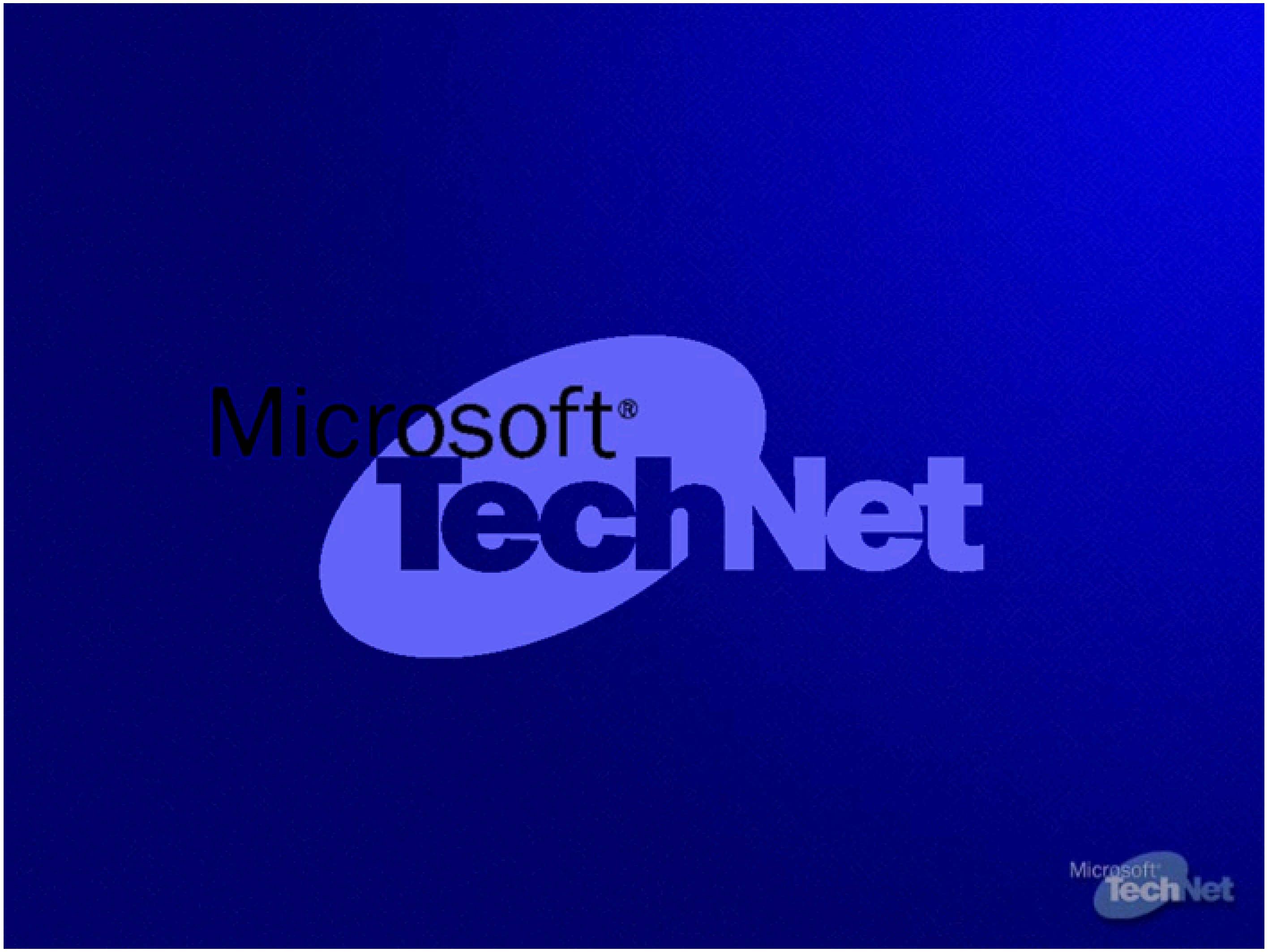
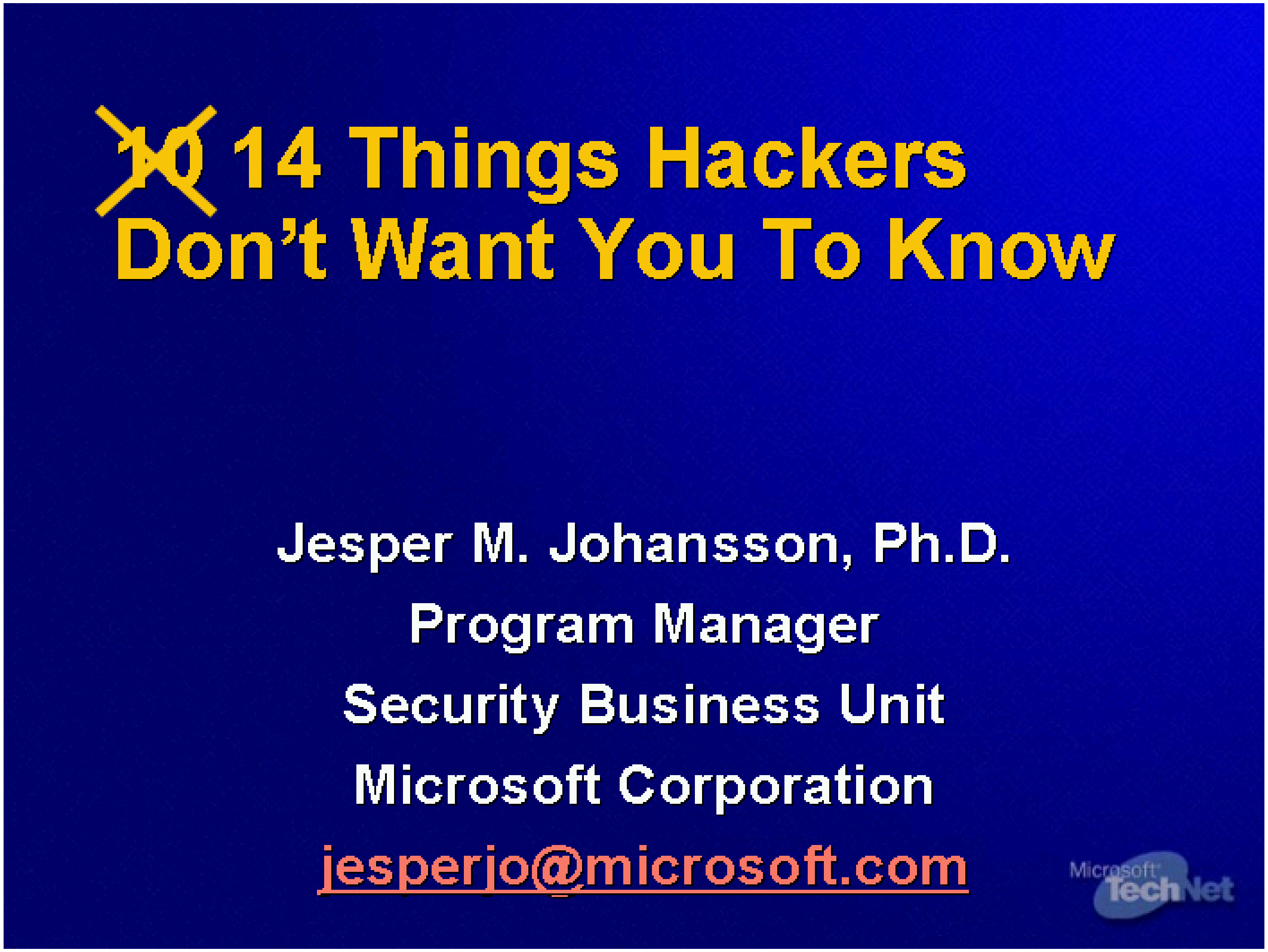


Slide 1



~~10~~ 14 Things Hackers Don’t Want You To Know

Jesper M. Johansson, Ph.D.

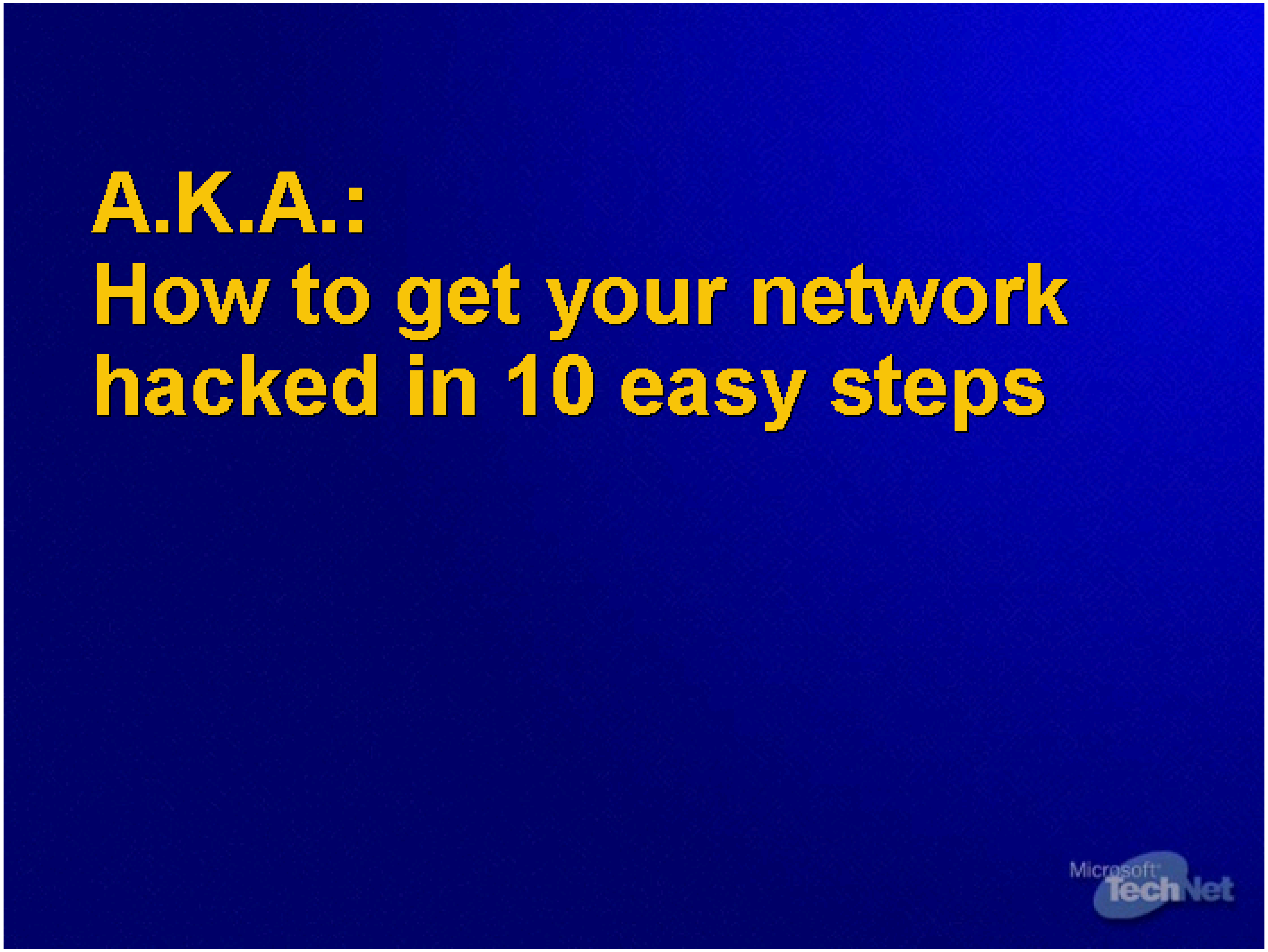
Program Manager

Security Business Unit

Microsoft Corporation

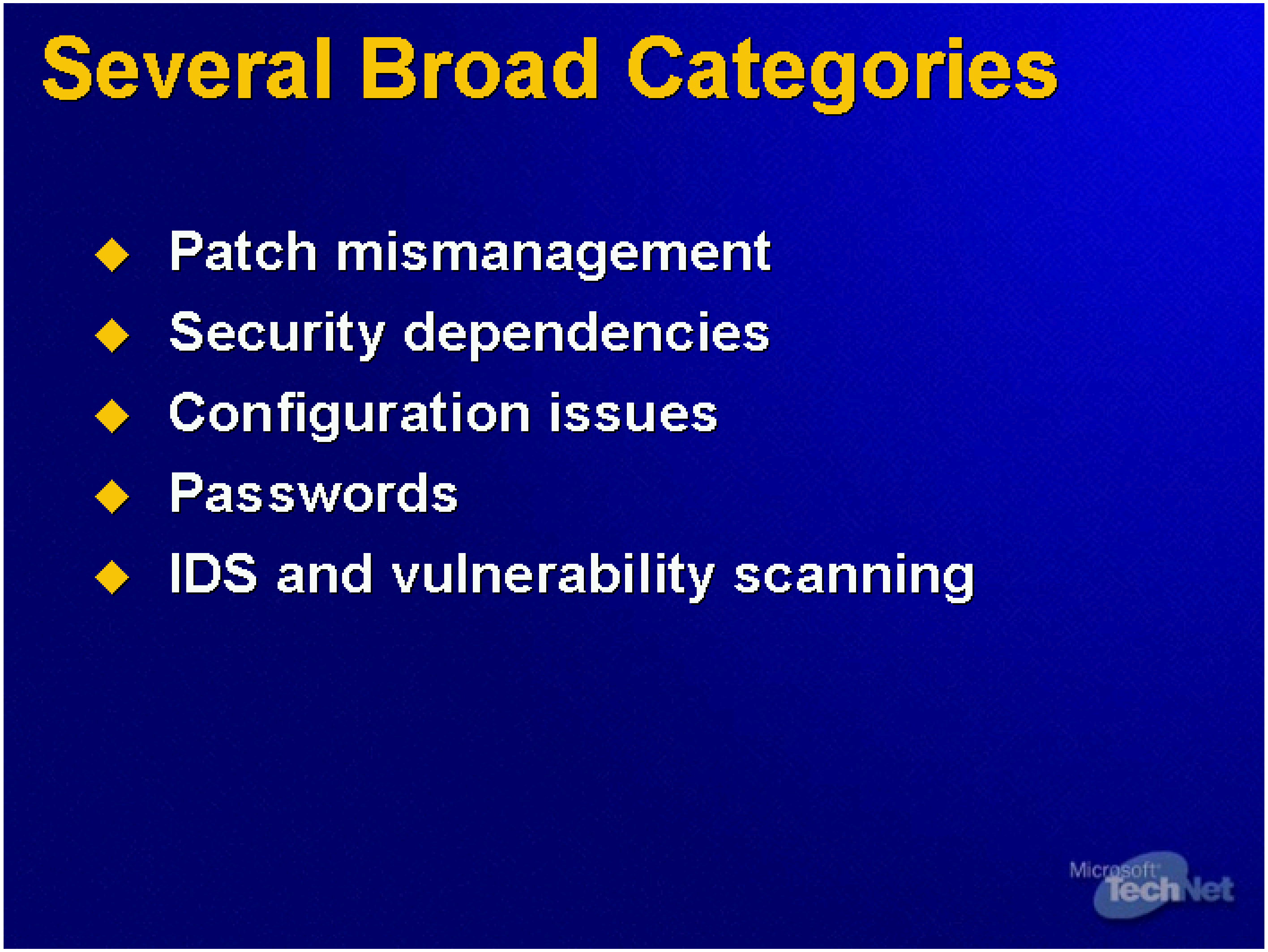
jesperjo@microsoft.com

10 14 Things Hackers Don’t Want You To Know



A.K.A.:
How to get your network hacked in 10 easy steps

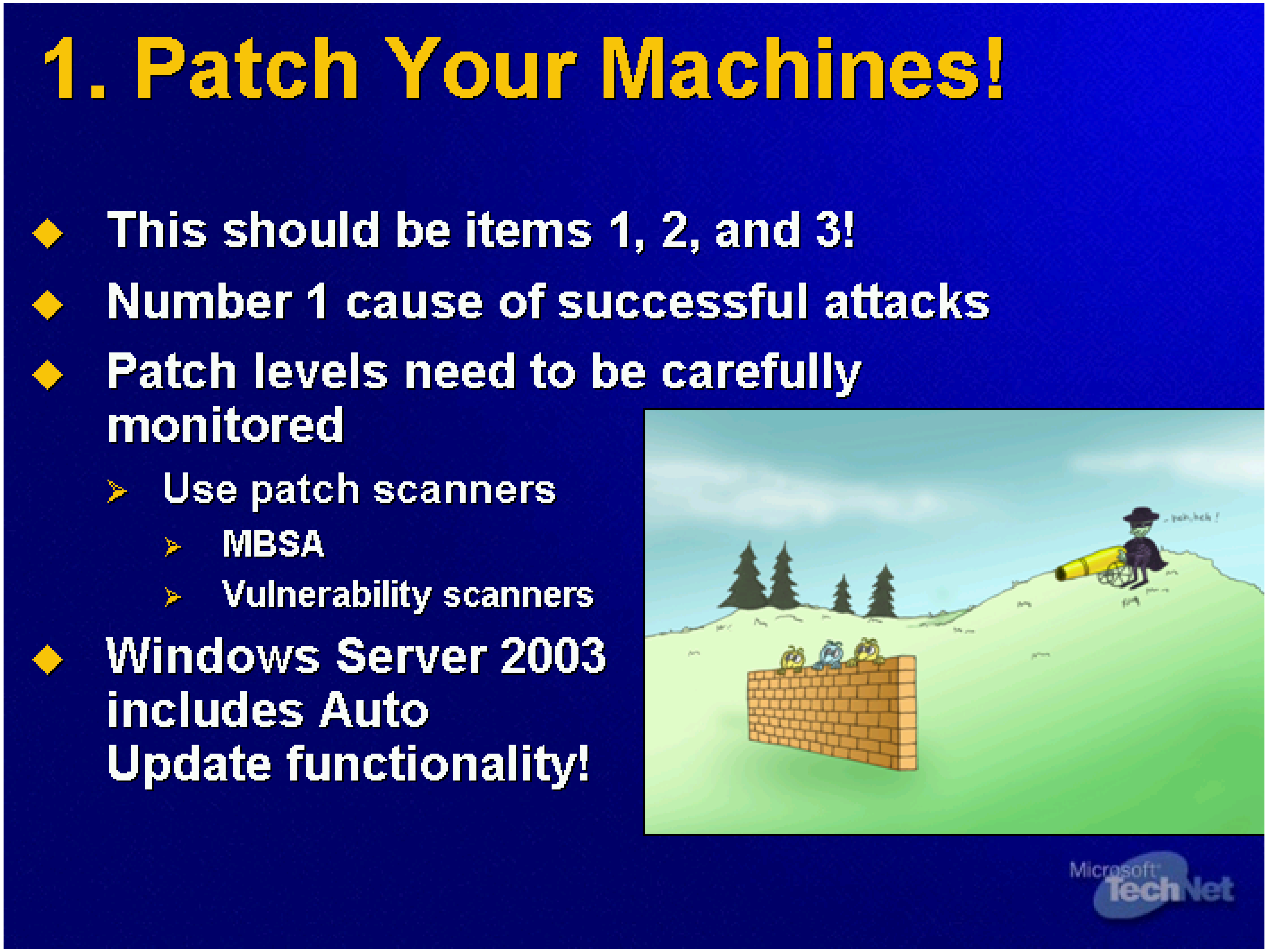
A.K.A.: How to get your network hacked in 10 easy steps



Several Broad Categories

- Patch mismanagement
- Security dependencies
- Configuration issues
- Passwords
- IDS and vulnerability scanning

Several Broad Categories

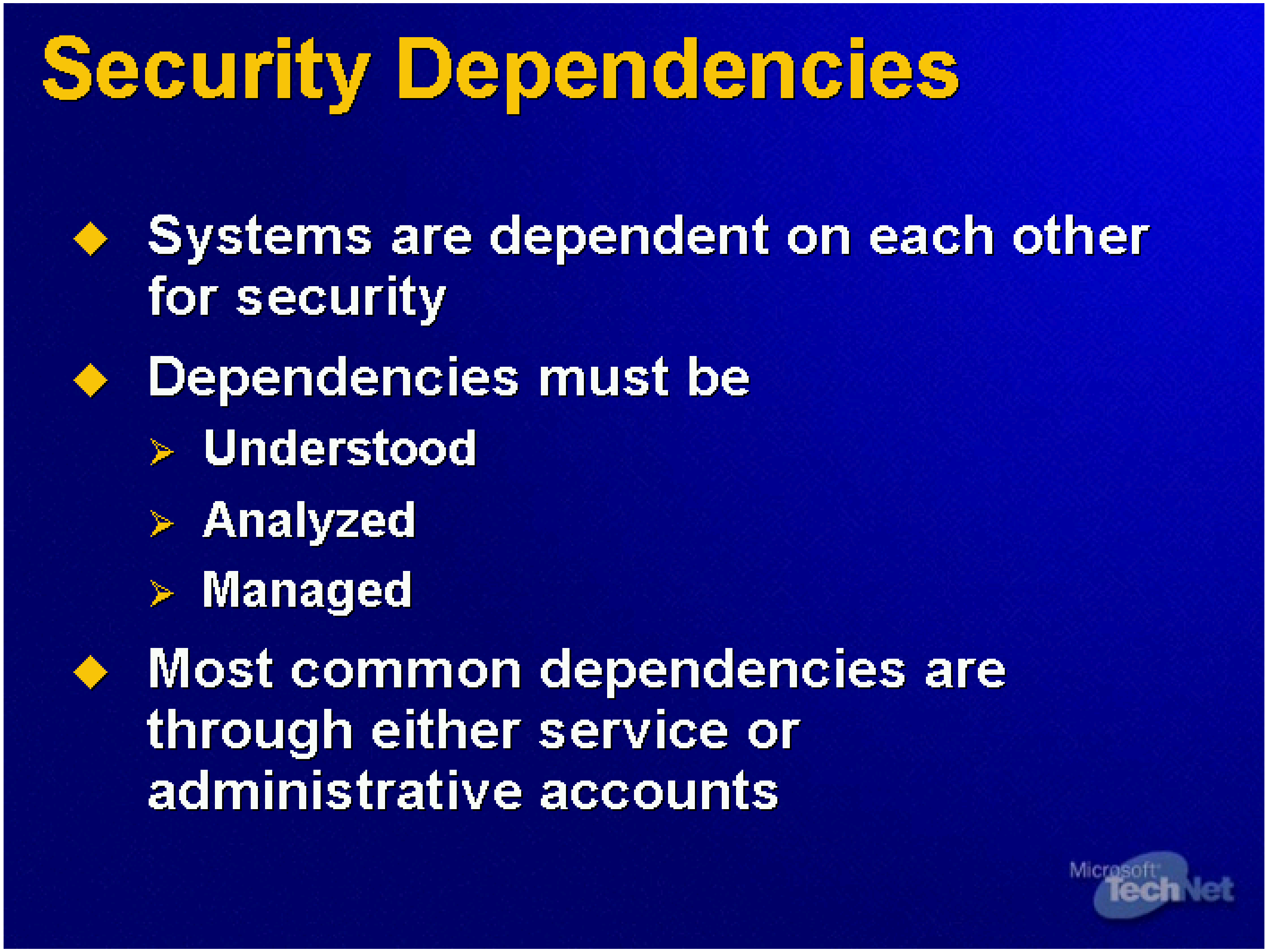


1. Patch Your Machines!

- This should be items 1, 2, and 3!
- Number 1 cause of successful attacks
- Patch levels need to be carefully monitored
  - Use patch scanners
    - MBSA
    - Vulnerability scanners
- Windows Server 2003 includes Auto Update functionality!

heh, heh !
Microsoft TechNet

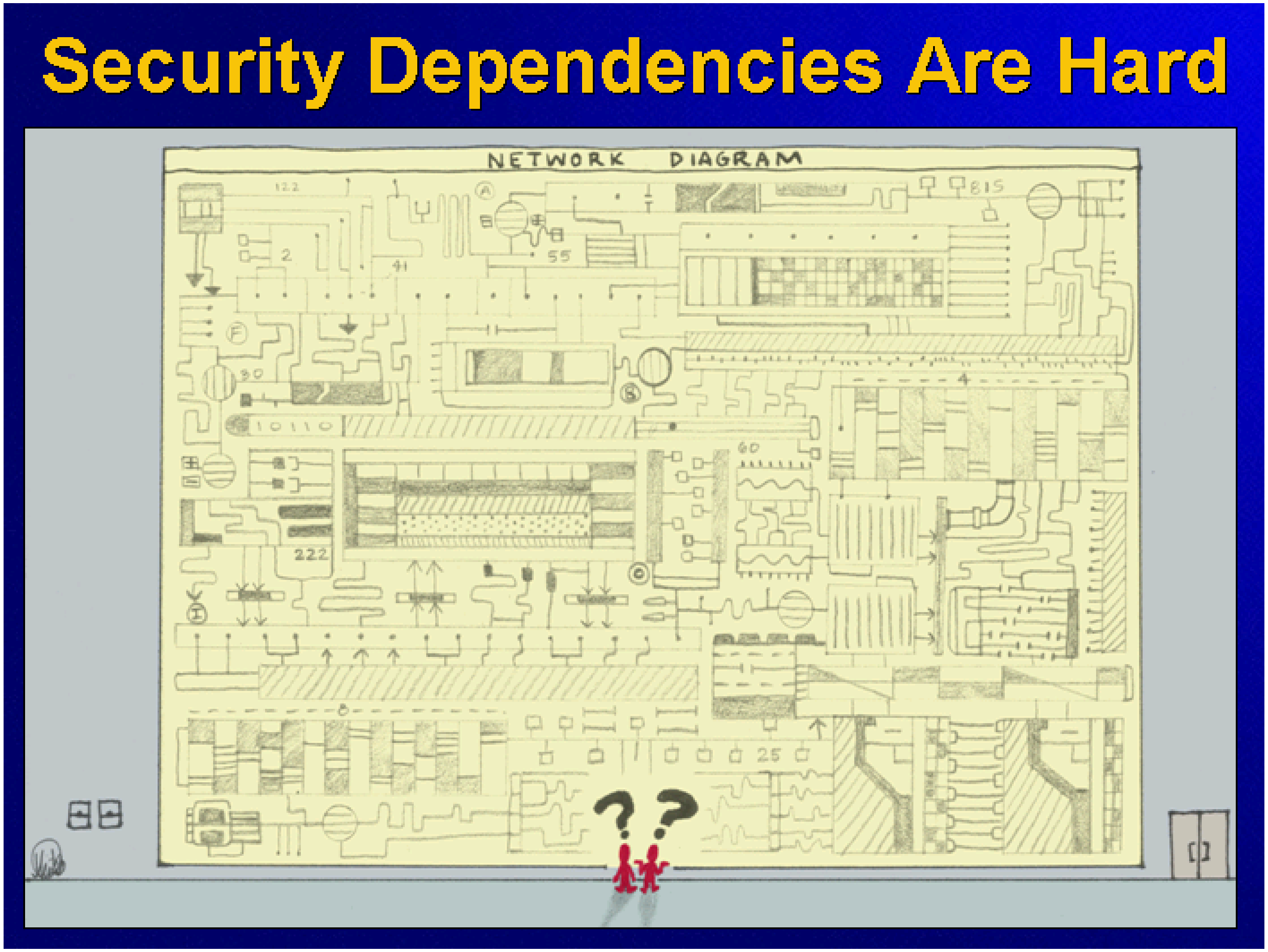
1. Patch Your Machines!



Security Dependencies

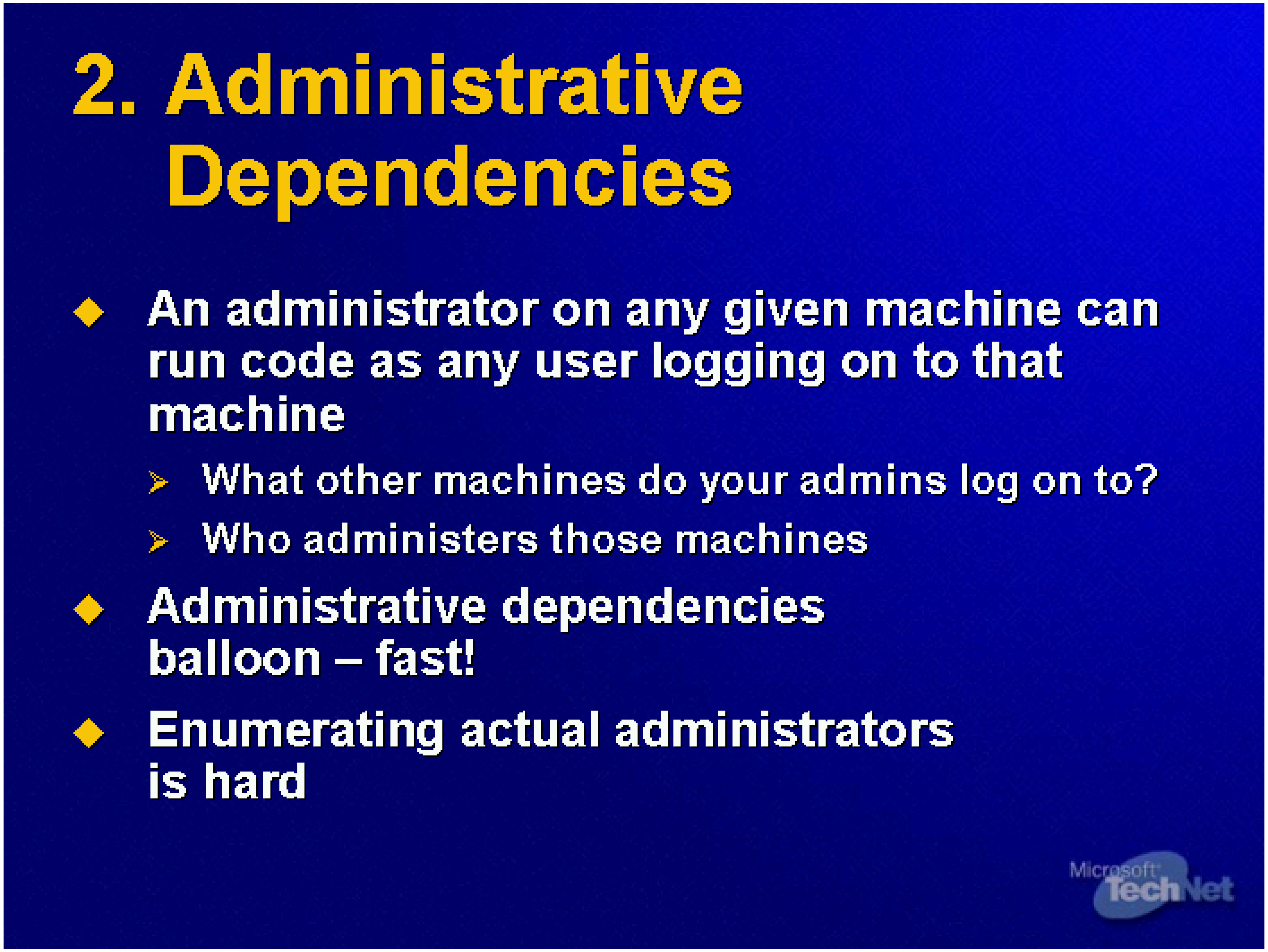
- Systems are dependent on each other for security
- Dependencies must be
  - Understood
  - Analyzed
  - Managed
- Most common dependencies are through either service or administrative accounts

Security Dependencies



Security Dependencies Are Hard

Security Dependencies Are Hard

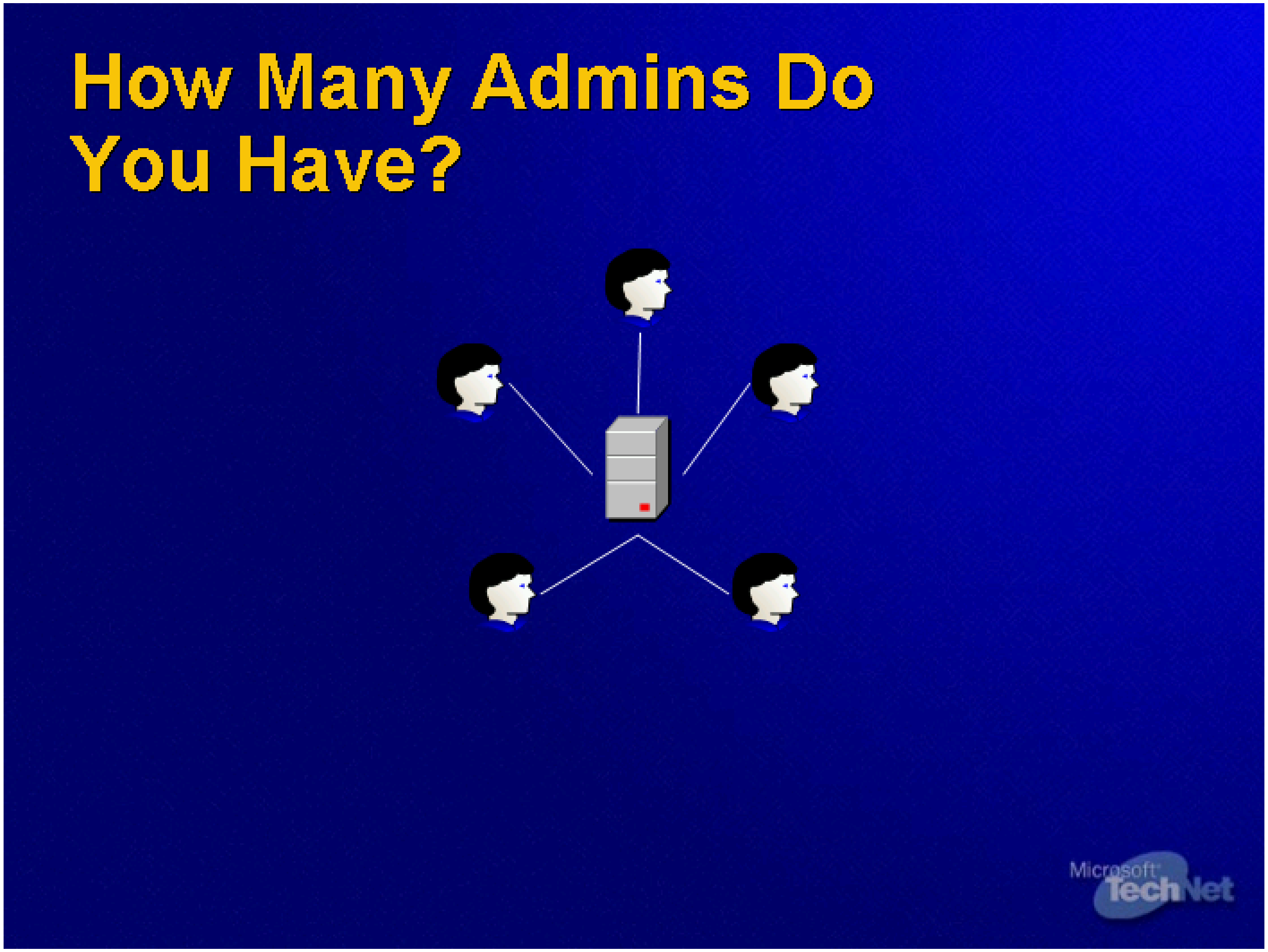


2. Administrative Dependencies

- An administrator on any given machine can run code as any user logging on to that machine
  - What other machines do your admins log on to?
  - Who administers those machines
- Administrative dependencies balloon – fast!
- Enumerating actual administrators is hard

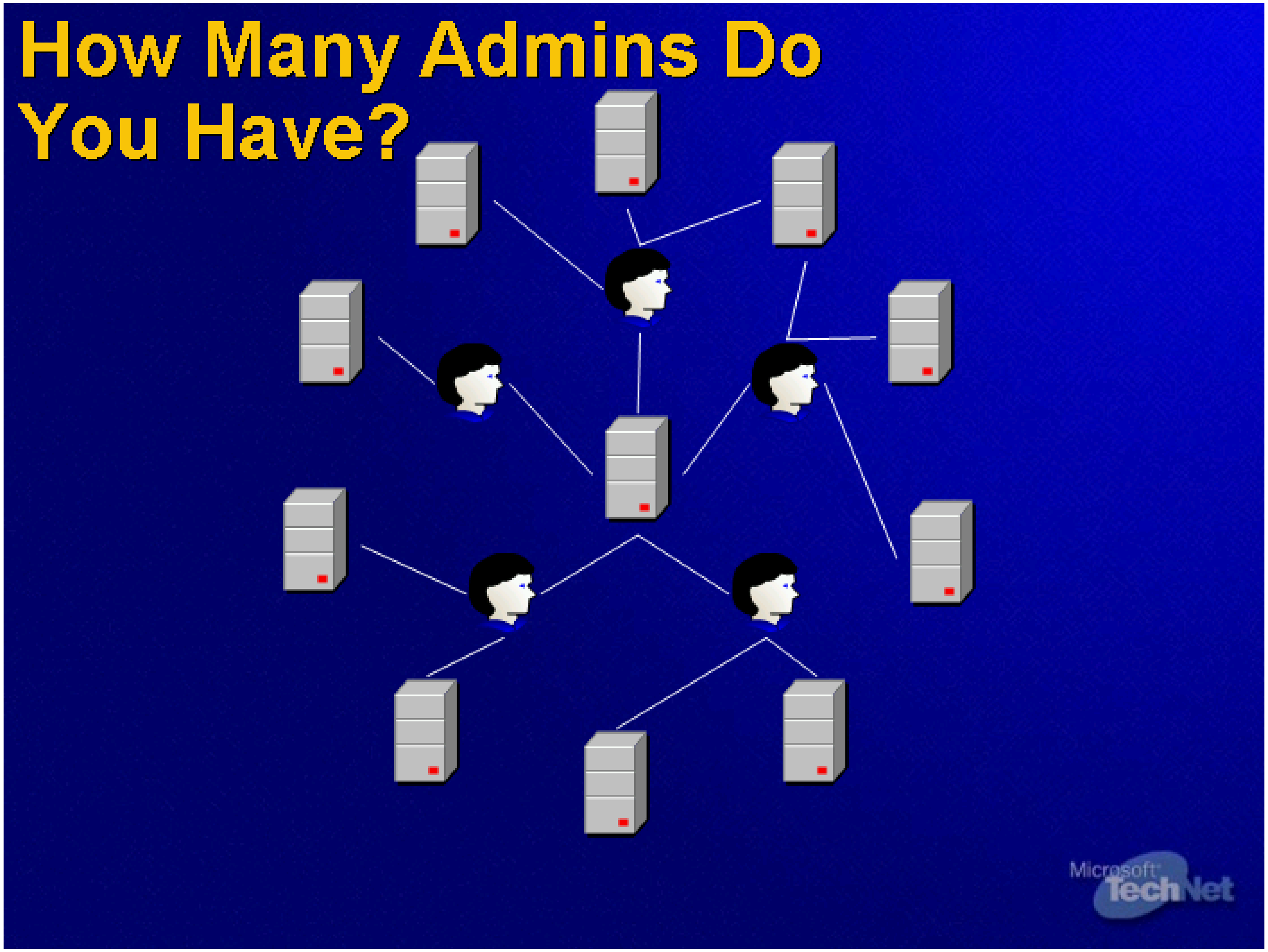
Microsoft TechNet

2. Administrative Dependencies



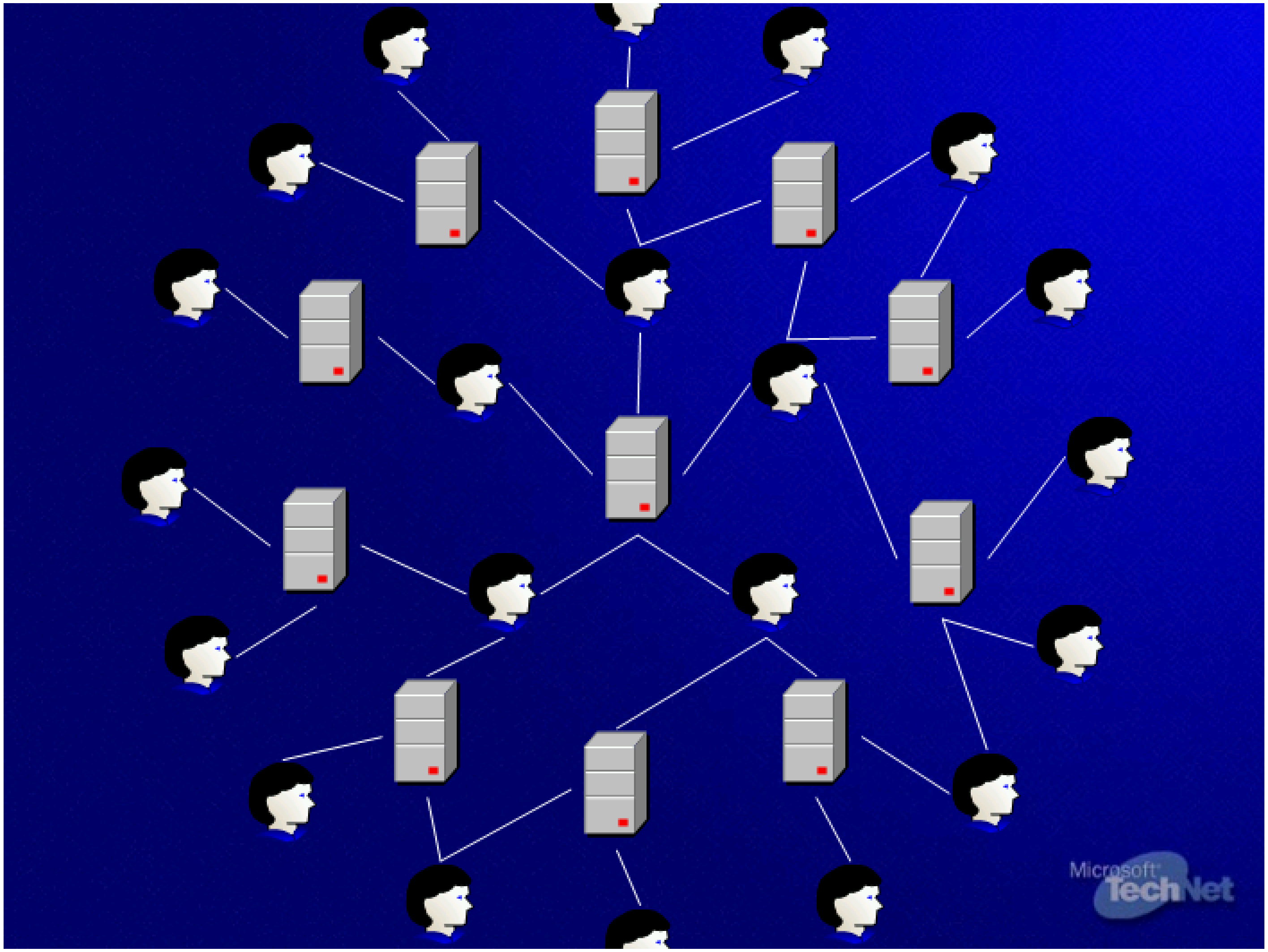
How Many Admins Do You Have?

How Many Admins Do You Have?

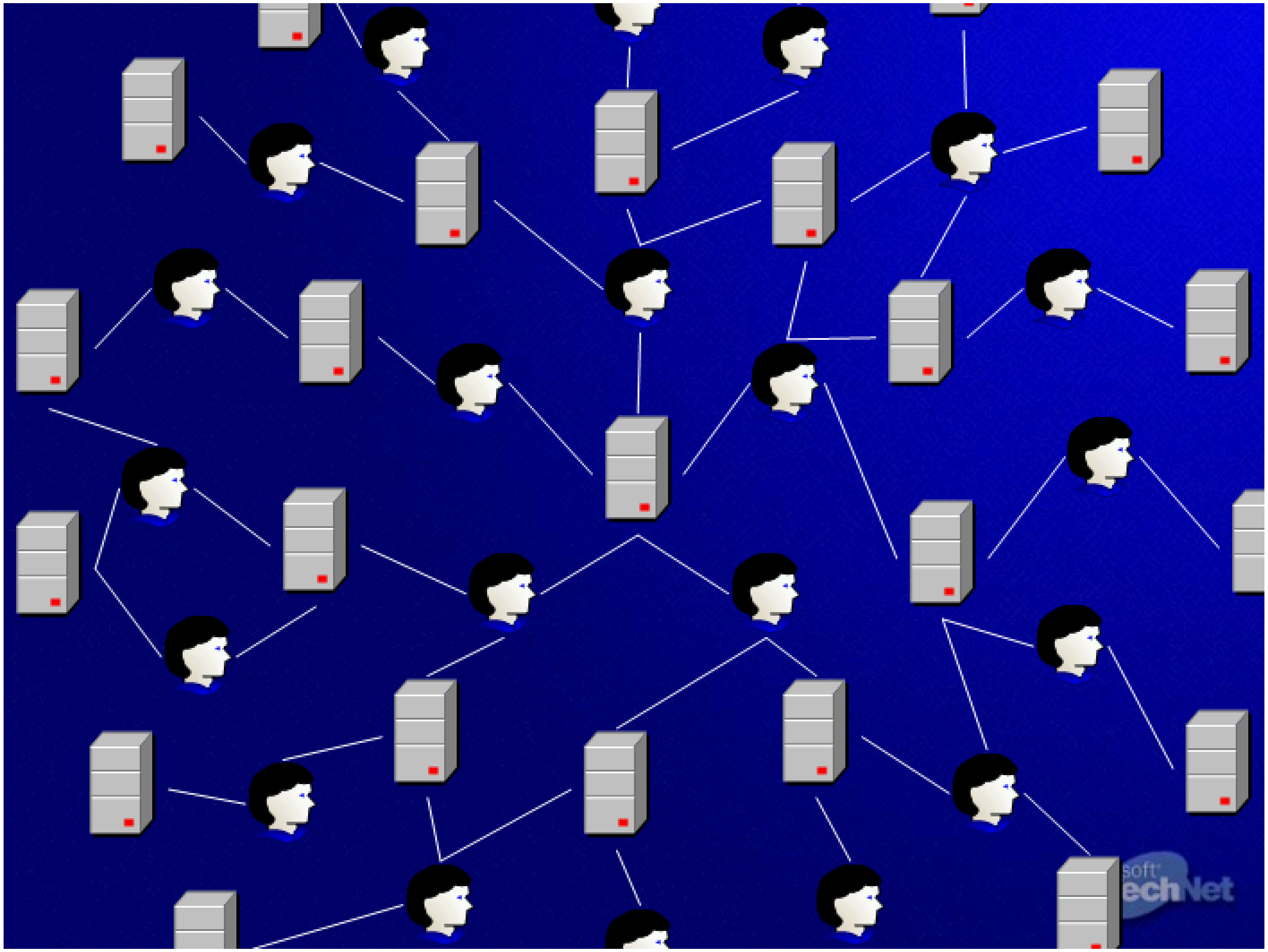


How Many Admins Do You Have?

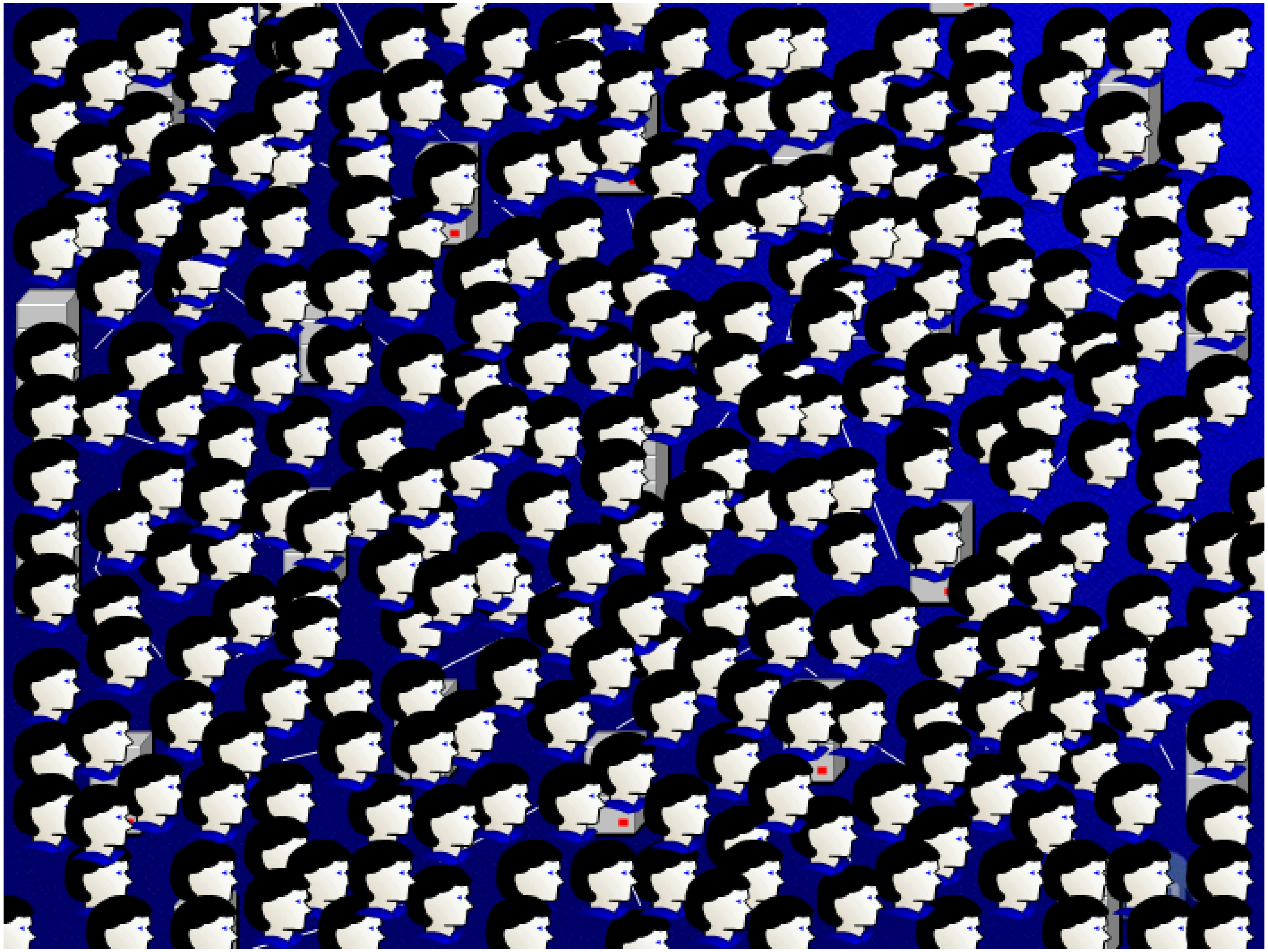
How Many Admins Do You Have?



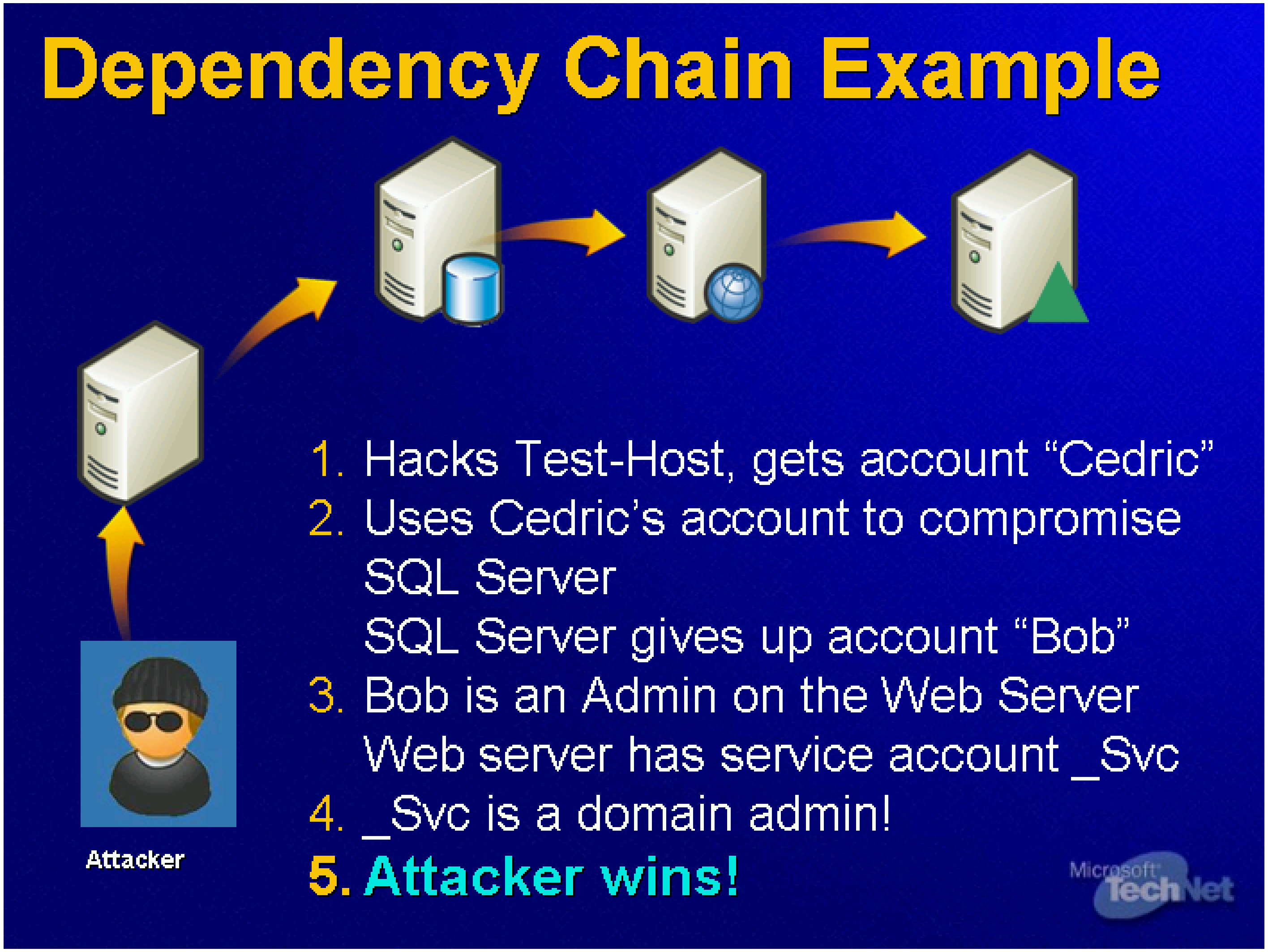
Slide 11



Slide 12



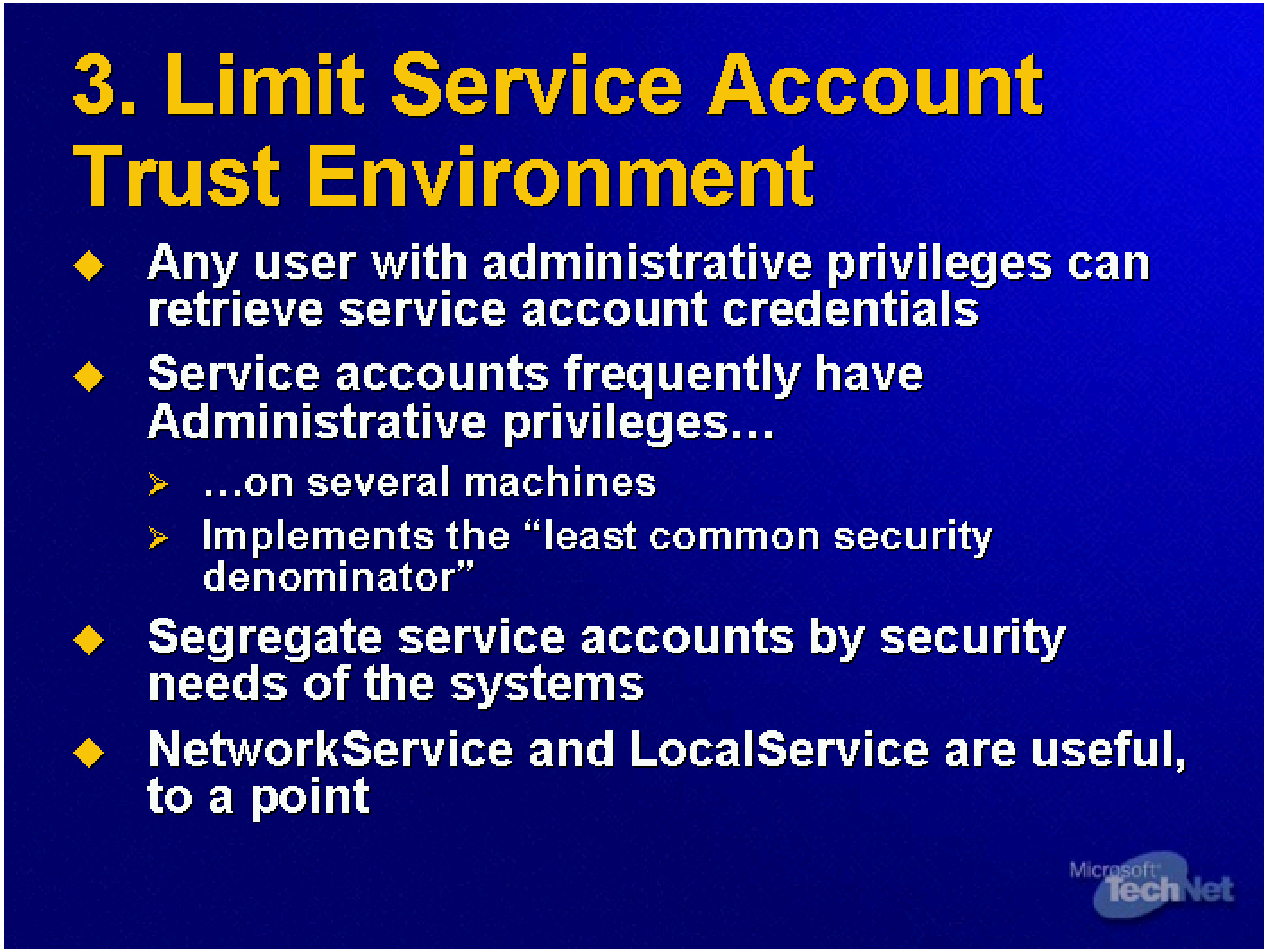
Slide 13



Dependency Chain Example

1. Hacks Test-Host, gets account "Cedric"
2. Uses Cedric's account to compromise SQL Server
   SQL Server gives up account "Bob"
3. Bob is an Admin on the Web Server
   Web server has service account _Svc
4. _Svc is a domain admin!
5. **Attacker wins!**

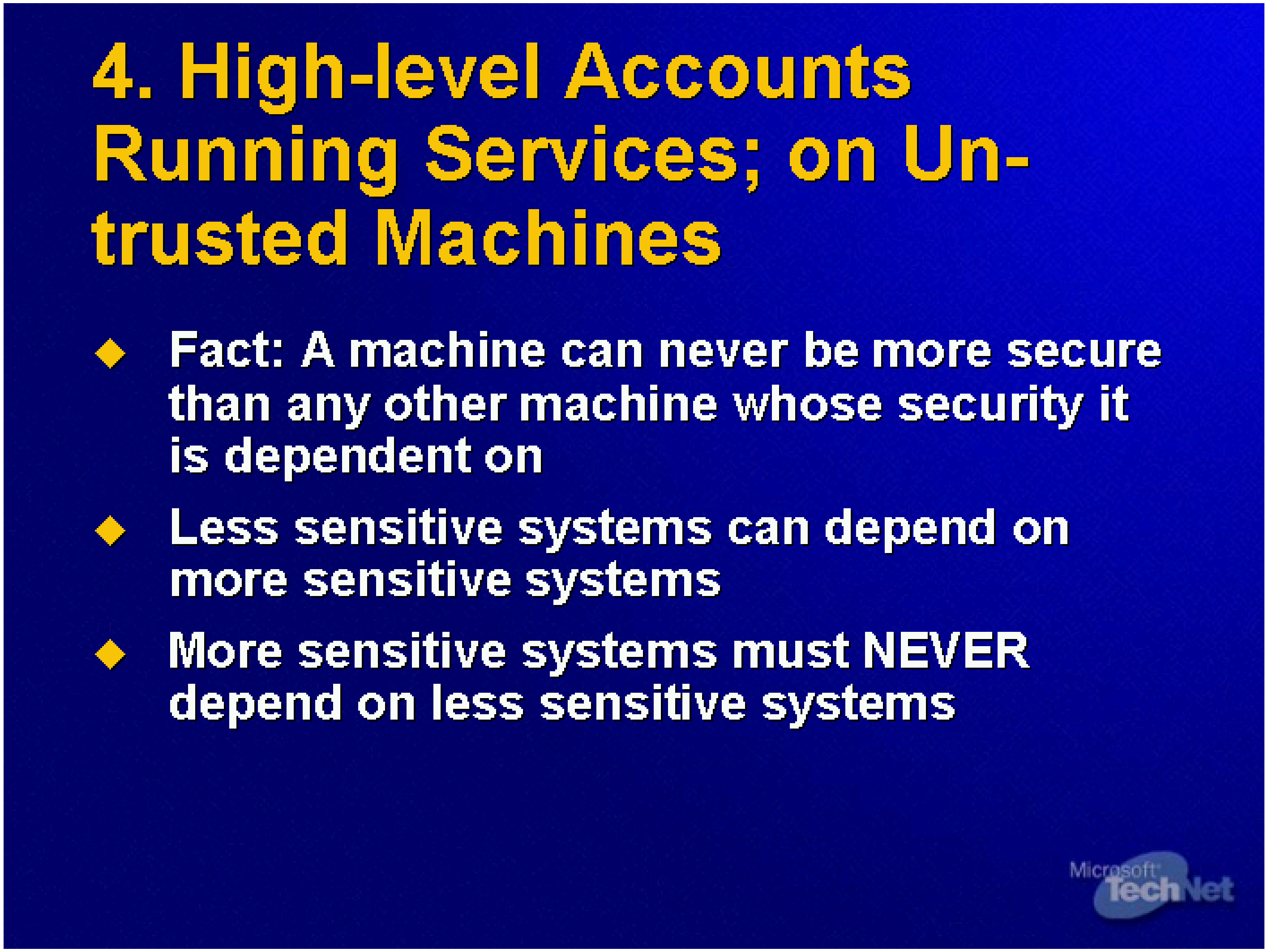
Dependency Chain Example



3. Limit Service Account Trust Environment

- Any user with administrative privileges can retrieve service account credentials
- Service accounts frequently have Administrative privileges…
  - …on several machines
  - Implements the "least common security denominator"
- Segregate service accounts by security needs of the systems
- NetworkService and LocalService are useful, to a point

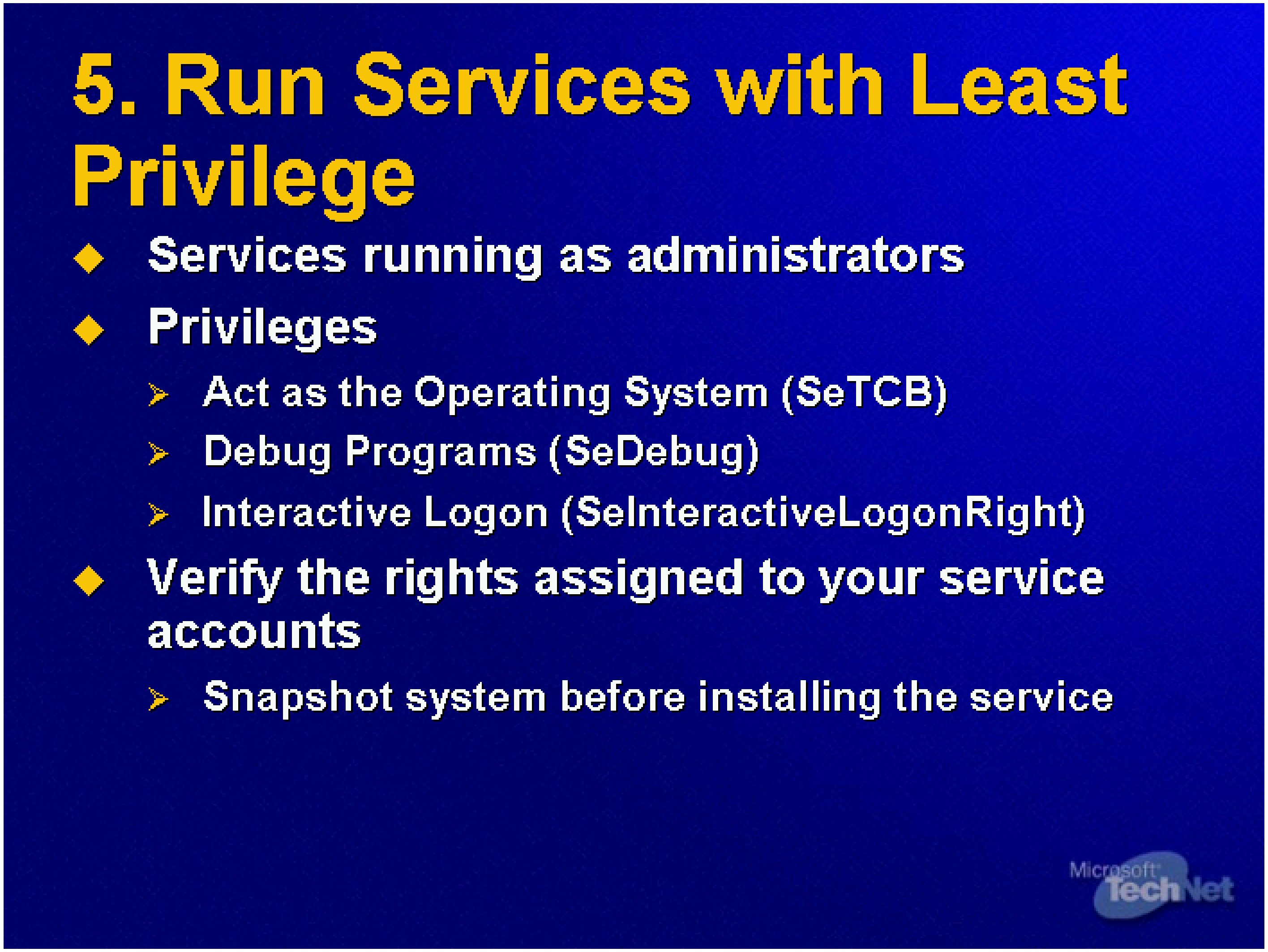
3. Limit Service Account Trust Environment



4. High-level Accounts Running Services; on Un-trusted Machines

- Fact: A machine can never be more secure than any other machine whose security it is dependent on
- Less sensitive systems can depend on more sensitive systems
- More sensitive systems must NEVER depend on less sensitive systems

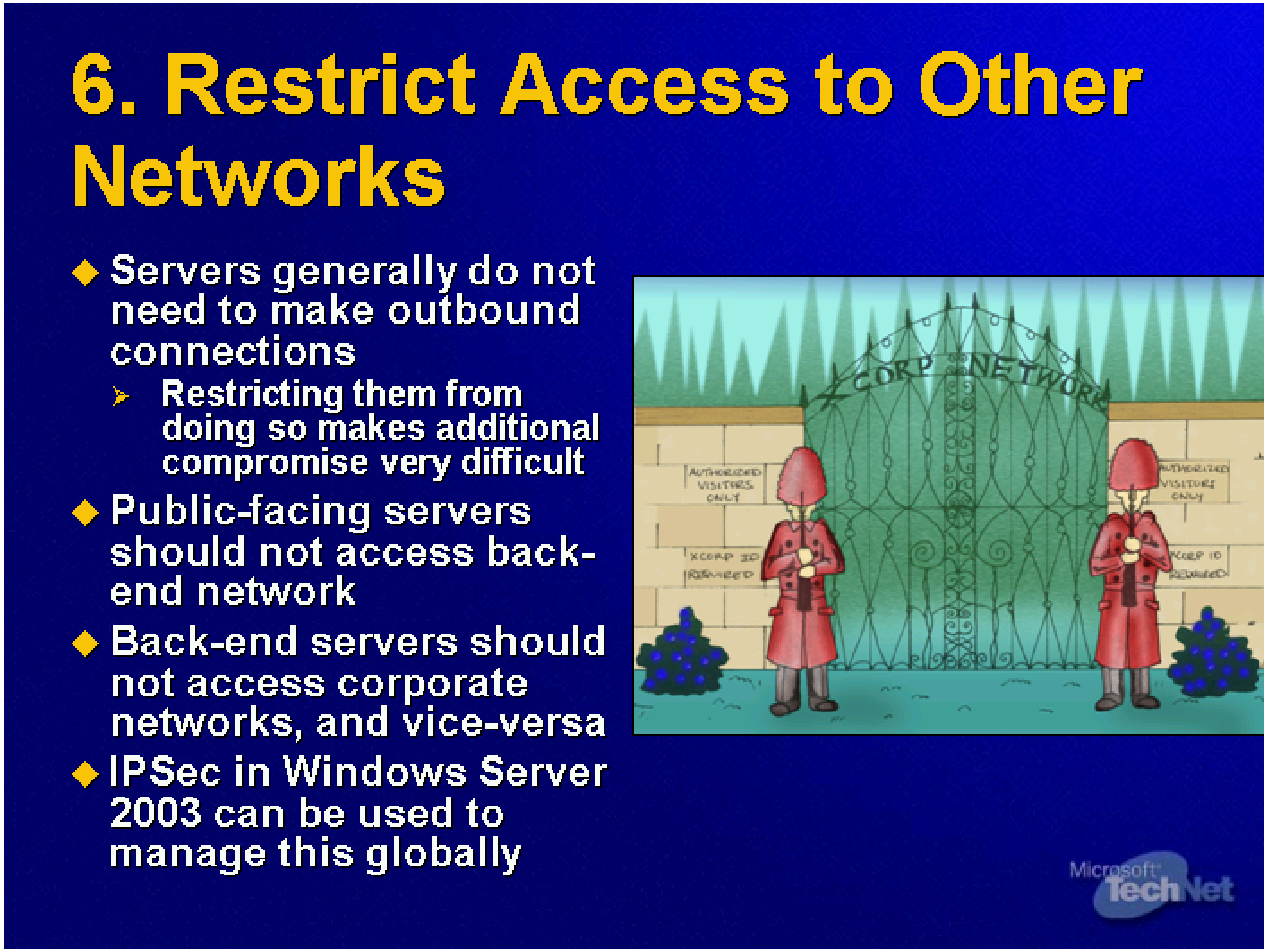
4. High-level Accounts Running Services; on Un-trusted Machines



5. Run Services with Least Privilege

- Services running as administrators
- Privileges
  - Act as the Operating System (SeTCB)
  - Debug Programs (SeDebug)
  - Interactive Logon (SeInteractiveLogonRight)
- Verify the rights assigned to your service accounts
  - Snapshot system before installing the service

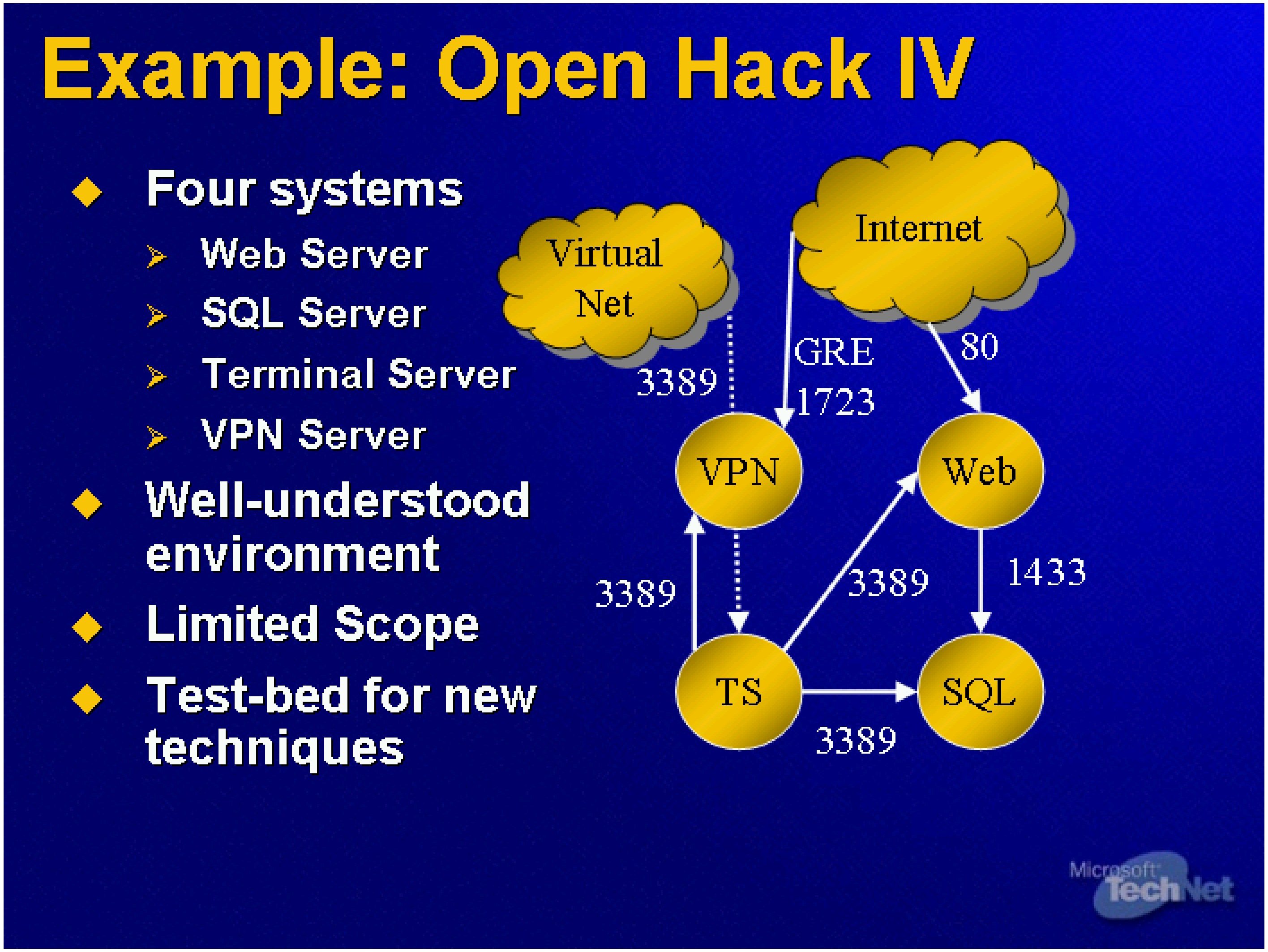
5. Run Services with Least Privilege



6. Restrict Access to Other Networks

- Servers generally do not need to make outbound connections
  - Restricting them from doing so makes additional compromise very difficult
- Public-facing servers should not access back-end network
- Back-end servers should not access corporate networks, and vice-versa
- IPSec in Windows Server 2003 can be used to manage this globally

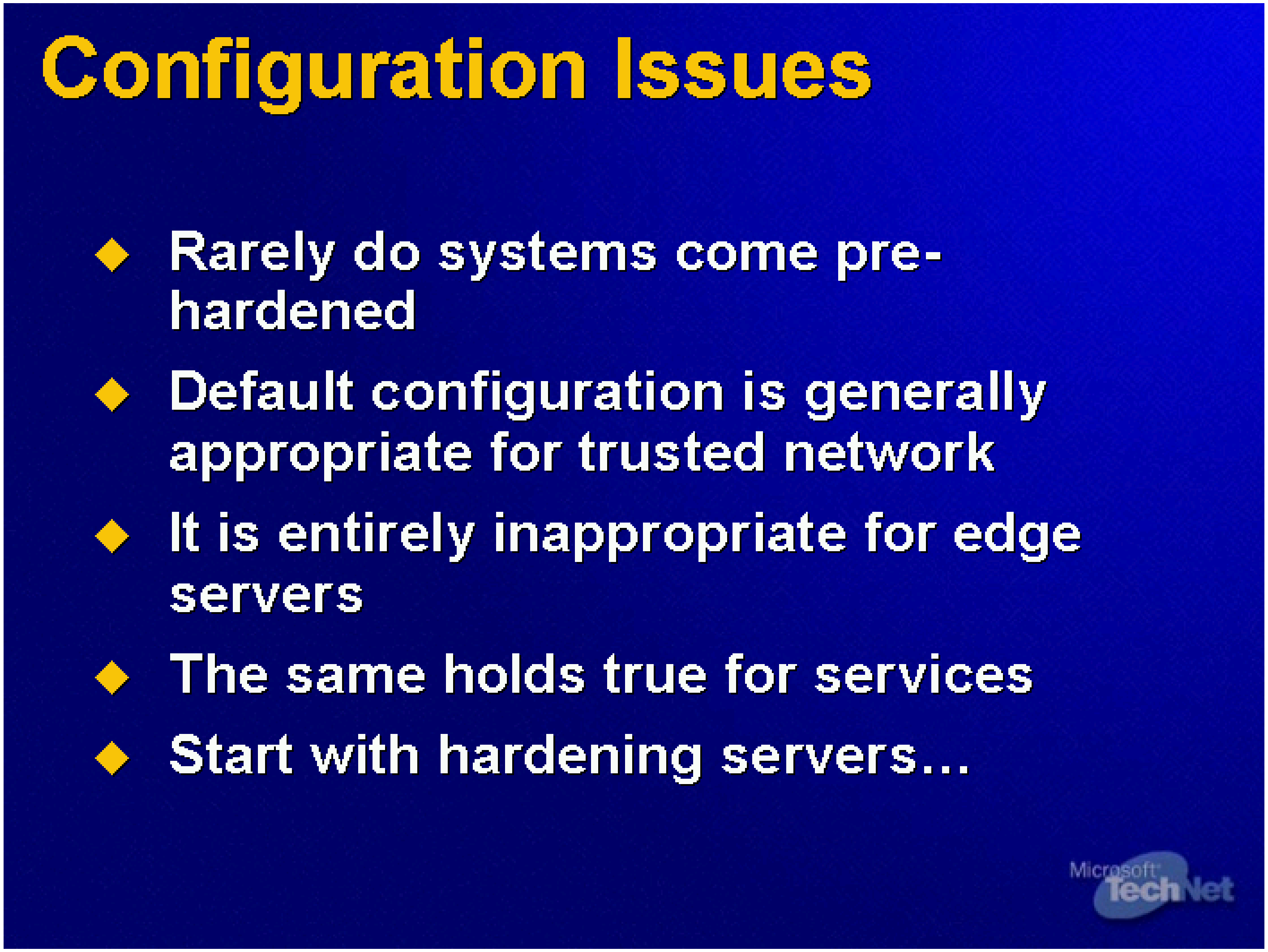
6. Restrict Access to Other Networks



Example: Open Hack IV

- Four systems
  - Web Server
  - SQL Server
  - Terminal Server
  - VPN Server
- Well-understood environment
- Limited Scope
- Test-bed for new techniques

Example: Open Hack IV

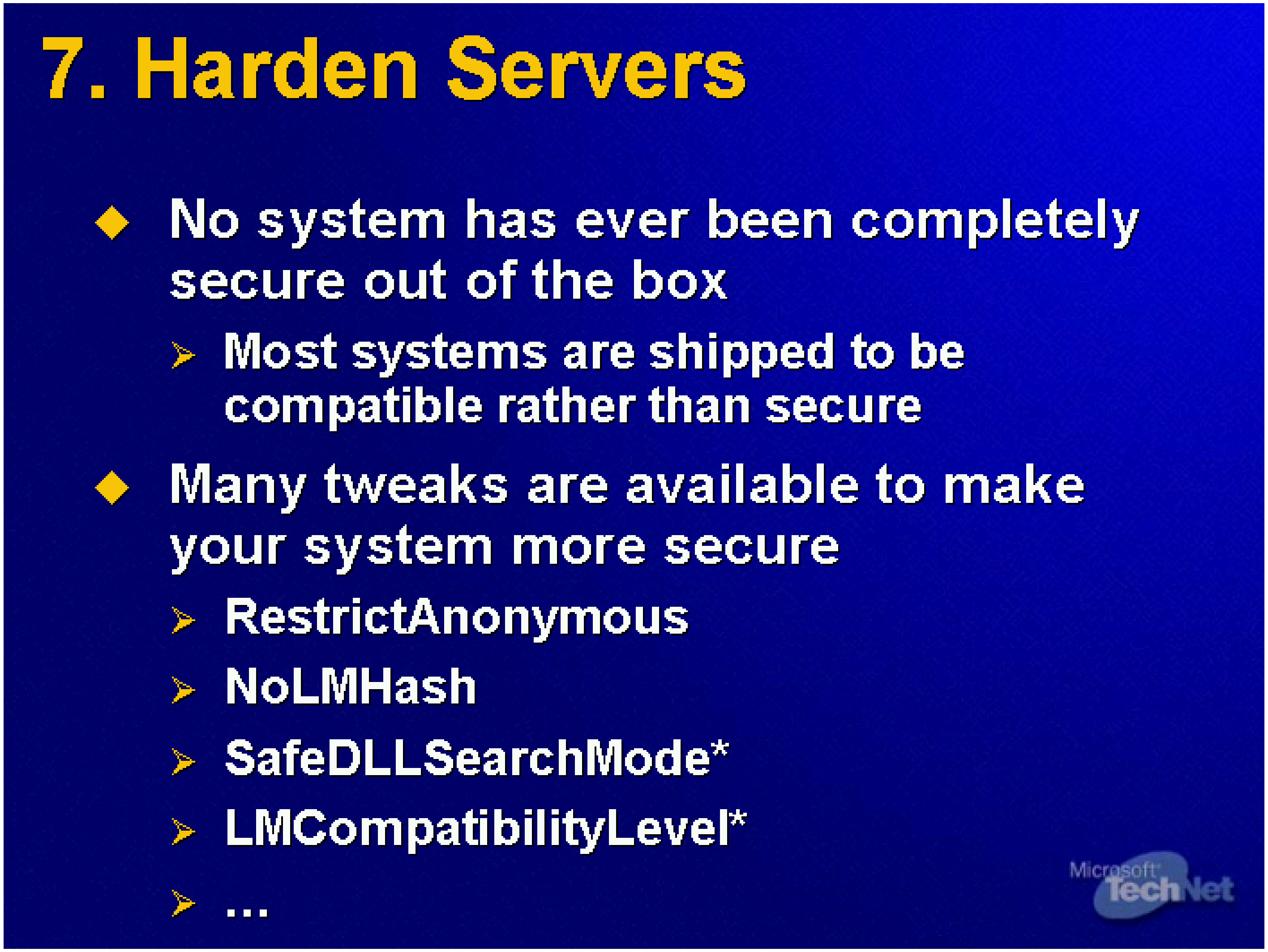


Configuration Issues

- Rarely do systems come pre-hardened
- Default configuration is generally appropriate for trusted network
- It is entirely inappropriate for edge servers
- The same holds true for services
- Start with hardening servers…

Microsoft TechNet

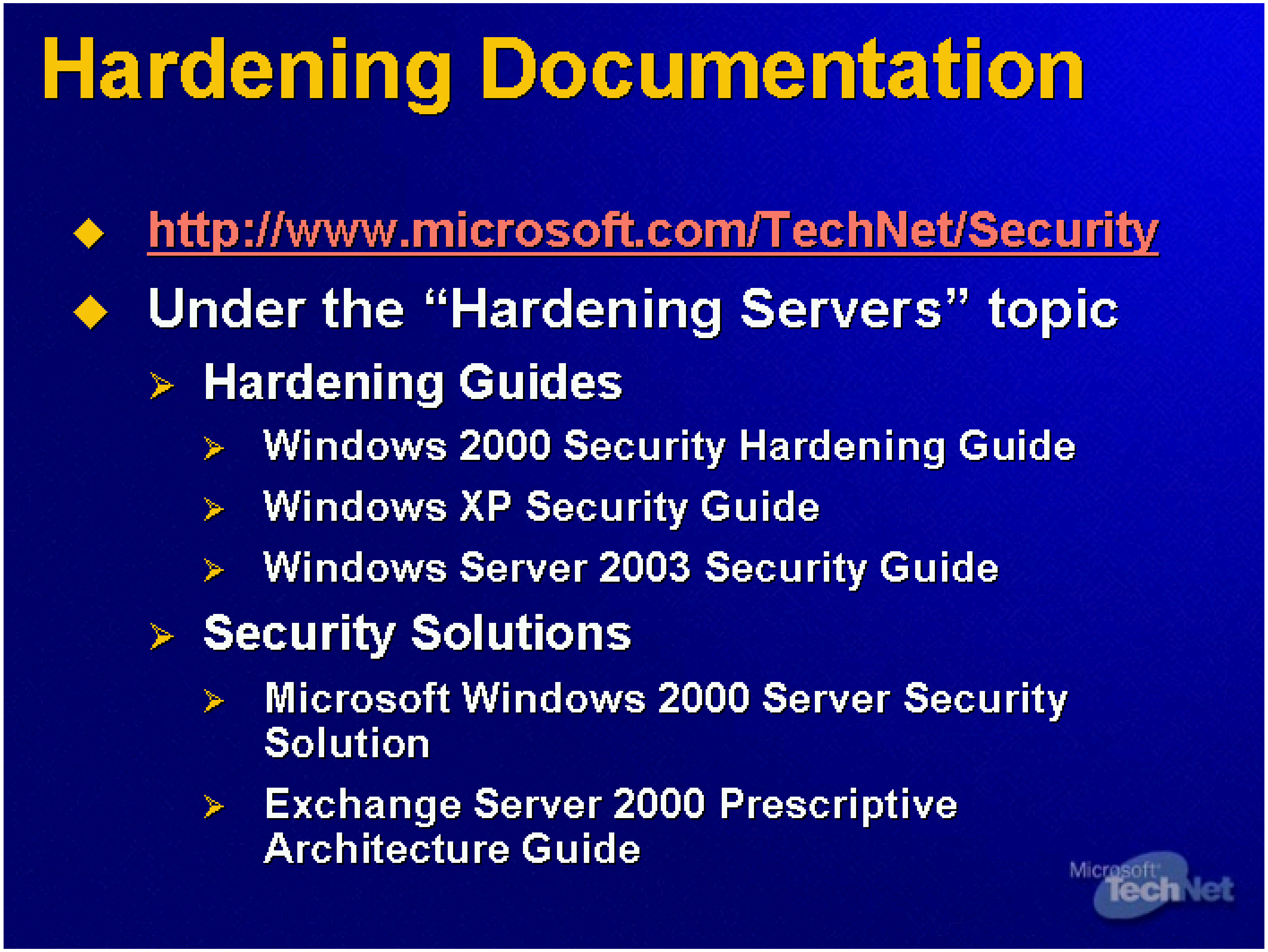
Configuration Issues



7. Harden Servers

- No system has ever been completely secure out of the box
  - Most systems are shipped to be compatible rather than secure
- Many tweaks are available to make your system more secure
  - RestrictAnonymous
  - NoLMHash
  - SafeDLLSearchMode*
  - LMCompatibilityLevel*
  - …

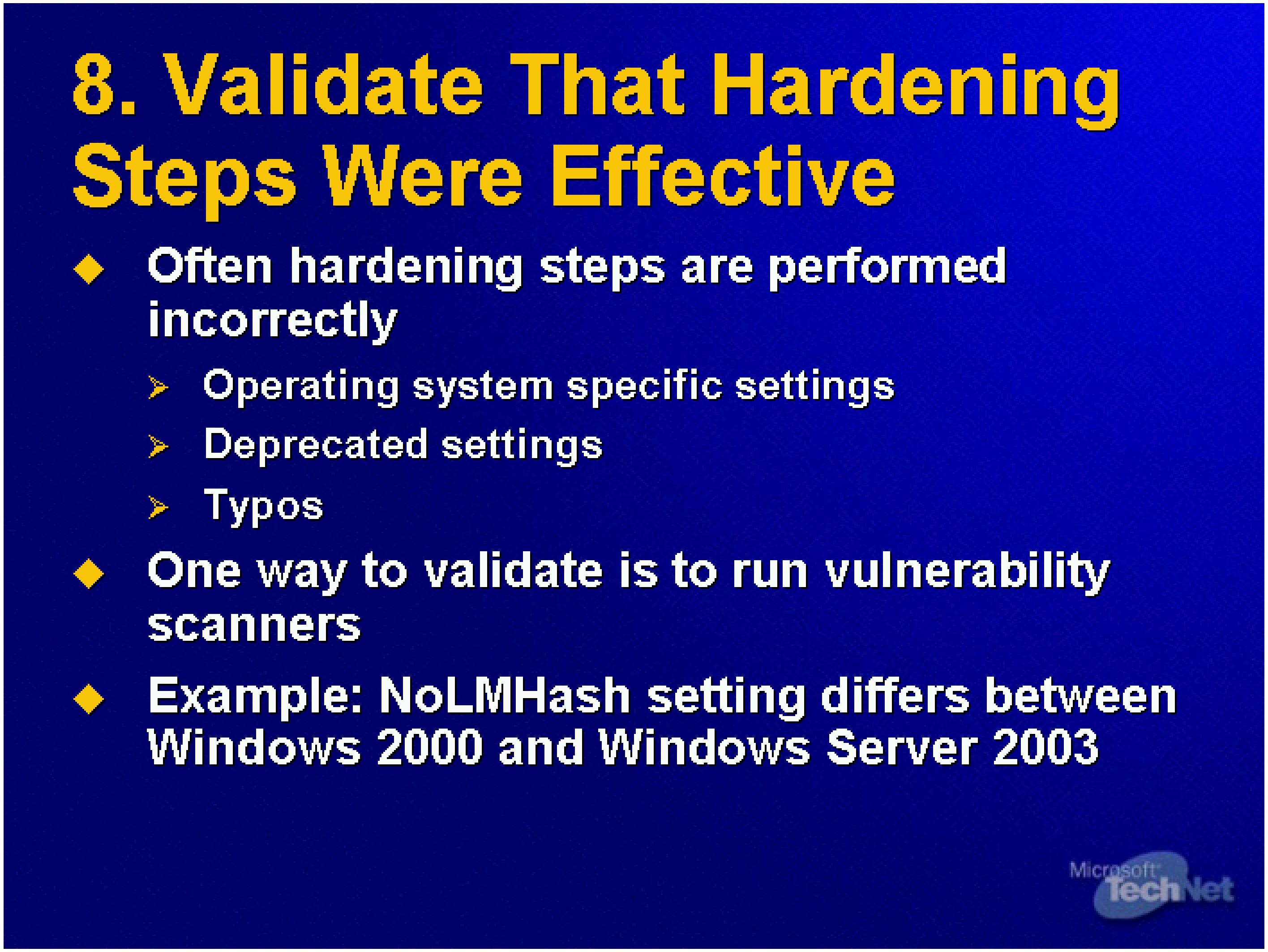
7. Harden Servers



Hardening Documentation

- http://www.microsoft.com/TechNet/Security
- Under the “Hardening Servers” topic
  - Hardening Guides
    - Windows 2000 Security Hardening Guide
    - Windows XP Security Guide
    - Windows Server 2003 Security Guide
  - Security Solutions
    - Microsoft Windows 2000 Server Security Solution
    - Exchange Server 2000 Prescriptive Architecture Guide

Hardening Documentation

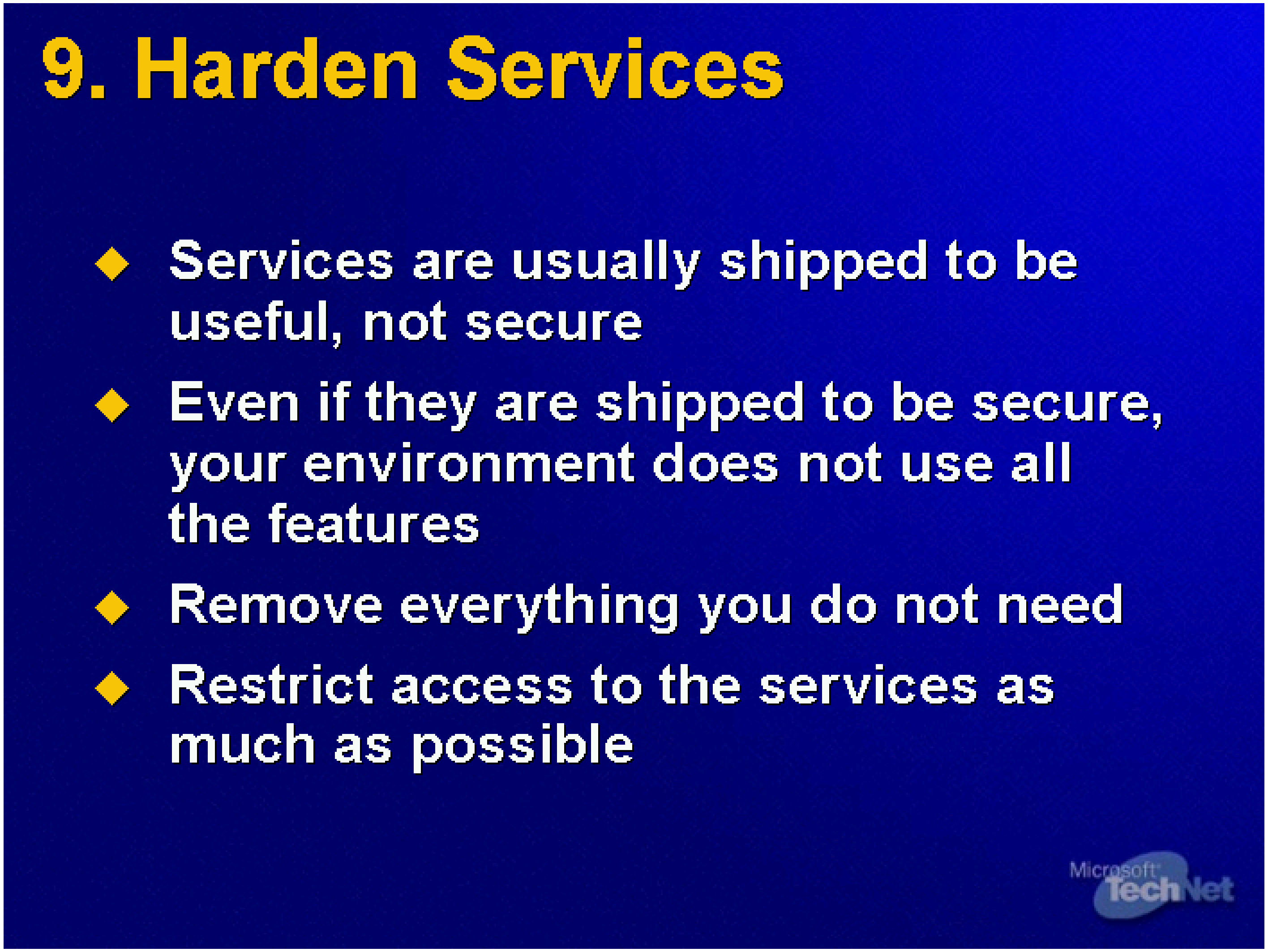


8. Validate That Hardening Steps Were Effective

- Often hardening steps are performed incorrectly
  - Operating system specific settings
  - Deprecated settings
  - Typos
- One way to validate is to run vulnerability scanners
- Example: NoLMHash setting differs between Windows 2000 and Windows Server 2003

Microsoft TechNet

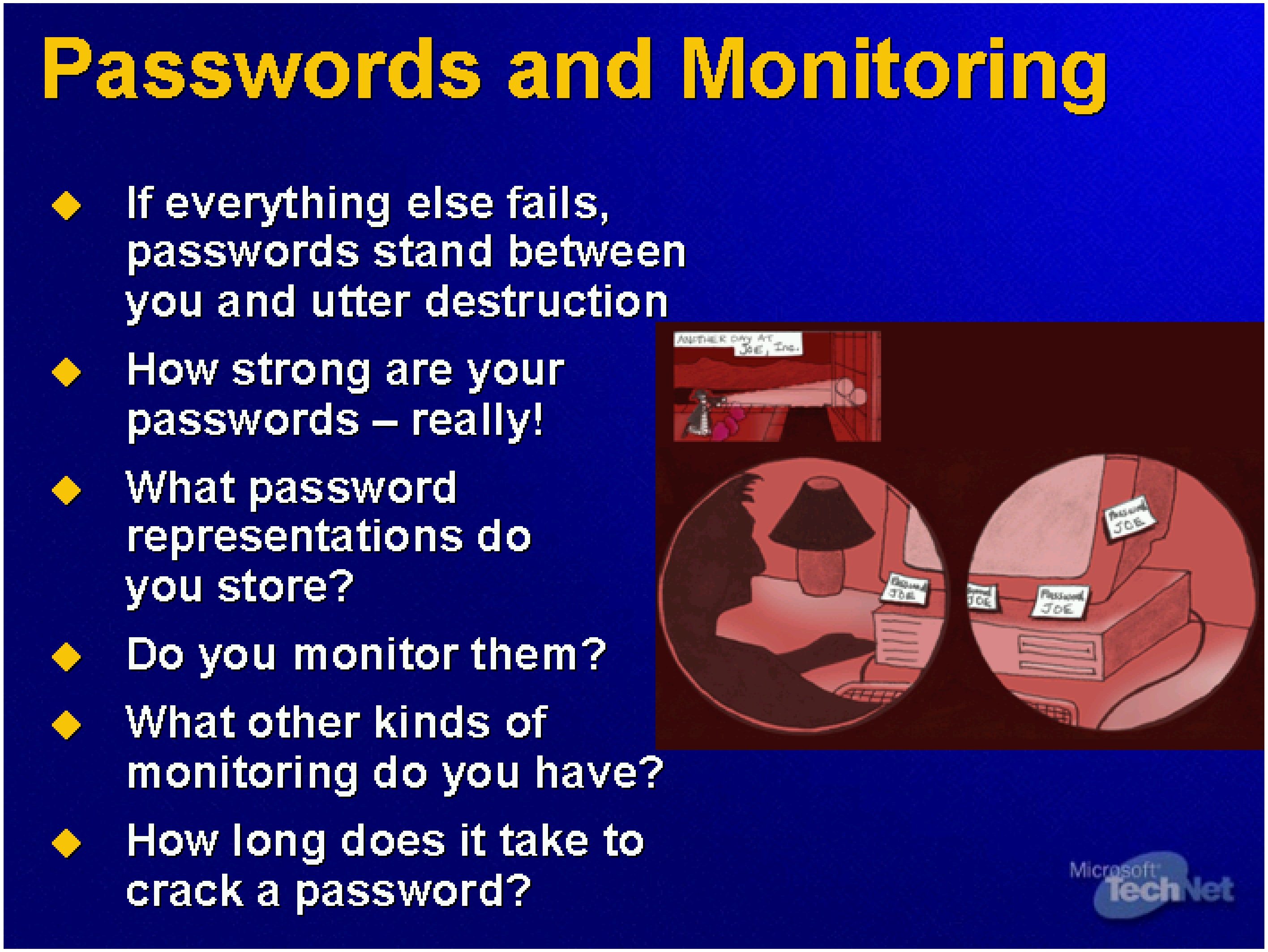
8. Validate That Hardening Steps Were Effective



9. Harden Services

- Services are usually shipped to be useful, not secure
- Even if they are shipped to be secure, your environment does not use all the features
- Remove everything you do not need
- Restrict access to the services as much as possible

9. Harden Services

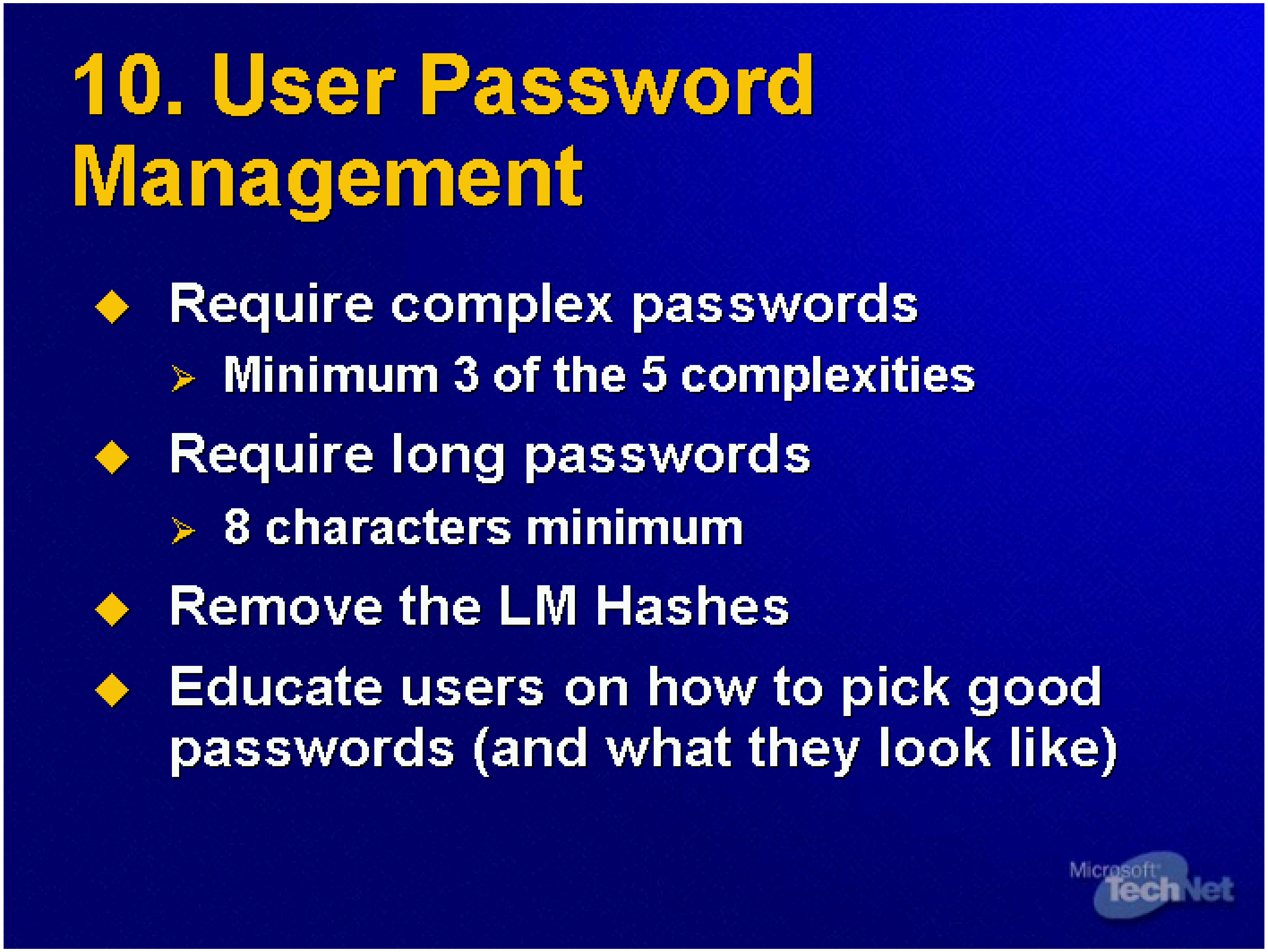


Passwords and Monitoring

- If everything else fails, passwords stand between you and utter destruction
- How strong are your passwords – really!
- What password representations do you store?
- Do you monitor them?
- What other kinds of monitoring do you have?
- How long does it take to crack a password?

ANOTHER DAY AT JOE, Inc.
Password JOE
Password JOE
Password JOE
Password JOE
Microsoft TechNet

Passwords and Monitoring

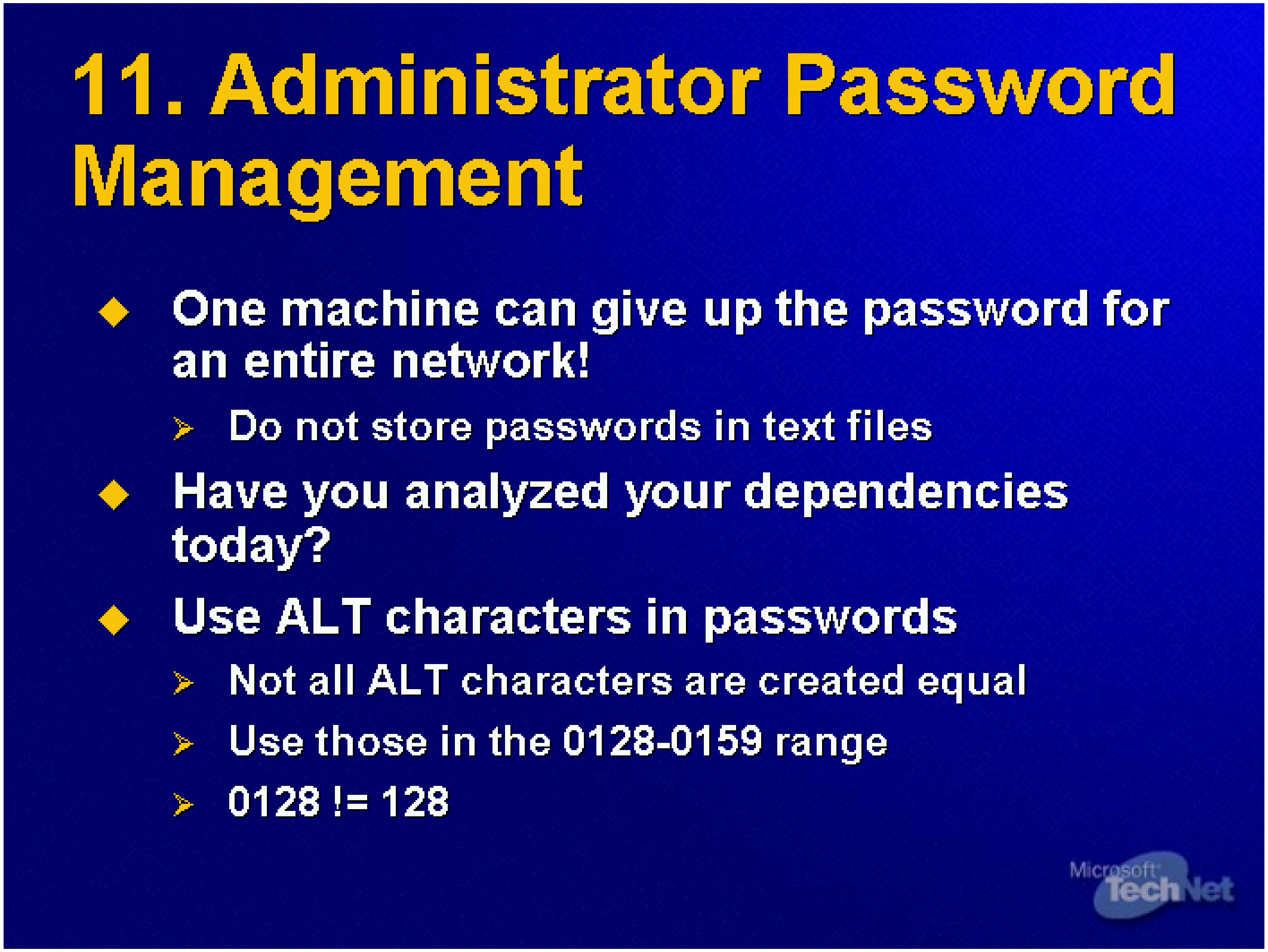


10. User Password Management

- Require complex passwords
  - Minimum 3 of the 5 complexities
- Require long passwords
  - 8 characters minimum
- Remove the LM Hashes
- Educate users on how to pick good passwords (and what they look like)

Microsoft TechNet

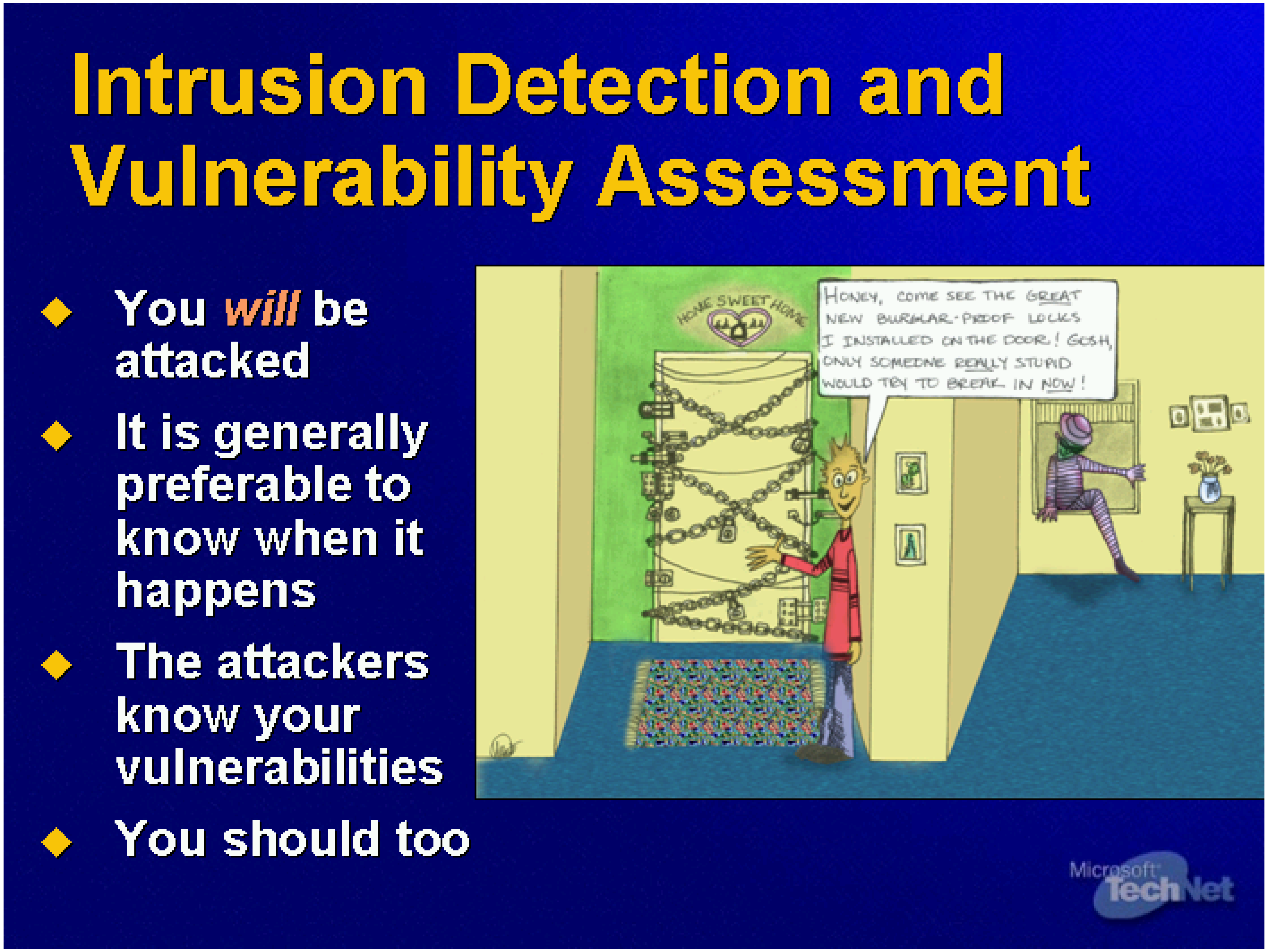
10. User Password Management



11. Administrator Password Management

- One machine can give up the password for an entire network!
  - Do not store passwords in text files
- Have you analyzed your dependencies today?
- Use ALT characters in passwords
  - Not all ALT characters are created equal
  - Use those in the 0128-0159 range
  - 0128 != 128

11. Administrator Password Management

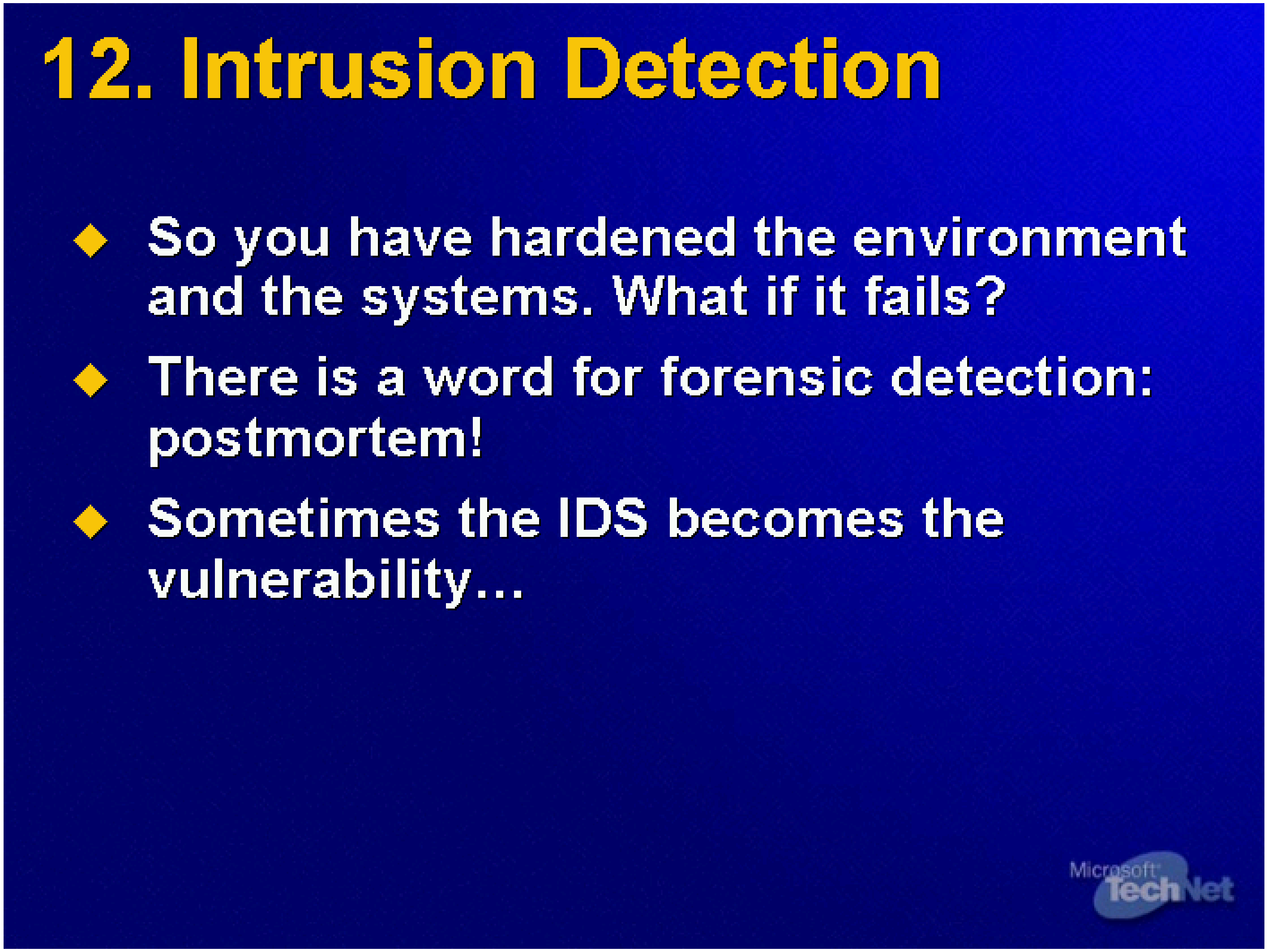


Intrusion Detection and Vulnerability Assessment

- You *will* be attacked
- It is generally preferable to know when it happens
- The attackers know your vulnerabilities
- You should too

HOME SWEET HOME
HONEY, COME SEE THE GREAT NEW BURGLAR-PROOF LOCKS I INSTALLED ON THE DOOR! GOSH, ONLY SOMEONE REALLY STUPID WOULD TRY TO BREAK IN NOW!

Intrusion Detection and Vulnerability Assessment

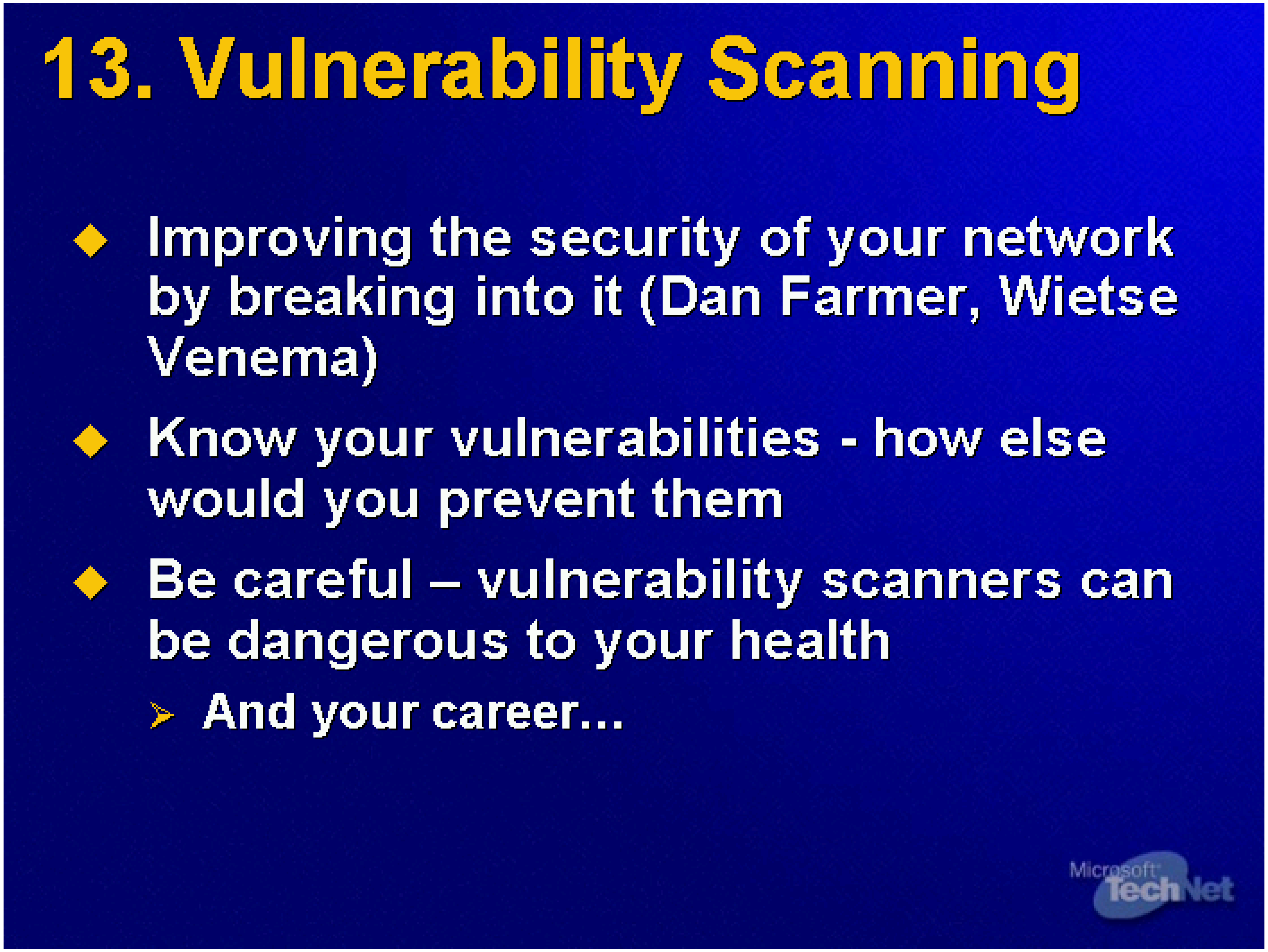


12. Intrusion Detection

- So you have hardened the environment and the systems. What if it fails?
- There is a word for forensic detection: postmortem!
- Sometimes the IDS becomes the vulnerability…

Microsoft TechNet

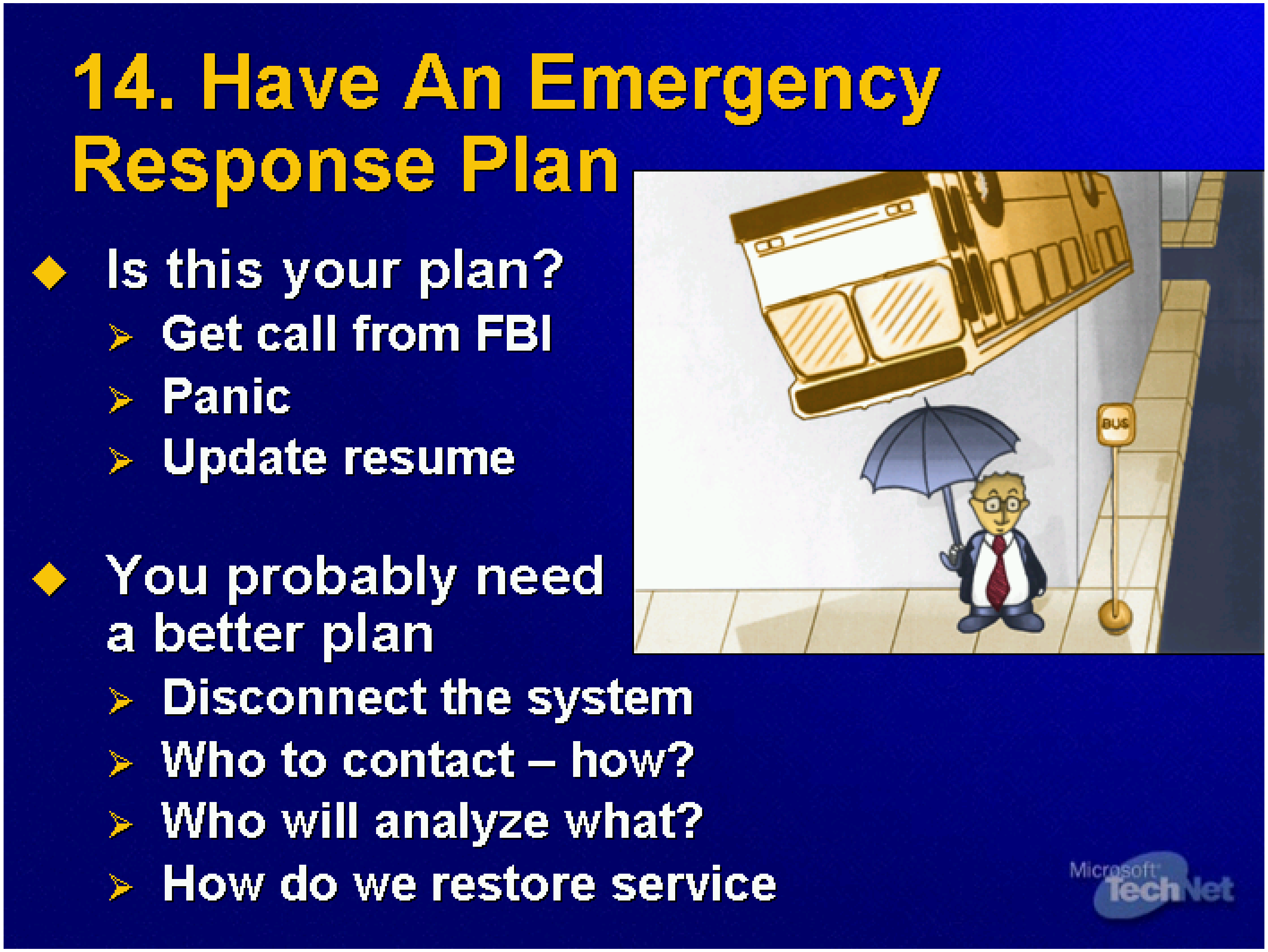
12. Intrusion Detection



13. Vulnerability Scanning

- Improving the security of your network by breaking into it (Dan Farmer, Wietse Venema)
- Know your vulnerabilities - how else would you prevent them
- Be careful – vulnerability scanners can be dangerous to your health
  - And your career…

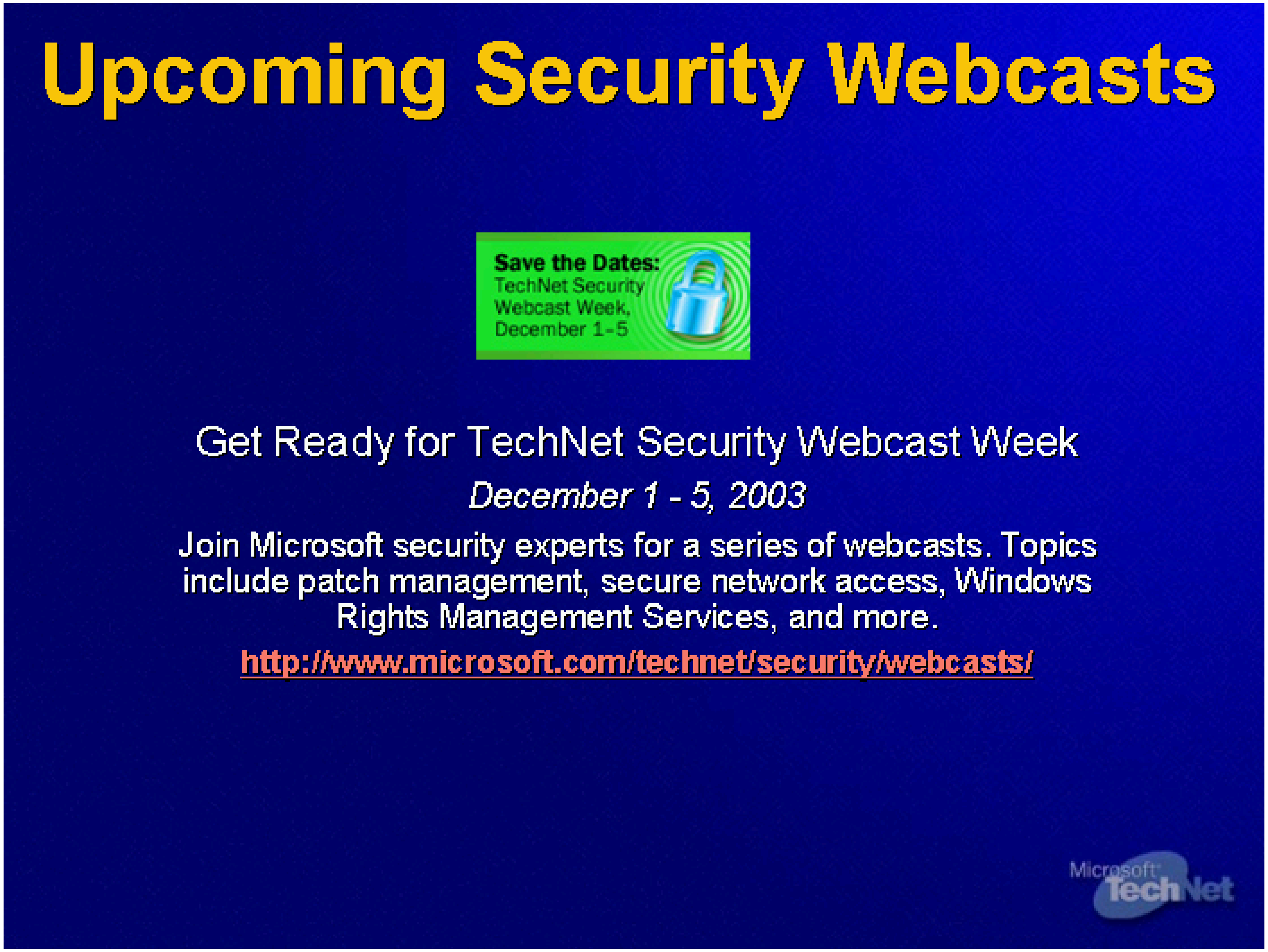
13. Vulnerability Scanning



14. Have An Emergency Response Plan

- Is this your plan?
  - Get call from FBI
  - Panic
  - Update resume
- You probably need a better plan
  - Disconnect the system
  - Who to contact – how?
  - Who will analyze what?
  - How do we restore service

14. Have An Emergency Response Plan



Upcoming Security Webcasts

Save the Dates:
TechNet Security
Webcast Week,
December 1-5

Get Ready for TechNet Security Webcast Week

December 1 - 5, 2003

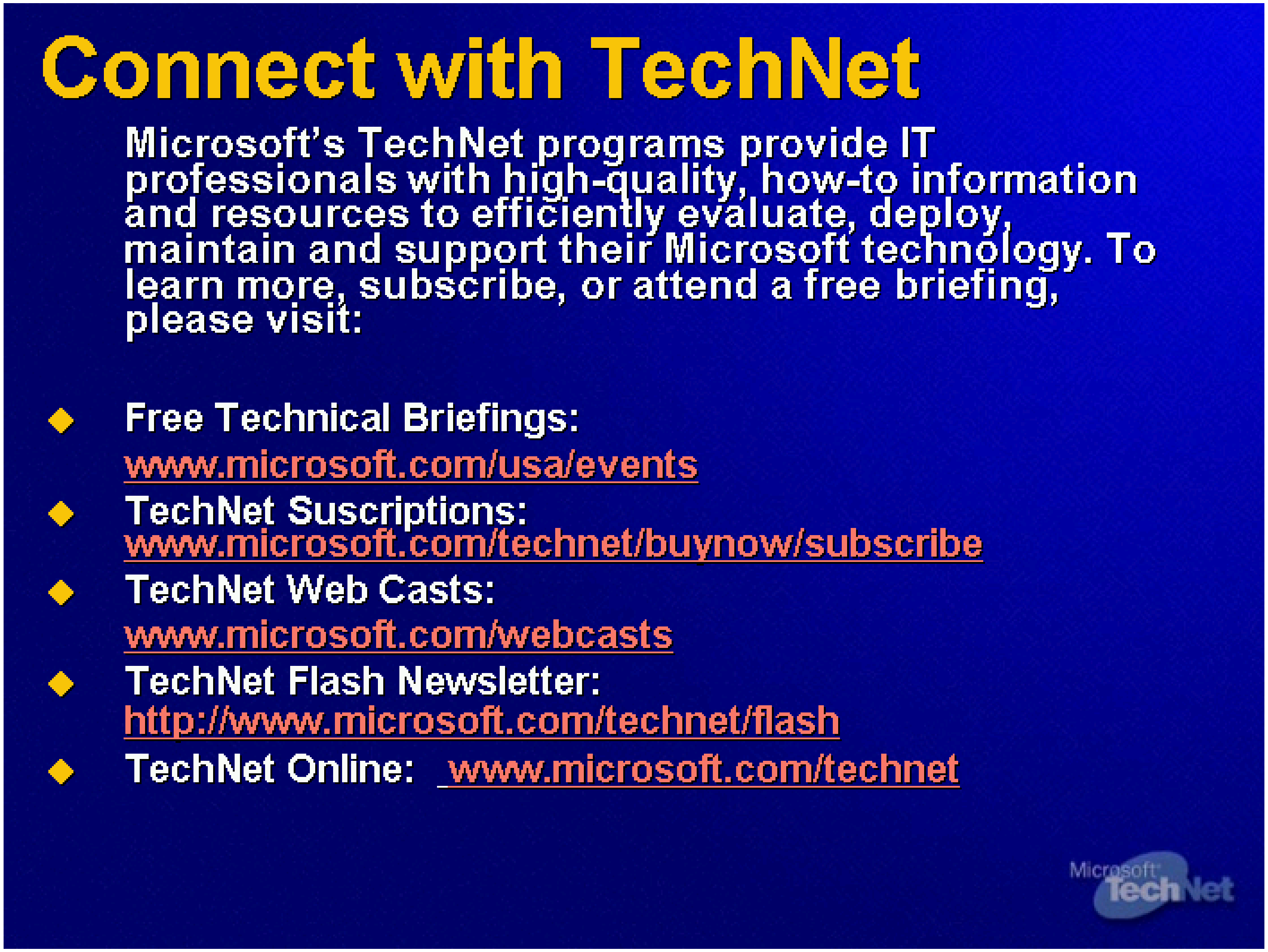
Join Microsoft security experts for a series of webcasts. Topics include patch management, secure network access, Windows Rights Management Services, and more.

http://www.microsoft.com/technet/security/webcasts/

Upcoming Security Webcasts

http://www.microsoft.com/technet/security/webcasts/

http://www.microsoft.com/technet/security/webcasts/



Connect with TechNet

Microsoft's TechNet programs provide IT professionals with high-quality, how-to information and resources to efficiently evaluate, deploy, maintain and support their Microsoft technology. To learn more, subscribe, or attend a free briefing, please visit:

- Free Technical Briefings: www.microsoft.com/usa/events
- TechNet Suscriptions: www.microsoft.com/technet/buynow/subscribe
- TechNet Web Casts: www.microsoft.com/webcasts
- TechNet Flash Newsletter: http://www.microsoft.com/technet/flash
- TechNet Online: www.microsoft.com/technet

Microsoft TechNet

Connect with TechNet

https://msevents.microsoft.com/emcui/WelcomePage.aspx?EventID=1032238908&Culture=en-US

https://msevents.microsoft.com/emcui/WelcomePage.aspx?EventI...