

***Penetration Testing***

**Michael Sowemimo**

**White Paper**

**Alberta University**

**School Arts, Media and Computer Games**

**\* Year E.g. 2016/2017\***

Contents

[2 Executive Summary 2](#_Toc479608543)

[3 Web Manager – Infrastructure Penetration Testing 3](#_Toc479608544)

[4 Methodology 4](#_Toc479608545)

[5 Web Manager – Web Application Testing 5](#_Toc479608546)

[6 Appendix 6](#_Toc479608547)

[7 References 7](#_Toc479608548)

# Executive Summary

## Introduction

This report contains findings from the Abertay Pentest agency which was implemented for Web file industries. The test was initiated between 17th and the 21st of March 2017. The objective of the exercise was to allocate security threats and vulnerabilities that affect web manager file web and infrastructure. The security test was conducted in a virtual environment, in which has its specific network parameters, the virtual environment will allow all stimulated attacks but also protects web manager file main network. The web application is used to upload files to the server, also allowing users to register and administrators. Additionally, the web application has a list of concerns which are listed as followed:

* The integrity of the users if the application
* Authorization and the confidentiality of the users
* The authentications policies

## key findings

The primary object of this test to determine the web file infrastructures weakness. The results of the will surface the correct remediation and mitigation in case of real life attack by a malicious user. The stimulated attacks that are discussed in this report can allow an unauthorized user to uphold the entire web file bank manger network infrastructure. The following attacks can be identified during the security test:

* **Input Validation Testing**
* **Authorization testing**

The main objective of this test the web application and report the critical threats surrounding the web file bank manger’s application and infrastructure layer weaknesses, plus finding the appropriate mitigation practices and remediation in case of future occurrences. The results of the security test, can allow a novice attacker to mishandle the client-server architecture of the web file network. If an attacker obtains this document, the attacker can gain access to the network infrastructure without the organisation without being detected. The following key findings were identified during the security assessment:

* **Improper input validation:** It appears that the web application is vulnerable to Boolean based SQL injection, with this vulnerability an attacker is able to read, update and delete a multitude amount of data from the database. The Boolean SQL injection itself, allows an attacker to steal data by asking the database a series of true or false questions.
* **Database user has admin privileges:** This vulnerability can allow an attacker to additional privileges through SQL injection. The attacker can execute a reverse shell in which can allow the user to implement commands on the operating system, plus a privilege escalation attack to gain access to the target system and its users.
* **Credentials transported over an encrypted channel:** This vulnerability allows an attacker to intercept the network traffic to steal user credentials.
* **Session management:** An attacker can force an already authenticated user to execute unwanted actions on the web application. This attack is known as cross-rite-script-forgery. A successful attack could contaminate end user data and if the target user is the administrator account, the CRSF attack can shut down the entire web application. **Poorly constructed authorization mechanisms:** This issue allows an attacker to gain privileges that should be only intended for system administrators and developer.

## Priority Recommendations

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Activity** | **Description** | **Priority** |
| A01 | Application  Security  Assessment | Web file manager needs to adhere input validation. This is because attacks such as SQL injection can be used to steal and modify data or an extreme case can facilitate command injection to gain entry to the operating system. Parametrized queries can be used to distinguish code and data. The parametrized query, despite what the user input is contributed. Since the web is built using PHP, it is recommended that the developers use PDO with strongly typed parameterized queries. | High |
|  |  |  |  |
| **Ref** | **Activity** | **Description** | **Priority** |
| A02 | Application  Security  Assessment | The database user should be created with the least possible permissions as possible. | High |
| A03 | Infrastructure Penetration Test | The password surrounding one the CLIENT 2 should be changed and ought to contain complex characters. Authentication must be locked after the number of password attempts is more than what was set initially. | High |
| A04 | Application  Security  Assessment | In relation to session management, checks must be made. This includes sourcing the origin of HTTP request and the target origin. It is recommended that the developers use origin headers and refer heads. | Medium |
| A05 | Application  Security  Assessment | Web developers should keep administrative accounts separate from the standard user accounts. Software that contains timely and security updates should be used to ensure that if any privilege escalation vulnerabilities are discovered there will be immediate fixes as they are surfaced | High |

## Conclusion

The web file bank manager web application is vulnerable to critical threats in relation to the infrastructure and the internal configurations. These threats can cause great implications if not treated immediately. Based on the threats found, an amateur hacker can reach a professional status easily. All it would take is a simple backdoor and the entire network could be uprooted. Even though the web site is used to share images with colleagues, there are pathways that exists on the web application. As mentioned earlier, an attacker can obtain the network through privilege escalation. Ignoring the immediate threats could result to organisations losing their reputation, plus important business assets. Web file managers should pay great attention to this document, for the reason that it could ruin the business transactions.

# infrastructure Penetration Test

## Introduction

With the permission of web file manager, an infrastructure test was withheld between the 17th and 21th of March 2017. The objective is to perform an in-depth review of configuration and the sourced security issues. This can only be accomplished when the entire web manager file network is mapped. It is crucial that all vulnerabilities are identified and corrected as there encountered. The test was conducted in a virtual environment, this method allows the managing directors to understand the type of methods and tools that are used during a live attack against the network infrastructure. The test was initiated as grey hat; this means that the knowledge surrounding the web file manager network is partially supplied. A detailed summary of the tools used, can be located in the Appendix.

|  |  |
| --- | --- |
| **Host** | **Description** |
| 192.168.0.1  (Server 1) | Domain Controller(Main): UADTARGETNET  Windows Server 2008 R2 Datacentre  Hosting web file manager  No access |
| 192.168.0.2  (Server 2) | Domain controller(Primary): UADTARGETNET  Windows Server 2008 R2 Datacentre  No access |
| 192.168.0.10  (Client 1) | Windows 7 professional 6.1  No access |
| 192.168.0.11  (Client 2) | Windows 7 professional 6.1 |
| 192.168.0.200  (Attack Machine) | Kali Linux |

# Web Manager – Infrastructure Penetration Testing

## Methodology

The methodology that was implemented will follow the penetration test framework, the following penetration test methodology is highly applicable to this test;

## Discovery & probing

During this phase, the attacker will implement operating system fingerprinting and probing. The attacker tries to identify active systems on the network and the services that are running momentarily. Tools such as Nmap which is a network discovery tool that can be used to determine active host on the network. During the security assessment, an aggressive and verbose scan was used to find out what type of operating system and service running on the web file manager network. Server1 appears to be hosting the web file manager web application on port 80 and plus the Server is the domain controller and running windows server 2008. Server 2 is also a domain controller and accepts the following http methods: TRACE, GET, and POST. Both operating systems seem to be up-to-date.

Client 1 and client 2 are both running windows 7 and appears to be out of date. There is no installed spyware on client 2.

## Vulnerability Scanning

In this phase, the attacker implements a vulnerability scan that detects and categorizes system weakness in network devices and consolidates the usefulness of the countermeasures. Although the vulnerability scan could only uncover threats relating to the web application in which is internet facing, although the threats can be used to get access to the network internal system. Additionally, several vulnerability scanners was used to compare and contrast the results. It is possible that a vulnerability will not be able to identify all the threats in the web application.

## Enumeration

At this stage, the attacker tries to find available host on the network and clarifying their purpose. The enumeration phase gives the attacker a better approach of assessing the web file manager vulnerability, also determining if the vulnerabilities are exploitable. As stated earlier Server1 is the active domain controller, since the clients are assets of the domain. It was possible to enumerate the entire domain by using basic privileges, with the assistance of Cain and Abel. The Cain and Abel application is a password recovery tool for Microsoft operating systems.

## Password Cracking

Once the attacker has obtained a target host, the attacker has many avenues of disrupting the network traffic. During this attack, the attacker implements password cracking tools to recover passwords that have been stored or transmitted by a computerised device. Since the users of the domain are exposed, it is quite possible to crack the entire organisation password. Tools like medusa can be used to crack a system password.

## Threat/Remediation Qualification

The results of the threats are successful attacks there were initiated against the web file manager site. The appropriate countermeasures will be assigned at the end of the document, also advice relating to the network topology.

# Key Findings - Internal Penetration Test

1. **Passing the Hash**

This attack should be the centre focus for remediation, the reason is that the attack is based on allocating a valid set of user credentials e.g. username and the password hash, and authenticating to a remote computer system as that user. The windows operating system usually saves two different hashed forms of the user accounts passwords. Once the hash forms are in its simplest form, the attack starts with a stolen windows password hash in which is loaded into memory on the targeted system. Since the attack only requires user account and domain name, it was possible to launch attack based on having access to client 2 and also residing on the same subnet as the attack machine.

Additionally, Server1 (Domain controller) appears to have an open SMB port open (port 445) which also plays as role for the attack. The SMB protocol, is known as an application layer or a presentation layer protocol which is used by window based computers. By searching the target location using PSEXEC, if the SMB protocol is available it is possible for the attacker to access the target machine by exploiting the SMB authentication. From here the attacker can access the target system by implementing a reverse TCP shell.

1. **Detailed Technical Findings infrastructure Penetration Test**

## Web file manager – Infrastructure Penetration Test

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ref** | **Target** | **Imp** | **SR** | **Description** | **Recommendation** |
| 5.1.2 | 192.168.0.10  (Client 1) | V  e  r  y    H  i  g  h | L  o  w | The following operating system has weak password verification. Since both clients are part of the domain, it is possible to login to client 1 using client 2 credentials. | The Passwords that are assigned to each client machine, should be unique and should be validated in case of a brute force attack or some form of privilege escalation. |
| 5.1.3 | 192.168.0.10,  192.168.0.2 | V  e  r  y    H  i  g  h | B  e  g  i  n  n  e  r | These targets can be accessed through an interactive shell, in which can allow an attacker to obfuscate the operating system infrastructure. This attack was accomplished by send a document with a payload that contains a listener. Once the client has open the document, the attacker can obtain the clients terminal remotely or the ability to elevate from a basic user. | Web file managers should restrict access to downloads, since the attack focuses on the client events. Income and outgoing emails should be separated. The firewall must be kept turned on at all times, plus a network monitoring tool to monitor the network traffic. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ref** | **Target** | **Imp** | **SR** | **Description** | **Recommendation** |
| 5.1.4 | 192.168.0.1,  192.168.0.10 | V  e  r  y    H  i  g  h | B  e  g  i  n  n  e  r | The target list are subjected to enumeration attacks. Since the credentials for client 2 was given before the security assessment. It was possible to enumerate all users on the domain using Cain and Abel. Which is known as a password recovery tool. | Port filtering should be implemented on port 445 and 135. Restrict remote access to basic users. Disable SMB services completely from network devices. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ref** | **Target** | **Imp** | **SR** | **Description** | **Recommendation** |
| 5.1.4 | 192.168.0.1,  192.168.0.10 | V  e  r  y    H  i  g  h | B  e  g  i  n  n  e  r | The target list are subjected to enumeration attacks. Since the credentials for client 2 was given before the security assessment. It was possible to enumerate all users on the domain using Cain and Abel. Which is known as a password recovery tool. | Port filtering should be implemented on port 445 and 135. Restrict remote access to basic users. Disable SMB services completely from network devices. |

# Application security assessment

## Introduction

The web file manager application was developed to administer bank accounts for new existing users. The application has two web accounts, one is for authenticated users and the other account is for the administrators. Administrators are able to register new users and can also send messages to other administrators in the organisation. Also in conjunction to the registration users, the administrators can upload files to the Server. It seems that the Administrators contain the highest privileges of the web file applications internal structure.

## scope

The URL that was assigned to the investigation is**:** [**http://192.168.0.1**](http://192.168.0.1)

The development team has informed Abertay pentest team that the entire web structure is really buggy and is hard to detect. As a result the pentest team at abertay has decided to implement a web application test on top of the infrastructure. Only one user account was assigned with minimal privileges. This was set up to evaluate the suitability of the authorisation and authentication.

## Methodology – OWAP (Open web application Security project)

The methodology that was applied in test was used in parallel with the owasp framework, the OWAP framework provides an open and collaborative platform f

# Information Gathering

## Fingerprint web server

### Identify Application entry points

Identifying the entry points in the crucial part of the security assessment, it involves identifying areas of the web application that may contain a particular weakness or a threat. In this step aims to identify and map areas surrounding the web application and documenting the investigation once the enumeration and the mapping has been finalized. The test begins by paying close attention to how the HTTP request are utilized. An intercepting proxy such as OWAP Zap proxy, was used to examine how the application communicated with the server. Meanwhile, during the security examination there was multiple pathways for entry points. Especially, the login form in which has 200 as the server status code. The server status code determines the class response that the client accepts, comprehended and handled correctly. The Login form indicated possible injection points that can be implemented to bypass the authentication of the web application.

### Review Webserver Metafiles for Information Leakage

This step is used to test for robots.txt file for information leakage of the web application file directory of path. However, the list of directories that are supposed to be avoided by spiders, robots or crawlers can also act as a mechanism to determine the paths through the application. The reason being that the entire web architecture can be linked to different file paths in which can be serving different functions. Although the robot.txt file can be used a gateway for the attacker enumerate the back end database. The robot txt file serves as an instruction base for every web site owner, if restrictions are not carefully structured it can result to attacks guessing and obtaining passwords.

### Testing for Credentials Transported over an Encrypted Channel

Throughout this stage, tests are made to undermine the credentials transport and verifying that the user’s authentication are encrypted in order to avoid interception by malicious users. The step is also critical, since related to the encryption of data used by the authenticated user. This step concentrates on the way data travels encrypted from the web browser to the server of if the web server takes charge and uses the correct security measures, for example using a protocol such as HTTPS. However, the web file manager has no traces of HTTPS or any other encryption mechanism to secure data. The main issue is that without encryption a malicious user can intercept the username and password by sniffing the network with wire shark or using a commercial vulnerability scanner such as Nets parker.

### Map execution paths through application

This stage relates to the understanding of the structure of the application, without an in-depth it is impossible to understand the principal workflow of the web application. Also in this test, the approach is to test each path and asses the boundary of each path. Additionally the testing the dataflow and the transformation of data throughout the application. Plus testing multiple instances of the application handling the same data. The main object of this test, is to spider the entire web application to see any hidden directories that may have valuable information that may be apprehended by malicious user.

# Key findings – Application Security Assessment

During the examination there where severe vulnerabilities that was obtain during the test, developers and third parties that invest capital to web file manager. Must pay great attention to these following findings:

## SQL injection

During the mapping execution test, it was noted that the main index page for the web file manager application was vulnerable to SQL injection. The SQL injection vulnerability is the most prevalent attack used against web application. The attack is critical and should not be ignored, also the attack focuses manipulating SQL statements and inserting the statements into an entry field for execution.Morever the SQL injection attack allows an attack to read and obtain sensitive data from the database and also being able to insert, delete and update at will. Although, the attack can also lead to more freighting attacks such as leveraging administrative rights to the database. This could lead to complete disclosure of all the data on the system whether it be external or internal. The SQL injection vulnerability was located using the OWAP proxy tool.

## Database enumeration

This vulnerability pertains the extension of the SQL vulnerability, in this case the attacker has already obtained a URL which refers to a specific id that links to a column within the database table. With this id, an attacker can enumerate different databases on the server. In this test, it was possible to obtain the web server content in spite of this vulnerability. With the assistance of SQL map, grabbing the passwords for the domain administrator was achievable.

## Cross-Rite-scripting

A cross-rite script vulnerability was located in the registration section of the web page, the cross rite script vulnerability is known as an injection type attack whereas the attacker uses a malicious script to a random user at choice. The user is unaware of the script but is tricked into execution, the user also believes that the attack comes from a trusted source. Consequently, the malicious script can access website components such as; session tokens, cookies or any sensitive information relation to the users website.

## Password over HTTP

The security test has detected that the passwords on the web manager file applications. Clear text passwords are a serious hazard. This vulnerability causes a great threat, the reason being that the passwords can be vulnerable in many ways such as the following:

* The password can be obtained using packet sniffing tools
* The availability of the password can be located in the browsing history
* The passwords can assist in brute force attacks and privilege escalation

## Web shell

Due to improper input validation techniques, a web shell was able to display all contents from the back end of the web application. This is the main vulnerability that was found during the security examination. The web shell is launched in the file upload page, the web shell was able to access the file structure of the Server1 (Primary domain). Seeing as server1 is the primary domain, the web shell was used to change the password of primary domain, as a result the main sever1 was comprised.

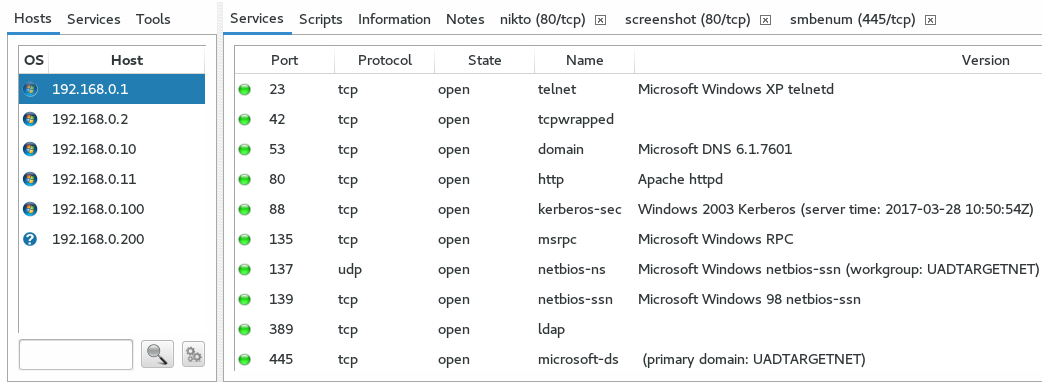
1. **Appendix – Security Assessment**

## Appendix –A Tools

|  |  |  |
| --- | --- | --- |
| **Tool** | **Description** | **Source** |
| Nmap | Nmap is a popular network port scanner with advanced service identification capabilities. | [http://www.insecure.org/nm a](http://www.insecure.org/nm)[p](http://www.insecure.org/nmap) |
| Nessus 4 | A leading commercial vulnerability scanner used for infrastructure scanning. | [http://www.nessus.org](http://www.nessus.org/) |
| Wireshark | A popular packet sniffing and analysis tool used to monitor network traffic. | <http://www.wireshark.org/> |
| Burp Professional | A popular man-in-the middle proxy tool used for assessing web-based applications. | <http://www.portswigger.net/> |
| Sqlmap | A popular penetration testing tool that automates the process of detecting SQL injection flaws and also attempts to override server configure | http://sqlmap.org/ |
| C99 Shell | Notorious PHP malware that allows an attacker to hijack the web server processes. | http://www.madirish.net/241 |
| Sparta | A python GUI that makes pen testing simpler by collaborating scanning and emuneration phase of pen testing | http://sparta.secforce.com/ |
| Netsparker | A Windows application which is used for wen application security scanner | https://www.netsparker.com/web-vulnerability-scanner/ |
| Nishang | An open source framework with a myriad of PowerShell scripts that used during the post exploitation phase of the penetration. | https://github.com/samratashok/nishang |

# Appendix

## Discovery & probing



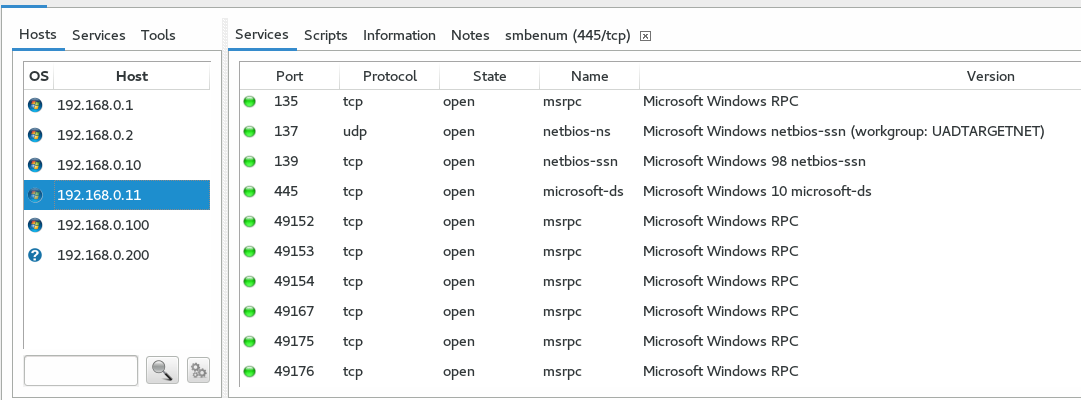
**Figure 1.1 Intense scan for Server 1**



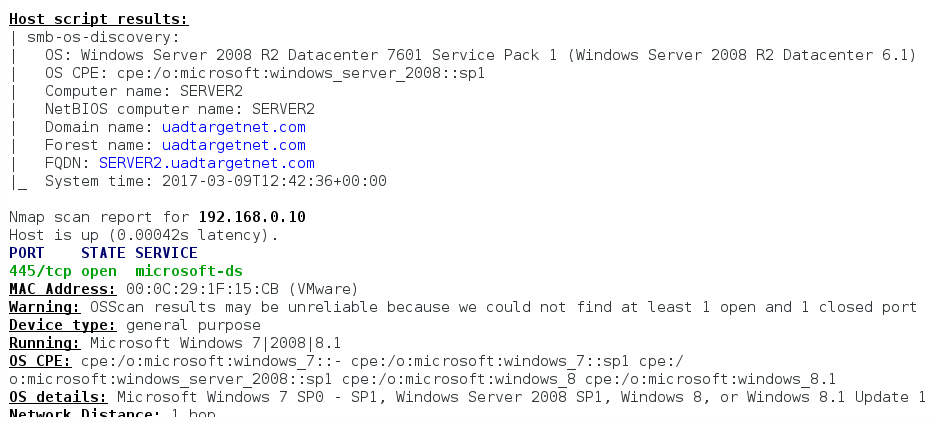
**Figure 1.1 OS fingerprinting for Server 1**



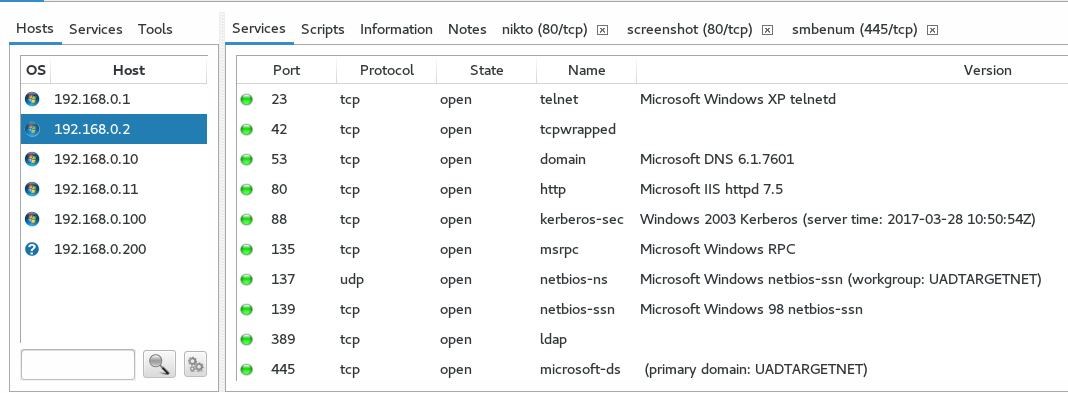
**Figure 1.2 Intense Scan For Server 1**



**Figure 1.2 Intense Scan for Server 2**

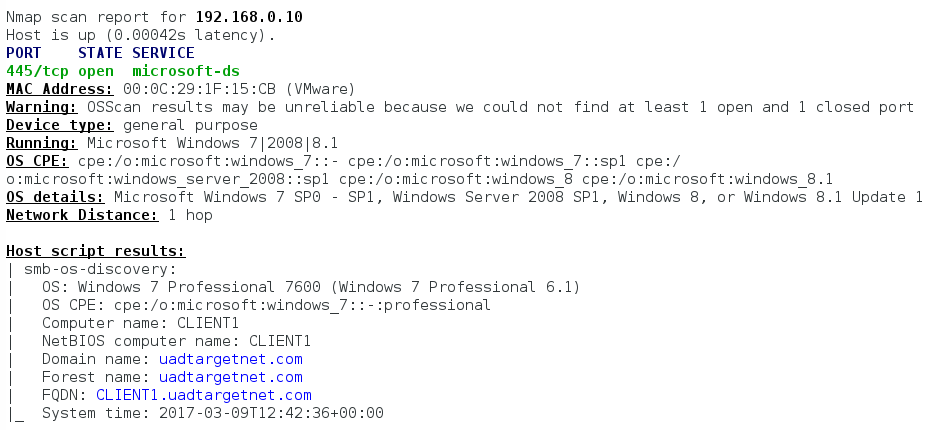


**Figure 1.2 OS Fingerprinting for Server 2**



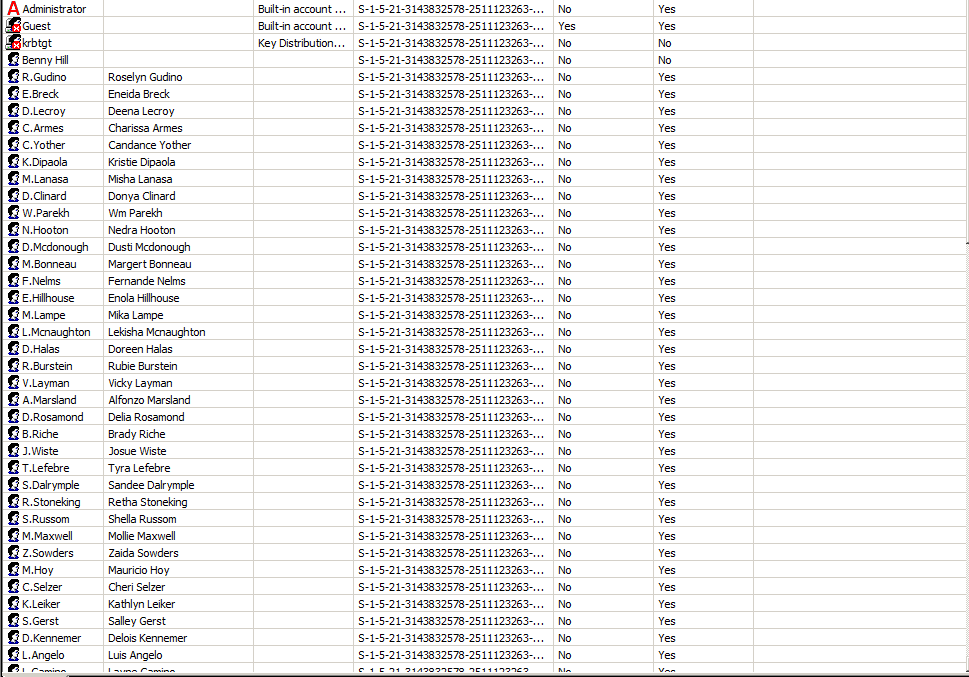
**Figure 1.4 Intense Scan for Client 2**

**Figure 1.5 Intense Scan for Client 1**



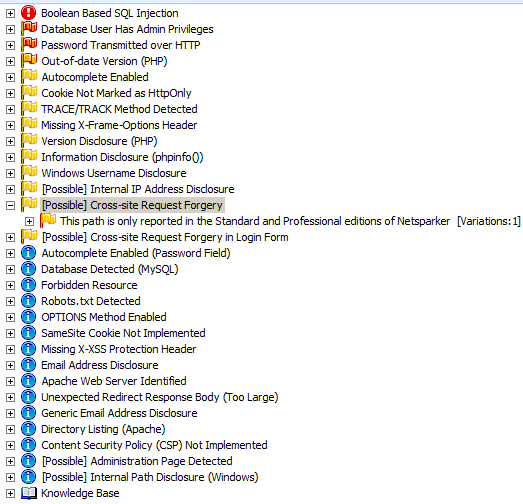
**Figure 1.5 OS Fingerprinting for Client 1**

## Enumeration



**Figure 1.4 Enumerating domain SID’s using Client 2 Credentials**

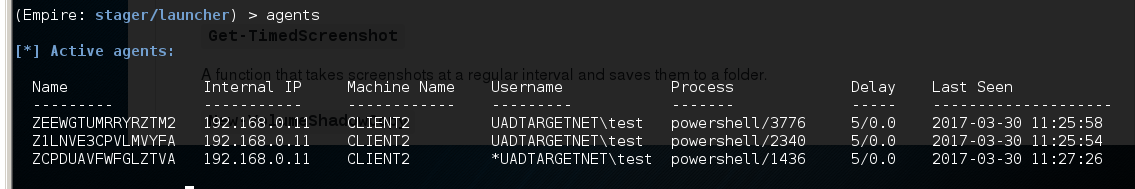
## Vulnerability assessments



## Nikto

## Nessus

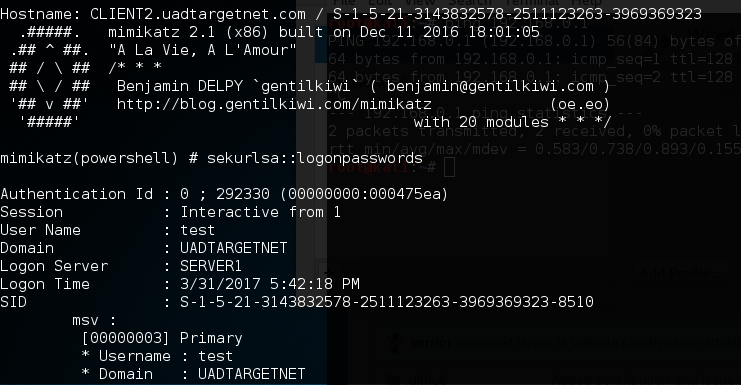
## Passing The Hash



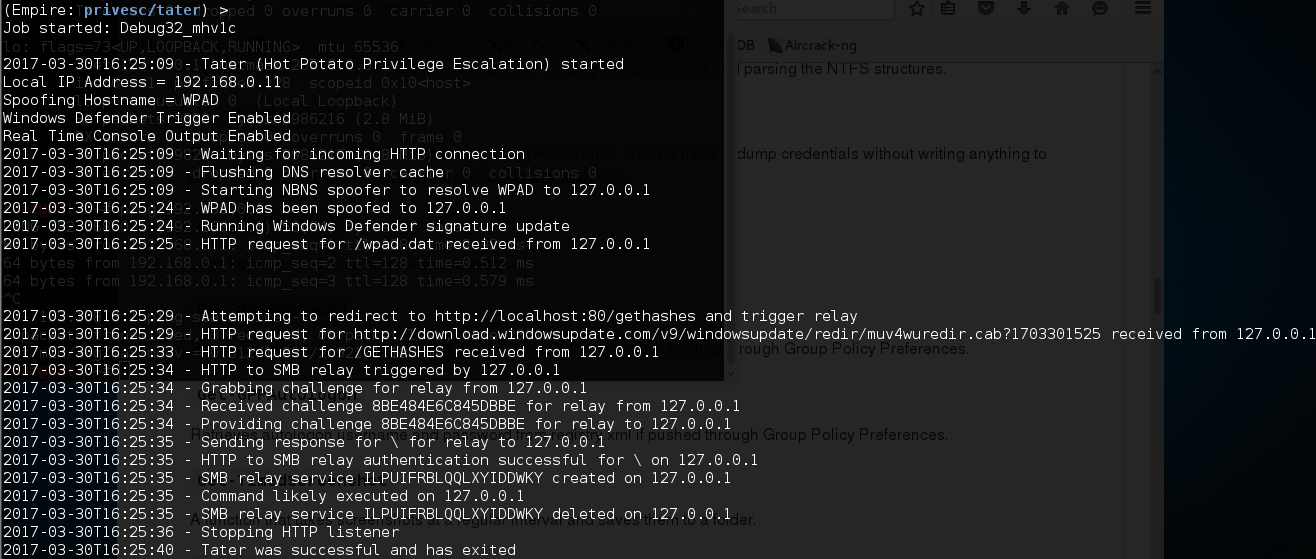
**Setting up the Agents, asterisks means that the client has Administrative Privileges**

## 

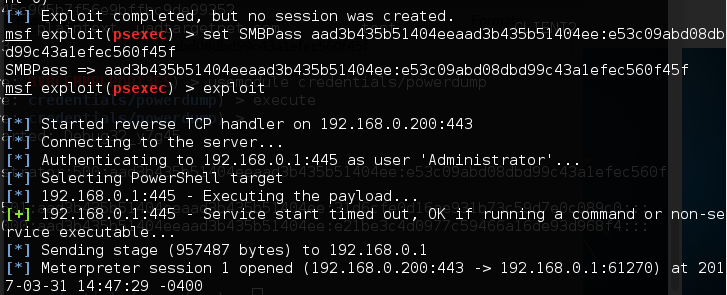
**Using the Prevesc/tater module for privilege Escalation, optimizing the configuration with the domain Username**



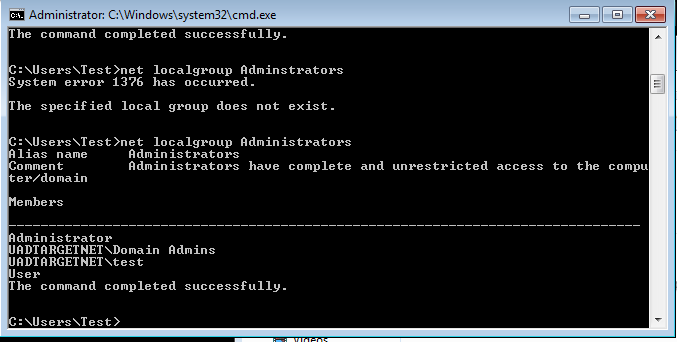
**Extracting the NTML Hashes**



**Interacting with client 2 and trying to elevate as Administrator**



**Pass the Hash Attack**



**Evidence of client 2 as an Elevated Admin**

# Discussion and Results

# Ethical Consideration

# Critical Evaluation of the Methodology

# Conclusion

# References