



BACKSTABBED

abusing disaster recovery systems

hd moore – first2005

Who am I?

Researcher at Digital Defense

- # Managed risk assessments

- # Security code reviews

Founder of the Metasploit Project

- # Created the Metasploit Framework

- # Project manager and exploit developer

What is this about?

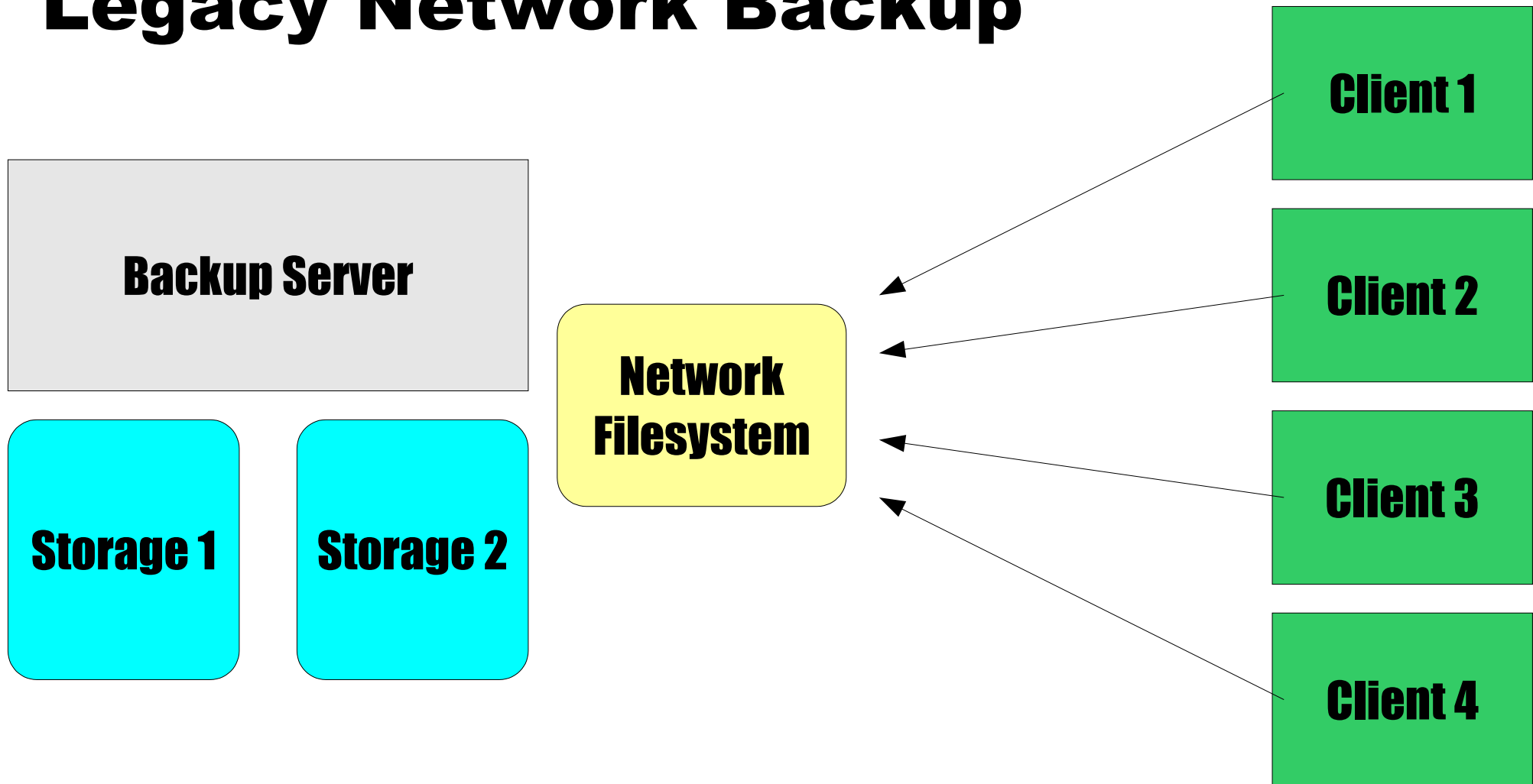
- # Network backup architectures
- # Backup agent discovery services
- # Backup agent vulnerabilities
- # Remotely exploitable flaws (**0day**)

- # **Why does this matter?**
- # Every company need backups
- # Backup software is in a bad state
 - # Requires administrative privileges
 - # Requires architecture changes
 - # Software quality is terrible
- # Attackers are exploiting this **now**

Network Architecture

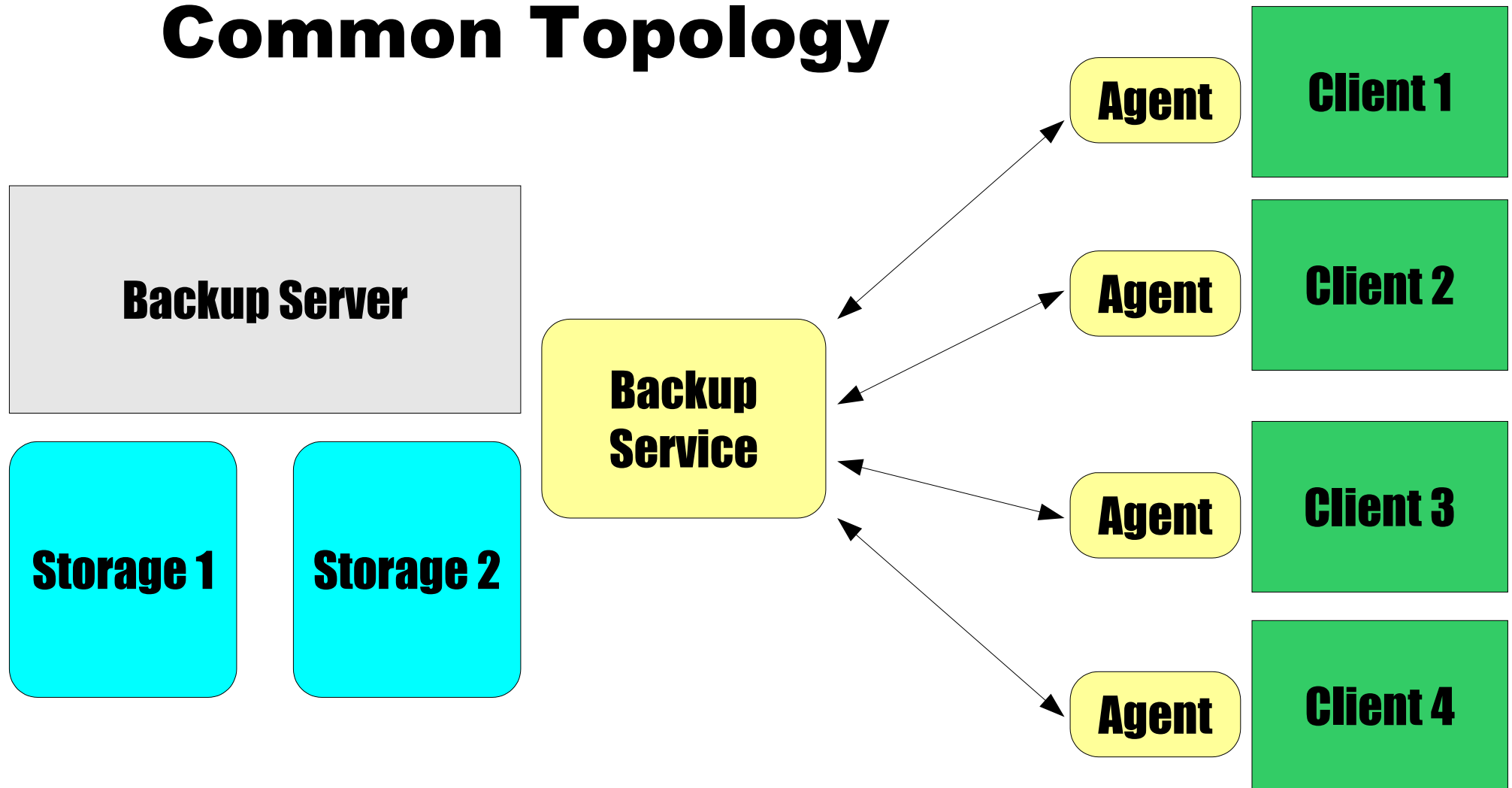
- # **Topologies are changing**
- # Storage requirements increase
- # Bandwidth limits affect backups
- # Network topology is updated...
 - # Efficient is not always secure
 - # Can invalidate internal firewalls

Legacy Network Backup



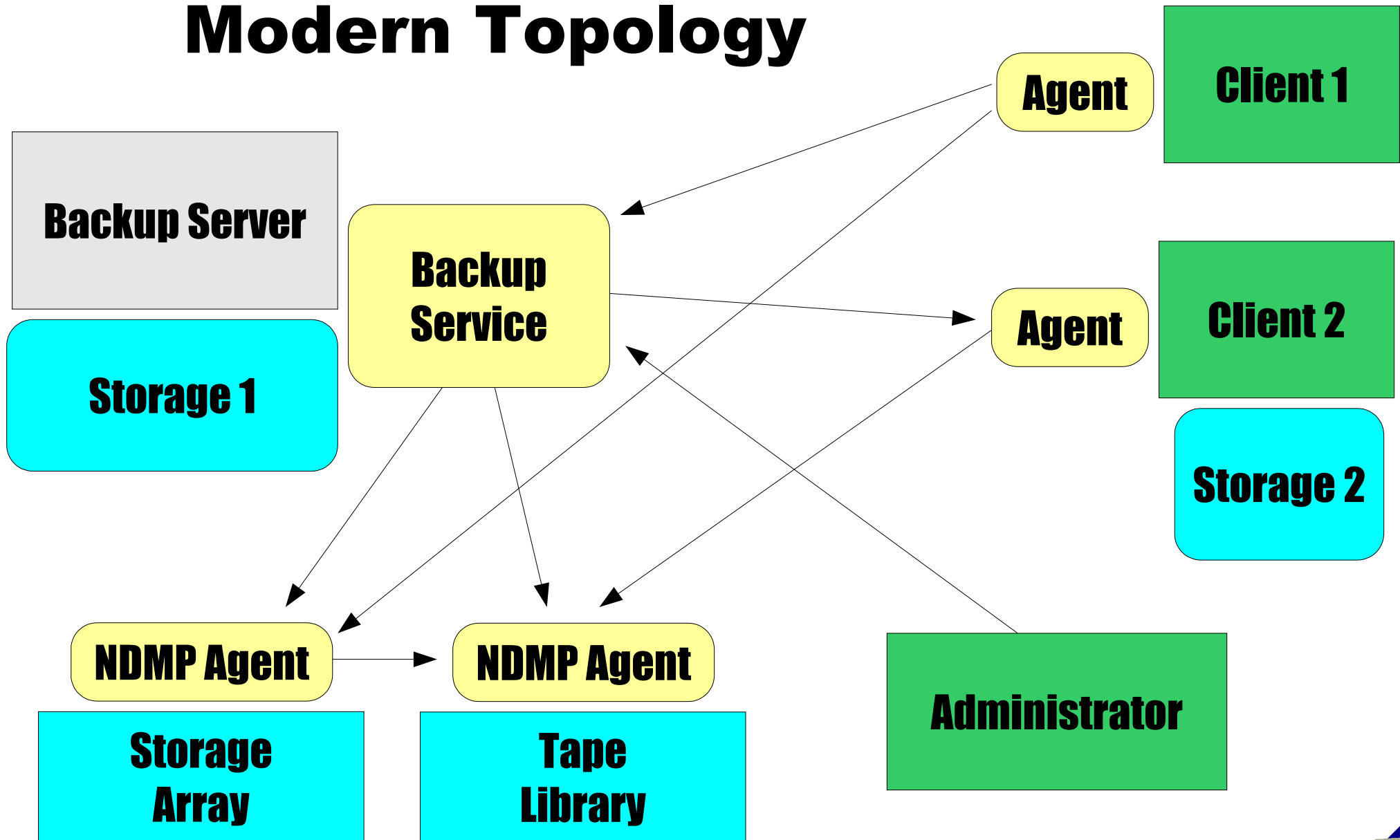
Client systems copy data to a central network file system

Common Topology



Client backup agents communicate with the backup server

Modern Topology



Admin connects to backup server, everything else cross-connects

- # **Distributed backup systems**
 - # Storage distributed across network
 - # Clients talk to storage devices
 - # Traffic between agents is common
 - # Each vendor has their own protocol
 - # Many are firewall “compatible” ...

Network Data Management

- # NDMP is an interoperability std.
- # Great firmware/hardware support
- # Software support via plugins
- # Extensive remote command set:

NDMP_CONFIG_GET_HOST_INFO, NDMP_TAPE_READ,
NDMP_CONNECT_OPEN, NDMP_LOG_FILE,
NDMP_MOVER_CONNECT, NDMP_TAPE_OPEN,
NDMP_SCSI_OPEN, NDMP_GET_FS_INFO, ...

- # **Access control is a nightmare**
 - # Connections between agents
 - # Connections between devices
- # **Vendors claim app-side security**
 - # Software supports common auth.
 - # Devices can auth against servers

Discovery Services

Discovery services

- # Each vendor has their own proto.
- # Easily find backup clients/servers
- # Integrated into GUI admin tools
- # Used to perform status checks
- # Often expose system information

Discovery protocols

- # UDP broadcast is most common
- # DNS and NetBIOS used as well
- # Some products scan the network
- # SNMP also for discovery

- # **Anything the software can do...**
 - # Find servers, agents, and devices
 - # Obtain system and version info
 - # Automated exploitation is easy...
 - # Definitely a potential for worms
 - # Automated “bots” more likely

Veritas BackupExec

- # Exposes vendor and version

CA BrightStor ARCserve

- # Leaks operating system and version

Knox/Arkeia Network Backup

- # Leaks system information and version

Backup Agents

- # **We all know defaults are bad...**
- # Default agent settings are terrible
- # Security docs are hard to find
- # Installation docs rarely mention it
- # Agent install is often automated
- # Awareness is simply not there!

- # **Configuring a new client agent**
 - # The admin installs a client agent
 - # The agent and server need to talk
 - # Who authenticates to who?
 - # Each vendor does this different
 - # One-way auth is a huge problem

- # **Veritas (Symantec) BackupExec**
 - # Agent makes server authenticate
 - # If the agent address is hijacked...
 - # Unix agents are password-only
 - # Unix agent registration spoofable
 - # Authentication replay is possible

- # **CA BrightStor ARCserve**
 - # Agent makes server authenticate
 - # Similar problems to BackupExec
 - # Backdoor user in the Unix agent
 - # Various heap overflows...

- # **Knox Arkeia Network Backup**
 - # Wide open to the world by default
 - # Read and write any resource
 - # Browse file system, registry, etc
 - # View detailed system information
 - # No authentication, only IP ACL's

Remote Exploits

- # **Exploits affect every vendor**
- # Public code for BackupExec,
BrightStor, ARCserve, NetVault
- # Many of these are simple bugs
- # Immature industry security-wise
- # ..they sell as security products!

- # **No automatic updates...**
- # Patching can be really painful
 - # 7 recent BE patches need reboot
- # Patches not included in releases
 - # CA finally made “service pack 1”
- # Evals often way behind patches
 - # “Upgrading” eval doesn't patch...

- # **Backup software at risk now**
- # About 7 new flaws in BackupExec
 - # At least 5 serious unpublished bugs
- # NetVault has yet to patch anything
- # CA BrightStor still massively vuln...
 - # At least 3 serious unpublished bugs
- # Arkeia has history of 0day...

- # **Information on Veritas flaws**
 - # Remote overflow in win32 agent
 - # Remote registry access
 - # Many DoS vulnerabilities
 - # Auth bypass in win32 agent
 - # DoS flaws in Unix agent

- # **CA BrightStor/ARCserve users**
 - # Many remotely exploitable flaws
 - # Most of these still unpublished!
 - # Firewalling is not really possible
 - # Other CA services even worse:
 - # The “CA Licensing” fiasco...
 - # Remote “caroot” password retrieval

BakBone NetVault users

- # Run away as fast as you can

- # Over 3 remote 0days and counting...

Arkeia/Knox users

- # Ask Arkeia to add authentication

- # **Handful of DoS vulnerabilities**

Questions?

Contact

hdm@metasploit.com

Code

<http://metasploit.com/>