

Windows 2000, Null Sessions and MSRPC

- Todd Sabin
- BlackHat Windows 2000, Feb. 2001

About Me

**Todd Sabin- RAZOR Team, Bindview
HackerShield vulnerability scanner**

Discovered NT vulnerabilities

- **SYSKEY keystream reuse**
- **LPC issues**

Written various utilities

- **Pwdump2**
- **Lsadump2**
- **Strace for NT**

Agenda

- Review
 - Wksta, Srv
 - LSA
 - SAM
- What's new in W2K
- MSRPC
- Countermeasures
- Q&A

What is a Null Session?

- ❑ Talking to a machine anonymously?
- ❑ “Authenticating” without credentials
 - ❑ not the Guest account
 - ❑ NT grants you
 - ❑ NT AUTHORITY\ANONYMOUS
 - ❑ Everyone (unless RA=2)
- ❑ Used by the SYSTEM account on NT4
- ❑ [c:\] net use \\a.b.c.d\ipc\$ "" /user: ""

What do you get

- ❑ **Browser lists - lots of domain info**
 - ❑ netviewx
- ❑ **Workstation svc**
 - ❑ Transports
- ❑ **Server svc**
 - ❑ Shares
 - ❑ Transports
- ❑ **Carvdawg's null.pl**

What do you get (cont.)

- ❑ **SAM**
 - ❑ **Password policy (“User Modals”)**
 - ❑ **Users**
 - ❑ **Groups (“Global Groups”)**
 - ❑ and members
 - ❑ **Aliases (“Local Groups”)**
 - ❑ and members
 - ❑ **User Info**
 - ❑ passwd change date, account flags (disabled, etc), allowed wksta, ...
 - ❑ **Tool: dumpacl**

What do you get (cont.)

- **LSA**
 - **Policy info**
 - Domain
 - Role
 - Trusts
 - **SID<-->Name mappings**
 - sid2user, user2sid
 - **Walking the SIDs 1000-?**
 - when to stop

What about Win2k?

- Professional, non DC Servers
 - More or less = NT4
- Add SMB over TCP 445
- new RestrictAnonymous = 2 option
 - very tight, but compatibility issues

Domain Controllers & Active Directory

- ❑ Things get complicated
- ❑ Factors
 - ❑ Pre-Windows 2000 Compatible Access
 - ❑ RestrictAnonymous
 - ❑ Trust relationships
 - ❑ ACLs on Active Directory objects
 - ❑ Presence of multiple DCs

Domain Controllers & Active Directory (cont.)

- ❑ **Pre-Windows 2000 Compatible Access**
 - ❑ Controls access to SAM calls
 - ❑ LSA still open
 - ❑ May require reboot
- ❑ **RestrictAnonymous=1**
 - ❑ same as NT4
 - ❑ LSA still open
 - ❑ requires reboot

Domain Controllers & Active Directory (cont.)

- ❑ **RestrictAnonymous=2**
 - ❑ **Shuts down everything**
 - ❑ (no longer have Everyone access)
 - ❑ **Backward compatibility problems**
 - ❑ **requires reboot**
- ❑ **Trust relationships**
 - ❑ **Allowing NT4 domains to trust**
- ❑ **Multiple DCs**
 - ❑ **complicates SID walking**

More about MSRPC

- a.k.a. DCE/RPC
- What does the actual work

Protocol breakdown - port 139

RPC Interface

MSRPC

SMB

NBT

TCP

IP

Protocol breakdown - port 445

RPC Interface

MSRPC

SMB

TCP

IP

Microsoft (DCE) RPC protseqs

- Different transport methods
- Primary ones:
 - ncacn_np (SMB)
 - ncacn_ip_tcp (TCP)
 - IP-TCP-MSRPC
 - ncadg_ip_udp (UDP)
 - IP-UDP-MSRPC
 - ncacn_nb_tcp (NBT)
 - IP-TCP-NBT-MSRPC
 - ncacn_http (HTTP)
 - others (ipx, apple talk, etc.)

ncacn_http (COM Internet Services)

- ❑ **RPC over port 80**
- ❑ **proxied by IIS**
 - not installed by default
 - must be explicitly enabled
- ❑ **lets DCOM (and normal RPC) work through firewalls**
- ❑ **somewhat similar to SOAP**

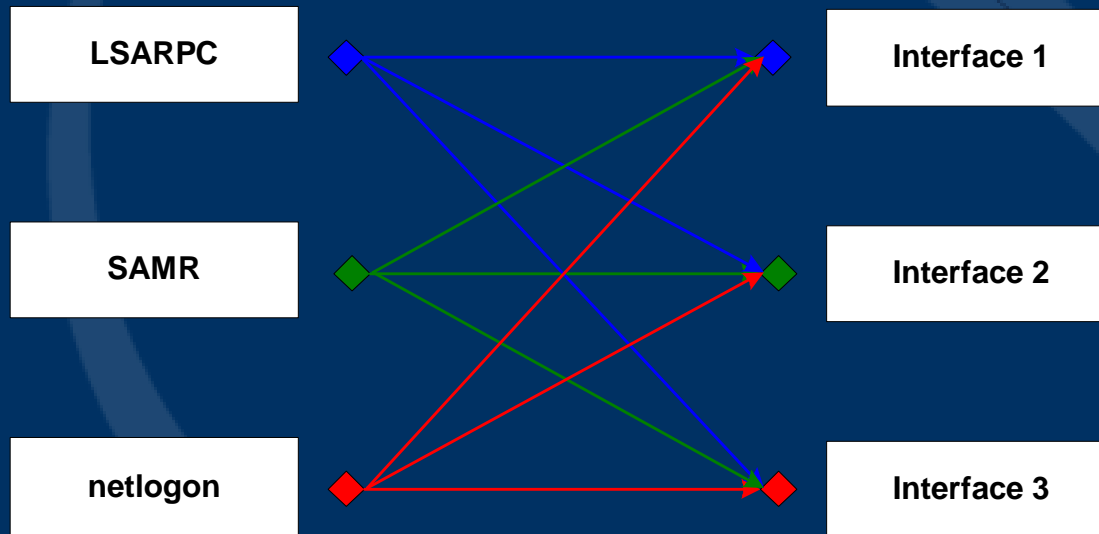
Endpoint Mapper

- ❑ Analagous to portmapper on unix
- ❑ Listens on
 - ❑ TCP 135
 - ❑ UDP 135
 - ❑ NBT 135 (SRVNAME<87>)
 - ❑ SMB “\pipe\epmapper”
 - ❑ HTTP 593
- ❑ rpcdump - Lists dynamically registered endpoints
- ❑ Note: also used for DCOM activation

RPC Management Interface

- ❑ RPC runtime implements
- ❑ All servers support it
- ❑ Provides general info about RPC server
- ❑ `rpc_mgmt_inq_if_ids`:
 - ❑ returns supported RPC interfaces
- ❑ Tool: `ifids`
 - ❑ can be used to identify RPC servers

Endpoints and Interfaces



What about Null Sessions?

- ❑ **Lsass on W2K Domain Controllers**
 - ❑ contains extra RPC servers
 - ❑ listens on:
 - ❑ TCP
 - ❑ UDP
 - ❑ HTTP, if COM Internet Services
- ❑ can enumerate users, etc. over TCP, UDP, possibly HTTP

Countermeasures – Firewalling

- ❑ Prefer default deny
- ❑ Block Endpoint mapper
 - ❑ UDP 135, TCP 135 & 593
- ❑ Block SMB access
 - ❑ TCP 139 & 445; also UDP 137 & 138
- ❑ Block TCP and UDP to RPC range
 - ❑ HKLM\Software\Microsoft\RPC
 - ❑ be careful with DNS
 - ❑ use split DNS
- ❑ Don't install COM Internet Services

Countermeasures – Configuration

- ❑ Unbind NetBIOS from TCP/IP
- ❑ Disable Server service
- ❑ RestrictAnonymous=1, or 2
- ❑ Pre-Windows 2000 Compatible Access
 - ❑ Remove “Everyone”

Countermeasures – ACLs

- ❑ Active Directory - ACLs on objects, properties, etc.
- ❑ What about non-AD machines?
- ❑ LSA and SAM object hierarchies
 - ❑ can still set ACLs on objects, but need special tools
 - ❑ Fixpol
 - ❑ Samacl & Isaac1
- ❑ No reboots required
- ❑ Downside: 'invisible' change somewhat dangerous

Summary

- ❑ Defaults favor attackers
- ❑ Assess - be sure
- ❑ Firewall
- ❑ RestrictAnonymous
- ❑ Tighten ACLs

Questions?

- For followup:
 - <http://razor.bindview.com>
 - tsabin@razor.bindview.com