesting UDP ports on 10.10.10.47:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.49**

Interesting TCP ports on 10.10.10.49:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	

Interesting UDP ports on 10.10.10.49:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.50**

Interesting TCP ports on 10.10.10.50:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	

Interesting UDP ports on 10.10.10.50:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.51**

Interesting TCP ports on 10.10.10.51:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	

Interesting UDP ports on 10.10.10.51:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.210**

Interesting TCP ports on 10.10.10.210:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	

Interesting UDP ports on 10.10.10.210:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.143**

Interesting TCP ports on 10.10.10.143:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	

Interesting UDP ports on 10.10.10.143:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike



## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.110**

Interesting TCP ports on 10.10.10.110:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	
8080/tcp	open	http	Apache Tomcat

Interesting UDP ports on 10.10.10.110:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.111**

Interesting TCP ports on 10.10.10.111:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	
8080/tcp	open	http	Apache Tomcat

Interesting UDP ports on 10.10.10.111:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.15**

Interesting TCP ports on 10.10.10.15:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
111/tcp	open	portmapper	
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	
10203/tcp	open	cals	CA_License_Service
10204/tcp	open	cals	CA_License_Service
6502/tcp	open	cabs	CA Brightstor ARC Serve
6504/tcp	open	cabs	CA Brightstor ARC Serve

Interesting UDP ports on 10.10.10.15:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.16**

Interesting TCP ports on 10.10.10.16:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
111/tcp	open	portmapper	
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	
10203/tcp	open	cals	CA_License_Service
10204/tcp	open	cals	CA_License_Service
6502/tcp	open	cabs	CA Brightstor ARC Serve
6504/tcp	open	cabs	CA Brightstor ARC Serve

Interesting UDP ports on 10.10.10.16:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.19**

Interesting TCP ports on 10.10.10.19:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
111/tcp	open	portmapper	
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	
10203/tcp	open	cals	CA_License_Service
10204/tcp	open	cals	CA_License_Service
6502/tcp	open	cabs	CA Brightstor ARC Serve
6504/tcp	open	cabs	CA Brightstor ARC Serve

Interesting UDP ports on 10.10.10.19:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain 'Anonymised1' – Continued...

**10.10.10.11**

Interesting TCP ports on 10.10.10.11:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
111/tcp	open	portmapper	
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	

Interesting UDP ports on 10.10.10.11:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.94**

Interesting TCP ports on 10.10.10.94:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
111/tcp	open	portmapper	
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	

Interesting UDP ports on 10.10.10.94:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1044/udp	open filtered	unknown
1050/udp	open filtered	unknown
1056/udp	open filtered	unknown
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain 'Anonymised1' – Continued...

**10.10.10.79**

Interesting TCP ports on 10.10.10.79:

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Microsoft IIS httpd 5.0
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	
445/tcp	open	netbios-ssn	
515/tcp	open	printer	
1036/tcp	open	msrpc	Microsoft Windows RPC
1166/tcp	open	msrpc	Microsoft Windows RPC
3389/tcp	open	ms-term-serv	
42509/tcp	open	unknown	
42510/tcp	open	msrpc	Microsoft Windows RPC

Interesting UDP ports on 10.10.10.79:

PORT	STATE	SERVICE
53/udp	open filtered	domain
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
1060/udp	open filtered	polestar
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
1032/udp	open filtered	iad3



## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.201**

Interesting TCP ports on 10.10.10.201:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
80/tcp	open	http	Microsoft IIS httpd 6.0
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1042/tcp	open	msrpc	Microsoft Windows RPC
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	

Interesting UDP ports on 10.10.10.201:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
1043/udp	open filtered	boinc
1060/udp	open filtered	polestar
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain ‘Anonymised1’ – Continued...

**10.10.10.9**

Interesting TCP ports on 10.10.10.9:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	

Interesting UDP ports on 10.10.10.9:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

## Windows infrastructure - Additional Servers – Domain 'Anonymised1' – Continued...

**10.10.10.57**

Interesting TCP ports on 10.10.10.57:

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	NFS-or-IIS?	
1026/tcp	open	msrpc	Microsoft Windows RPC
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1053/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	
10000/tcp	open	BackupExec	Veritas Backup Exec

Interesting UDP ports on 10.10.10.57:

PORT	STATE	SERVICE
53/udp	open filtered	domain
88/udp	open filtered	kerberos-sec
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
389/udp	open filtered	ldap
445/udp	open filtered	microsoft-ds
464/udp	open filtered	kpasswd5
500/udp	open filtered	isakmp
1040/udp	open filtered	unknown
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
1032/udp	open filtered	iad3
4500/udp	open filtered	nat-t-ike

### 3.4.4. Linux Servers – Ubuntu 11.04

#### 10.10.10.77

Interesting TCP ports on 10.10.10.77:

PORT	STATE	SERVICE	VERSION
80/tcp	open	httpd	Apache 2.2.14 ((Ubuntu))
22/tcp	open	tcpwrapped	(unavailable)
53/tcp	open	domain	ISC Bind 9.X

Interesting UDP ports on 10.10.10.77:

PORT	STATE	SERVICE	VERSION
53/udp	open	domain	ISC Bind 9.X

### 3.4.5. Apple Workstations – Mac OSX 10.7.2 (Lion)

#### 10.10.10.78

Interesting TCP ports on 10.10.10.78:

PORT	STATE	SERVICE	VERSION
5900/tcp	open	vnc	Apple remote desktop vnc

Interesting UDP ports on 10.10.10.78:

PORT	STATE	SERVICE	VERSION
67/udp	open filtered	dhcps	
123/udp	open	ntp	NTP v4
137/udp	open	netbios-ns	Microsoft Windows XP netbios-ssn
138/udp	open filtered	netbios-dgm	
5353/udp	open	mdns	DNS-based service discovery

#### 10.10.10.90

Interesting TCP ports on 10.10.10.90:

PORT	STATE	SERVICE	VERSION
5900/tcp	open	vnc	Apple remote desktop vnc

Interesting UDP ports on 10.10.10.90:

PORT	STATE	SERVICE	VERSION
67/udp	open filtered	dhcps	
137/udp	open	netbios-ns	Microsoft Windows XP netbios-ssn
138/udp	open filtered	netbios-dgm	
5353/udp	open	mdns	DNS-based service discovery

### 3.4.6. Windows Workstations – Windows XP Professional Service Pack 3

#### 10.10.10.215

Interesting TCP ports on 10.10.10.215:

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1053/tcp	open	msrpc	Microsoft Windows RPC

Interesting UDP ports on 10.10.10.215:

PORT	STATE	SERVICE
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp

#### 10.10.10.127

Interesting TCP ports on 10.10.10.127:

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc?	
139/tcp	open	netbios-ssn	
1029/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1053/tcp	open	msrpc	Microsoft Windows RPC

Interesting UDP ports on 10.10.10.127:

PORT	STATE	SERVICE
123/udp	open filtered	ntp
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp
4500/udp	open filtered	nat-t-ike
137/udp	open filtered	netbios-ns
138/udp	open filtered	netbios-dgm
445/udp	open filtered	microsoft-ds
500/udp	open filtered	isakmp