**Pentesting Active Directory and kerberos bypass**

Archit Benipala, Chandra Sekhar Rao Batthulab, Prathyusha Musunuria, Rohith Marvathua, Krishnaiah Tellagaddac, Aditya varma Yarraa, Reshmi Mitraa

South East Missouri State University -Cape Girardeau, Missouri.

[{ asbenipal1s@semo.edu, cabbthula1s@semo.edu](mailto:%7b%20asbenipal1s@semo.edu,%20cabbthula1s@semo.edu), pmusunuri1s@semo.edu, rmarvathu1s@semo.edu, ktellagadda1s@semo.edu, ayarra1s@semo.edu}

***Abstract*—** **Penetration testing, also known as ethical hacking, is a vital process for identifying vulnerabilities and weaknesses in computer systems or networks. This article focuses on the basics of penetration testing using three primary tools: Nmap, Metasploit, and John the Ripper. Nmap is used for the reconnaissance and scanning phases of penetration testing, which involves identifying the services running on a target system or network. Metasploit is used for exploiting identified vulnerabilities, while John the Ripper is used for password cracking. The article provides an overview of penetration testing, its importance, and how it is done, along with a detailed explanation of how to use each of the three tools.**

# INTRODUCTION

Penetration testing, also known as "pen testing," is the practice of assessing the security of computer systems, networks, and web applications by simulating an attack from a malicious hacker. The goal of pen testing is to identify vulnerabilities in a system before an attacker can exploit them. This process involves using various tools and techniques to identify weaknesses in a system's defences and attempting to exploit them in a controlled and ethical manner.

Penetration testing can be divided into several stages, including reconnaissance, scanning, enumeration, vulnerability assessment, exploitation, and post-exploitation. During reconnaissance, the tester gathers information about the target system, such as the IP address, network architecture, and operating system. Scanning involves using tools to identify open ports and services running on the target system. Enumeration involves gathering information about users and services running on the system. Vulnerability assessment involves identifying and evaluating vulnerabilities in the target system. Exploitation involves attempting to exploit vulnerabilities to gain access to the target system. Finally, post-exploitation involves attempting to maintain access to the target system and cover up any evidence of the penetration test.

Penetration testing is an essential tool for organizations that want to ensure the security of their computer systems and networks. By identifying vulnerabilities in their defenses, they can take steps to patch them before they are exploited by malicious attackers. Penetration testing can also help organizations comply with regulatory requirements and improve their overall security posture.

Nmap is a popular open-source network exploration and security auditing tool that is widely used by security professionals and network administrators. The name Nmap stands for "Network Mapper". Nmap can be used to discover hosts and services on a network, as well as identify vulnerabilities and potential security issues.

Nmap uses various scanning techniques to gather information about hosts and services on a network. Some of the most used Nmap scanning techniques include:

TCP Connect Scan - This technique connects to a target machine using a full TCP three-way handshake and determines if the port is open, closed, or filtered.

SYN Scan - This technique sends SYN packets to a target machine and examines the response to determine if the port is open, closed, or filtered.

UDP Scan - This technique sends UDP packets to a target machine to determine if the port is open, closed, or filtered.

OS Detection - This technique sends packets to a target machine and analyses the responses to determine the operating system running on the target machine.

Nmap also includes features such as version detection, scriptable interaction with the target system, and the ability to perform ping sweeps and traceroutes. It can be used from a command-line interface or through a graphical user interface, making it accessible to users with varying levels of technical expertise.

Overall, Nmap is a powerful tool that can provide valuable information about a network and its vulnerabilities. However, it should be used ethically and with the appropriate permissions from network administrators or system owners.

In this scenario we have been given an IP (or multiple IP addresses) to perform a security audit on. Before we do anything else, we need to get an idea of the “landscape” we are attacking. What this means is that we need to establish which services are running on the targets.

For Example perhaps, one of them is running a webserver, and another is acting as a Windows Active Directory Domain Controller. The first stage in establishing this “map” of the landscape is something called port scanning. When a computer runs a network service, it opens a networking construct called a “port” to receive the connection. Ports are necessary for making multiple network requests or having multiple services available. For example, when we load several webpages at once in a web browser, the program must have some way of determining which tab is loading which web page. This is done by establishing connections to the remote webservers using different ports on the local machine. Equally, if we want a server to be able to run more than one service (for example, perhaps we want the webserver to run both HTTP and HTTPS versions of the site), then we need some way to direct the traffic to the appropriate service. Once again, ports are the solution to this. Network connections are made between two ports – an open port listening on the server and a randomly selected port on the computer. For example, when we connect to a web page, computer may open port 49534 to connect to the server’s port 443.

Diagram

Description automatically generated

As in the previous example, the diagram shows what happens when we connect to numerous websites at the same time. Your computer opens up a different, high-numbered port (at random), which it uses for all its communications with the remote server.

Every computer has a total of 65535 available ports; however, many of these are registered as standard ports. For example, a HTTP Webservice can nearly always be found on port 80 of the server. A HTTPS Webservice can be found on port 443. Windows NETBIOS can be found on port 139 and SMB can be found on port 445.

If we do not know which of these ports a server has open, then we do not have a hope of successfully attacking the target; thus, it is crucial that we begin any attack with a port scan. This can be accomplished in a variety of ways – usually using a tool called Nmap. Nmap can be used to perform different kinds of port scan, basic theory is this: Nmap will connect to each port of the target in turn. Depending on how the port responds, it can be determined as being open, closed, or filtered (usually by a firewall). Once we know which ports are open, we can then look at enumerating which services are running on each port – either manually, or more commonly using Nmap.

John the Ripper, often referred to simply as "John," is a free and open-source password cracking tool that is widely used by security professionals and researchers. The tool is designed to identify weak or easily guessable passwords, and it can crack passwords from a variety of sources, including password files, encrypted files, and network traffic captures.

Metasploit is a popular open-source framework used for developing and executing security exploits. The tool is widely used by security professionals and penetration testers to test the security of computer systems and networks. Metasploit provides a comprehensive and flexible platform for developing, testing, and deploying security exploits, making it a valuable tool for both offensive and defensive security operations.

Metasploit includes a large collection of exploits, payloads, and auxiliary modules, which can be used to test and exploit various vulnerabilities in target systems. It also provides a command-line interface and a graphical user interface, making it accessible to users with varying levels of technical expertise.

Some of the key features of Metasploit include:

Exploit Development - Metasploit provides a comprehensive platform for developing exploits for various vulnerabilities.

Payload Generation - Metasploit includes a large collection of payloads that can be used to take control of a target system.

Post-Exploitation - Metasploit includes modules that can be used to maintain access to a compromised system and cover up any evidence of the penetration test.

Scanning - Metasploit includes modules for scanning networks and identifying vulnerable systems.

Integration - Metasploit can be integrated with other security tools, such as Nmap and Nessus, to provide a comprehensive security testing solution.

Metasploit is a powerful tool that can be used for both legal and illegal purposes, so it is important to use it ethically and with the appropriate permissions from network administrators or system owners. As with any security testing tool, it is important to use Metasploit responsibly and with the goal of improving the security of systems and networks.

John the Ripper is a command-line tool that is available for a variety of operating systems, including Windows, Linux, and macOS. It uses various techniques to crack passwords, including dictionary attacks, brute-force attacks, and hybrid attacks that combine these two techniques. It also supports a variety of password hash formats, including UNIX crypt, MD5, SHA-1, and Windows NTLM.

In addition to its core functionality as a password cracking tool, John the Ripper can be extended with custom plugins and scripts to support additional password cracking methods and password hash formats. It can also be used in conjunction with other tools and techniques, such as rainbow tables and distributed password cracking.

John the Ripper is a powerful tool that can be used for both legal and illegal purposes, so it is important to use it ethically and with the appropriate permissions from network administrators or system owners. As with any password cracking tool, it is important to use John the Ripper responsibly and with the goal of improving the security of systems and networks.

Top of Form

# II. Port Scanning with Nmap

Here we are performing black box testing or Unknown environment testing. Testers have zero knowledge of the environment prior to starting an unknown environment test (sometimes called a black box test). Instead, they approach the test with the same knowledge as an attacker. When testing new applications, they wouldn’t have any prior experience with the application. When testing networks, they aren’t provided any information or documentation on the network before the test. These testers often use fuzzing to check for application vulnerabilities. This has been commonly called a black box test.

**Foot printing:** Network foot printing provides a big-picture view of a network, including the Internet Protocol (IP) addresses active on a target network.

**Fingerprinting:** Fingerprinting then homes in on individual systems to provide details of each. This is similar to how fingerprints identify an individual. Operating system fingerprinting identifies the operating system. For example, is this a Linux system or a Windows system? A fingerprinting attack sends protocol queries or port scans to a server and analyses the responses. These responses can verify that a service is running and often include other details about the operating system because different operating systems often respond differently to specific queries. The “Network Scanners” section described how many scanners do this to identify operating systems.

**Active directory:** Network operating systems commonly use a directory service to streamline management and implement secure authentication. A common directory service use case is to provide secure access to the network. As an example, many organizations use Microsoft Active Directory Domain Services (AD DS). AD DS is a database of objects that provides a central access point to manage users, computers, and other directory objects.

**Ldap:** Lightweight Directory Access Protocol (LDAP) specifies the formats and methods used to query directories, such as Microsoft AD DS. LDAP is an extension of the X.500 standard that Novell and early Microsoft Exchange Server versions used extensively. LDAP uses TCP port 389. LDAP Secure (LDAPS) encrypts data with TLS using TCP port 636. Windows domains use Active Directory, which is based on LDAP. Queries to Active Directory use the LDAP format. Similarly, Unix realms use LDAP to identify objects. LDAP Secure (LDAPS) uses encryption to protect LDAP transmissions. When a client connects with a server using LDAPS, the two systems establish a Transport Layer Security (TLS) session, and TLS encrypts all data sent between the two systems.

**SSO:** Single sign-on (SSO) refers to a user’s ability to log on once and access multiple systems without logging on again. SSO increases security because the user only needs to remember one set of credentials and is less likely to write them down. It’s also much more convenient for users to access network resources if they only have to log on one time. As an example, consider a user who needs to access multiple servers within a network to perform normal work. Without SSO, the user needs to know one set of credentials to log on locally and an additional set of credentials for each of the servers. Many users would write these credentials down to remember them. Alternatively, in a network with SSO capabilities, the user only needs to log on to the network once. The SSO system typically creates some type of SSO secure token used during the entire login session. Each time the user accesses a network resource, the SSO system uses this secure token for authentication. Kerberos includes SSO capabilities in networks. There are also several SSO alternatives used on the Internet. SSO requires strong authentication to be effective. If users create weak passwords, attackers might guess them, giving them access to multiple systems. Some people debate that SSO adds in risks because if an attacker can gain the user’s credentials, it provides the attacker access to multiple systems.

**Kerberos:**

Kerberos is a network authentication mechanism used within Windows Active Directory domains and some Unix environments known as realms. It was originally developed at MIT (the Massachusetts Institute of Technology) for Unix systems and later released as a request for comments (RFC). Kerberos provides mutual authentication that can help prevent on path attacks (also known as man-in-the-middle attacks) and uses tickets to help prevent replay attacks.

Kerberos includes several requirements for it to work properly. They are A method of issuing tickets used for authentication. The Key Distribution Center (KDC) uses a complex process of issuing ticket-granting tickets (TGTs) and other tickets. The KDC (or TGT server) packages user credentials within a ticket. Tickets provide authentication for users when they access resources such as files on a file server. These tickets are sometimes referred to as tokens, but they are logical tokens, not a key fob type of token discussed earlier in the “Something You Have” section. Time synchronization. Kerberos version 5 requires all systems to be synchronized and within five minutes of each other. The clock that provides the time synchronization is used to timestamp tickets, ensuring they expire correctly. This helps prevent replay attacks. In a replay attack, a third-party attempts to impersonate a client after intercepting data captured in a session. However, if an attacker intercepts a ticket, the timestamp limits the amount of time an attacker can use the ticket. A database of subjects or users. In a Microsoft environment, this is Active Directory, but it could be any database of users. When a user logs on with Kerberos, the KDC issues the user a ticket granting ticket, which typically has a lifetime of 10 hours to be useful for a single workday. When users try to access a resource, they present the ticket- granting ticket as authentication, and the user is issued a ticket to access the resource. However, the ticket expires if users stay logged on for an extended period, such as longer than 10 hours. This prevents them from accessing network resources. In this case, users may be prompted to provide a password to renew the ticket-granting ticket, or they might need to log off and back on to generate a new ticket-granting ticket. Additionally, Kerberos uses symmetric-key cryptography to prevent unauthorized disclosure and to ensure confidentiality.

**Scenario :**

For this scenario we have taken a cloud based Windows 7 Professional 7601 machine as the victim machine and created a ParrotOS virtual machine as the attacker machine.

We established the connection between these two machines using OpenVPN software, which created a network tunnel for the transmission of encapsulated data between the two machines.

What is tunnelling?

In the physical world, tunnelling is a way to cross terrain or boundaries that could not normally be crossed. Similarly, in networking, tunnels are a method for transporting data across a network using protocols that are not supported by that network. Tunnelling works by encapsulating packets: wrapping packets inside of other packets. (Packets are small pieces of data that can be re-assembled at their destination into a larger file.)

Tunnelling is often used in virtual private networks (VPNs). It can also set up efficient and secure connections between networks, enable the usage of unsupported network protocols, and in some cases allow users to bypass firewalls.

A picture containing diagram

Description automatically generated

**Tools/Software used:**

VirtualBox – For the attacker machine

OpenVPN – Establishing connection between host and client

Nmap – For port scanning

JohnTheRipper – Cracking hashes

Kerbrute: A tool to quickly bruteforce and enumerate valid Active Directory accounts through Kerberos Pre-Authentication.

Impacket: Impacket is a collection of Python classes for working with network protocols. Impacket is focused on providing low-level programmatic access to the packets and for some protocols (e.g. SMB1-3 and MSRPC) the protocol implementation itself. Packets can be constructed from scratch, as well as parsed from raw data, and the object-oriented API makes it simple to work with deep hierarchies of protocols. The library provides a set of tools as examples of what can be done within the context of this library.

**Scripts Used:**

GetNPUsers.py: This script will attempt to list and get the TGTs for the users that have the property ‘Do not require Kerberos preauthentication’ set (UF\_DONT\_REQUIRE\_PREAUTH)

Secretsdump.py: This script dumps the NTLM hashes associated with the account.

Psexec.py: It allows us to execute a fully interactive shell on remote windows machines.

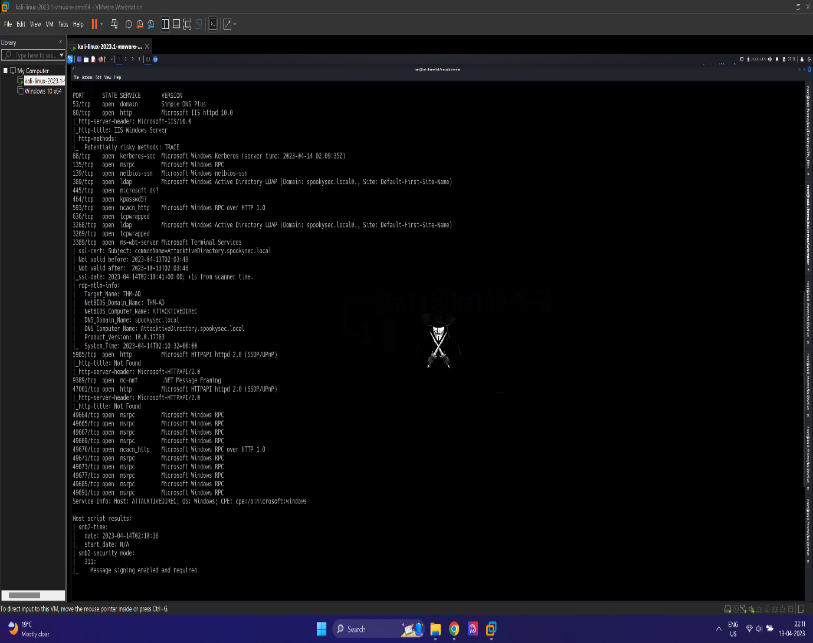
We have made step-by-step process for the exploitation:

Step 1: In the first step we will perform the active footprinting of the network. We start with Nmap scan of the network.

A screenshot of a computer

Description automatically generated with medium confidence

Step 2: Here from the results of the nmap scan we can see that port 389 which is ldap port is active which brings us to the conclusion that the IP address: 10.10.21.225 is associated with a Domain controller.



Step 3: After the active footprinting of the network we can start by enumeration the domains associated with the domain controller for this we will use a tool called kerbrute which runs on go language, here we have used the users.txt wordlist for enumeration of the accounts in the AD

A screenshot of a computer

Description automatically generated with medium confidence

Step 4: After we get the usernames, we focus on the user svc-admin. What we did now is bypass the AS (Authentication service) in Kerberos and directly query the TGS (ticket granting service) with a valid TGT to get the service hash associated with svc-admin. After we get the AS-REP hash we crack it johntheripper offline. Here we cracked the hash offline due to the account lockout policy in Kerberos. For cracking the password we have used the passwd.txt for the dictionary attack.

A screenshot of a computer

Description automatically generated

After we get the password, we list all the SMB shares using ‘smbclient -L’ which lists all the share after that we went into the backup share and extracted the ‘backup\_credentials.txt’. Upon reading the file we found that it was base64 encoded. After decoding the base64 we found the password associated with the account [backup@spookysec.local](mailto:backup@spookysec.local) which we found in step 3.

Step 5: Here we used another impacket script ‘secretsdump.py’ to dump all the NTLM hashes. We then selected the Administrator hash to gain access to the system

A screenshot of a computer

Description automatically generated with medium confidence

Step 6: Here we use another impacket python script psexec.py to perform a pass-the-hash attack on the DC with username: Administrator. Here we can see that psexec.py has sent a staged payload to get the reverse shell to our machine.

A screenshot of a computer

Description automatically generated with medium confidence

Step 7: Cleared all the logs and application from the system and closed the connection.

References:

* <https://nvd.nist.gov/vuln/detail/cve-2017-0143>
* <https://www.exploit-db.com/>
* <https://nmap.org/book/>
* <https://www.vulnhub.com/>

Video-Link: <https://youtu.be/dytqZmVzPls>

Contribution:

|  |  |  |
| --- | --- | --- |
| Name | SEMO ID | Role |
| Archit Benipal | S02048216 |  |
| Batthula ChandrSekhar Rao | S02049570 |  |
| Prathyusha Musunuri | S02052832 |  |
| Yarra Aditya Varma | S02052277 |  |
| KrishnaiahTellagadda | S02050713 |  |
| Rohith Marvathu | S02050694 |  |