

# [REVS] Attacks on Kerberos V in a Windows 2000 Environment

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0097.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 07/23/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 23 Jul 2003 14:03:17 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----  
Attacks on Kerberos V in a Windows 2000 Environment  
-----

## SUMMARY

Kerberos V is a trusted third-party authentication mechanism designed for TCP/IP networks. It uses strong symmetric cryptography to enable authentication in an insecure network. Microsoft introduced Kerberos V as the authentication mechanism for Windows 2000. It is used in many networking applications. An example is SMB, which is a protocol used for file and print services. In this paper, we discuss attacks against Kerberos V that enable retrieving passwords and stealing users' identities on the local network. SMB is used as an example in one of the attacks. We also discuss Windows 2000 implementation specifics that affect the feasibility of these attacks.

## DETAILS

Introduction:

Kerberos was developed at MIT as a part of Project Athena. It is based on a key distribution model invented by Roger Needham and Michael Schroeder.

## Securiteam: [REVS] Attacks on Kerberos V in a Windows 2000 Environment

Symmetric cryptography and a trusted third party are the basis of this authentication mechanism. There have been two versions of the protocol in public use, namely Kerberos IV and V. In this paper we discuss only Kerberos V, which has multiple advantages over the previous version.

Kerberos V is the authentication mechanism used in Windows 2000. It is used to authenticate users logging into workstations on a domain environment and to other network services. In this paper, we use SMB (Server Message Block) as an example of a protocol that primarily uses Kerberos for authentication in a Windows 2000 domain. SMB is the protocol used for file and print services. The security of Kerberos has been discussed in several papers: see [1] for an example. Possible weak points include password attacks against Ticket-Granting tickets or preauthentication data, replay attacks, attacks against network time protocols (Kerberos requires time synchronization) and malicious client software. In this paper, we focus on the first two scenarios: password attacks and replay attacks. We show that a password attack is feasible, thus allowing the attacker to discover weak user passwords. We use pre-authentication data for this attack. A replay attack is presented with the SMB protocol. This allows an attacker to access file shares with the victim's credentials without actually knowing the password.

The chapters are divided as follows: Chapter 2 includes technical descriptions of the protocols discussed in this paper. Chapter 3 will cover some of the vulnerabilities in the Kerberos V protocol. We discuss the attacks we implemented in chapter 4, and analyze the results of these attacks in chapter 5. Some possible protection mechanisms are described in chapter 6. Finally, in chapter 7, we draw conclusions from the presented results and discuss possible future research.

### ADDITIONAL INFORMATION

The complete article is available from:

[http://www.hut.fi/~autikkan/kerberos/docs/phase1/pdf/LATEST\\_final\\_report.pdf](http://www.hut.fi/~autikkan/kerberos/docs/phase1/pdf/LATEST_final_report.pdf)  
[http://www.hut.fi/~autikkan/kerberos/docs/phase1/pdf/LATEST\\_final\\_report.pdf](http://www.hut.fi/~autikkan/kerberos/docs/phase1/pdf/LATEST_final_report.pdf)

The information has been provided by <mailto:kimmo.kasslin@hut.fi> Kimmo Kasslin and <mailto:antti.tikkanen@hut.fi> Antti Tikkanen.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

## Securiteam: [REVS] Attacks on Kerberos V in a Windows 2000 Environment

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.