4 juni 2012

ISACA

# Detect the hack, sooner
# Audit (investigate) cybercrime

**Robert-Jan Mora RE CISSP**
Coördinator Cybercrime & Audits

hoffmann
Vertrouwen is goed, Hoffmann is beter.

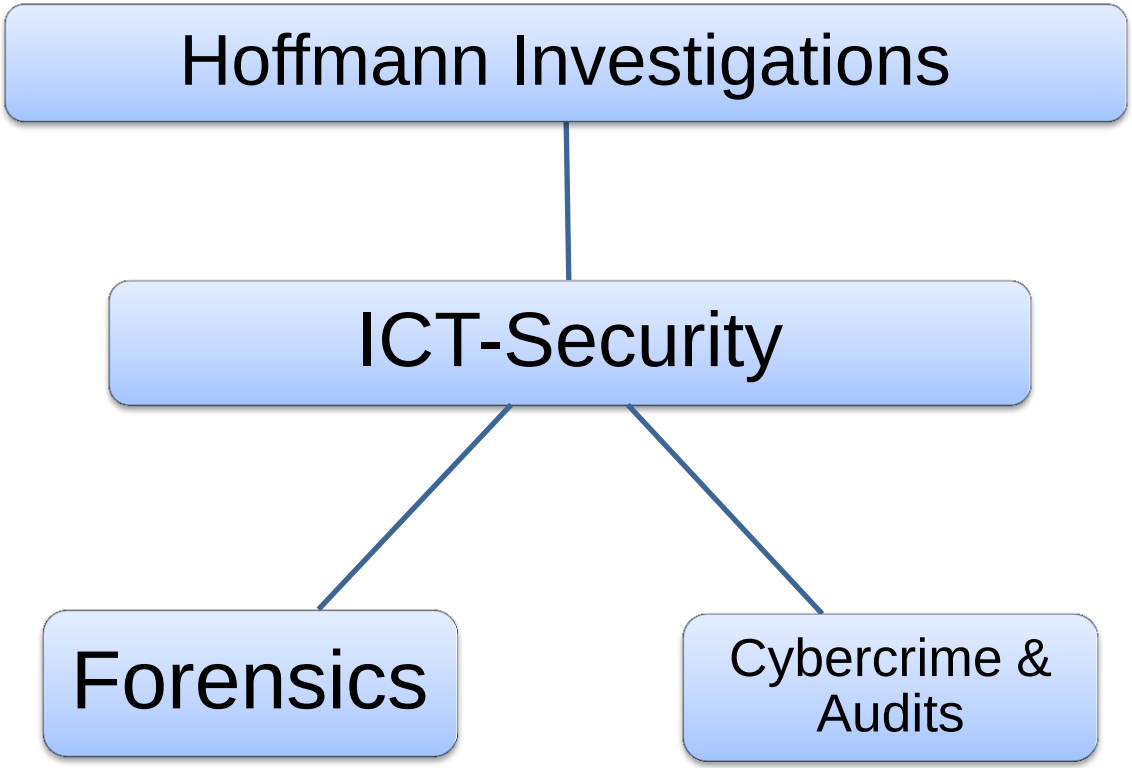
# Hoffmann Investigations

- Investigations in private sector and government
  - Police, FIOD-ECD, NMA, OPTA en OM
- Investigates fraud, theft, corporate espionage, hacking
- Experienced investigations team:
  - *PO, CISSP, RE,CISA, CEH, MSCE, LPIC*

Services:

- Digital forensics
- Open Source Development, Linux forensics libs: libewf, libpff
- Pentesting
- Malware analysis
- Hacking investigations

# ICT-Security



# Outline

- Starting point
- Criminal hacking
- Sources of evidence
- Autonomy of a hacking attack (The five P's)
- General Controls and specific control measures
- Conclusion
- Inside an APT investigation
- Discussion
- Sources

# Starting Point

- You will get hacked, sooner or later!
- Getting hacked is certain and organizations should have control measures in place to detect these hacking incidents

## NSA considers its networks compromised

Posted on 17 December 2010.

BOOKMARK ...

Debora Plunkett, head of the NSA's Information Assurance Directorate, has confirmed what many security experts suspected to be true: no computer network can be considered completely and utterly impenetrable - not even that of the NSA.

"There's no such thing as 'secure' any more," she said to the attendees of a cyber security forum sponsored by the Atlantic and Government Executive media organizations, and confirmed that the NSA works under the assumption that various parts of their systems have already been compromised, and is adjusting its actions accordingly.

# Criminal hacking

- Criminal hacking means finding out weaknesses in computer software or computer networks and exploiting them for profit, protest, sabotage terrorism or cyber war.
- This definition has been derived from the hacking definition on Wikipedia.
- In this presentation we focus on the risk of criminal hacking. No permission was given.
- The goal for the victims of a criminal hacker (organizations) would be to correlate several sources of evidence that usually are already present within a organization and detect intruder attempts as early as possible.

# Sources of evidence in organizations

Usually these sources of evidence are present (implement them if not!):

- Firewall logging
- Network traffic (Netflow data)
- Intrusions/Extrusion detection systems logging
- Mail and messaging (spam) logging
- Host intrusion prevention systems logging
- Web application logging (logfiles webservers)
- Anti-virus logging
- System and Security logging (Authentication logging)
- Proxy logging
- DNS logging
- Remote access/ VPN logging

These sources should be analyzed based on malicious threat indicators and events. Usually these indicators are called indicators of compromise or IOC's.

# Autonomy of a hacking attack (The five P's)

A hacking attack consists of several phases in which a hacker or hacker group can reveal its interest for a particular organization or individual.

These phases are:

1. **P**robe
2. **P**enetrate
3. **P**ersist
4. **P**ropagate
5. **P**aralyze

# Probe

In this phase an attacker gathers intelligence about its target. This means the attacker tries to gather as much information about the network, people (social media) and web services as possible, in order to find vulnerable services or systems.

Hacker probe actions:

- Harvest the internet (Social media)
- Sending web bugs or e-mails
- Nmapping
- SQLMapping and DirBustering etc.

General Controls

1. Information Security Policy
2. SLA's with service providers, extarnal and internal about breach obligation
3. Make sure software that is used is up-to-date!
4. Make sure time is synchronized
5. Implement secure coding and configuration principles
6. Have a computer security incident handling process in place , NIST SP 800-61 Revision 1

# Probe

## Specific Controls

1. Continuously analyze and correlate IP-addresses used by attackers (from the different sources off evidence like the firewall logging, ids logging, spam, anti-virus and web application logging)
2. Continuously block suspicious IP's and alert providers or organizations via abuse messages and monitor on the origin.
3. Inspect if these suspicious IP-addresses can already be linked to malicious activities.
4. Report serious hacking attempts to Nationaal Cyber Security Centrum (NCSC), the former Govcert.
5. Employees should have the ability to report security incidents to the internal or external security organization.
6. Analyze the output of the hacker probes to learn what he has learned, either by inspecting the log files or run the tools yourself on the systems.

# Probe example

## Firewall probes

Date: May 20, 2011.txt:14:28:51 drop 10.10.110.2 >eth-s1p1c0 rule: 3; rule_uid: {7DBA415E-3CC9-494A-8072-55825555DA3F2}; rule_name: S10-999; SmartDefense profile: Default_Protection; src: 82.101.xxx.xxx; dst: 62.xx.xx.xxx; proto: tcp; product: VPN-1 & FireWall-1; service: Symantec; s_port: 51868;

Times 100000.....!!!!

## DirBuster Probes

W3SVC430286685\ex110607.log:2011-06-07 11:19:07 W3SVC430286685 10.10.20.61 HEAD

/images/ - 443 – 7x.xx.xx.7x DirBuster-0.12+(http://www.owasp.org/index.php/Cat

egory:OWASP_DirBuster_Project) 404 0 2

W3SVC430286685\ex110607.log:2011-06-07 11:19:07 W3SVC430286685 10.9.1.11 HEAD

/full/ - 443 - 7x.xx.xx.7x DirBuster-0.12+(http://www.owasp.org/index.php/Categ

ory:OWASP_DirBuster_Project) 404 0 2

Times 10000.....!!

# Penetrate

A result from the **P**robing phase are vulnerable servers, interesting targets (people). The attackers usually uses a lot of different IP-addresses that already could have been discovered.

Hacker Penetration methods:

1. Brute force authentication services
2. Exploiting programming errors/Buffer overflows
3. Exploiting application logic flaws (../)
4. System configuration errors (snmp, printers)
5. User input validation problems
6. Phishing
7. Spear Phishing
8. Physical Attacks (Wifi, Teensy)

General Controls

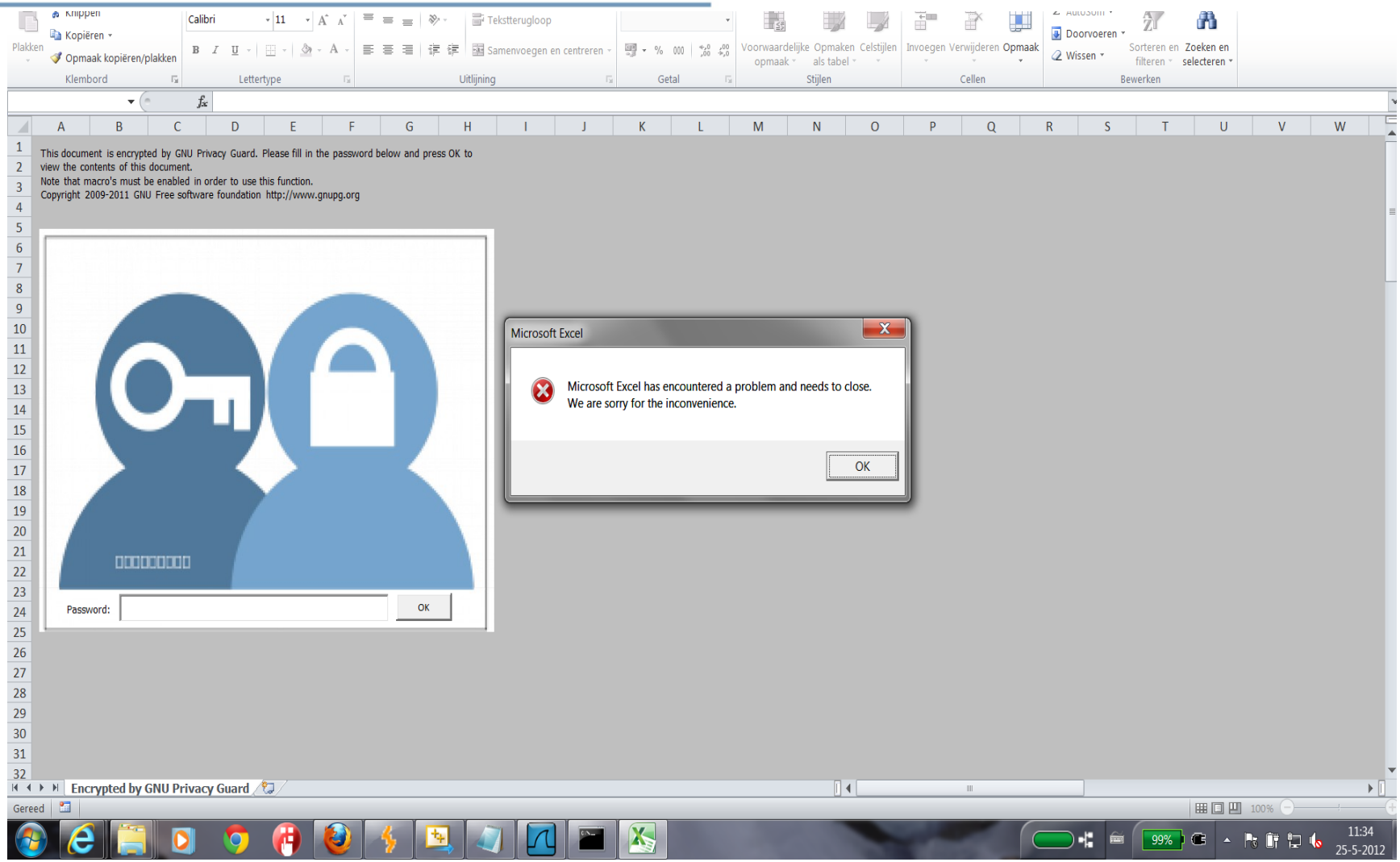
1. Implement corporate error reporting
2. Secure coding and configuration principles (never trust anything a user or other process tells you)
3. Implement ICT technology that leaves forensic traces of user activity on data carriers. If you make use of thin client technology (Citrix, RDP), be sure to implement a compensating control on user, security and system activity monitoring.
4. Implement a security awareness program where users are taught in detecting the signs of malicious activities like phishing or spear phishing.
5. Regularly perform holistic pentests on the organization
6. Also (pen)test the quality of the control measures like anti-virusscanners or Intrusion Detection Systems
7. Audit on how quick new signatures can be implemented to detect malware

# Penetrate

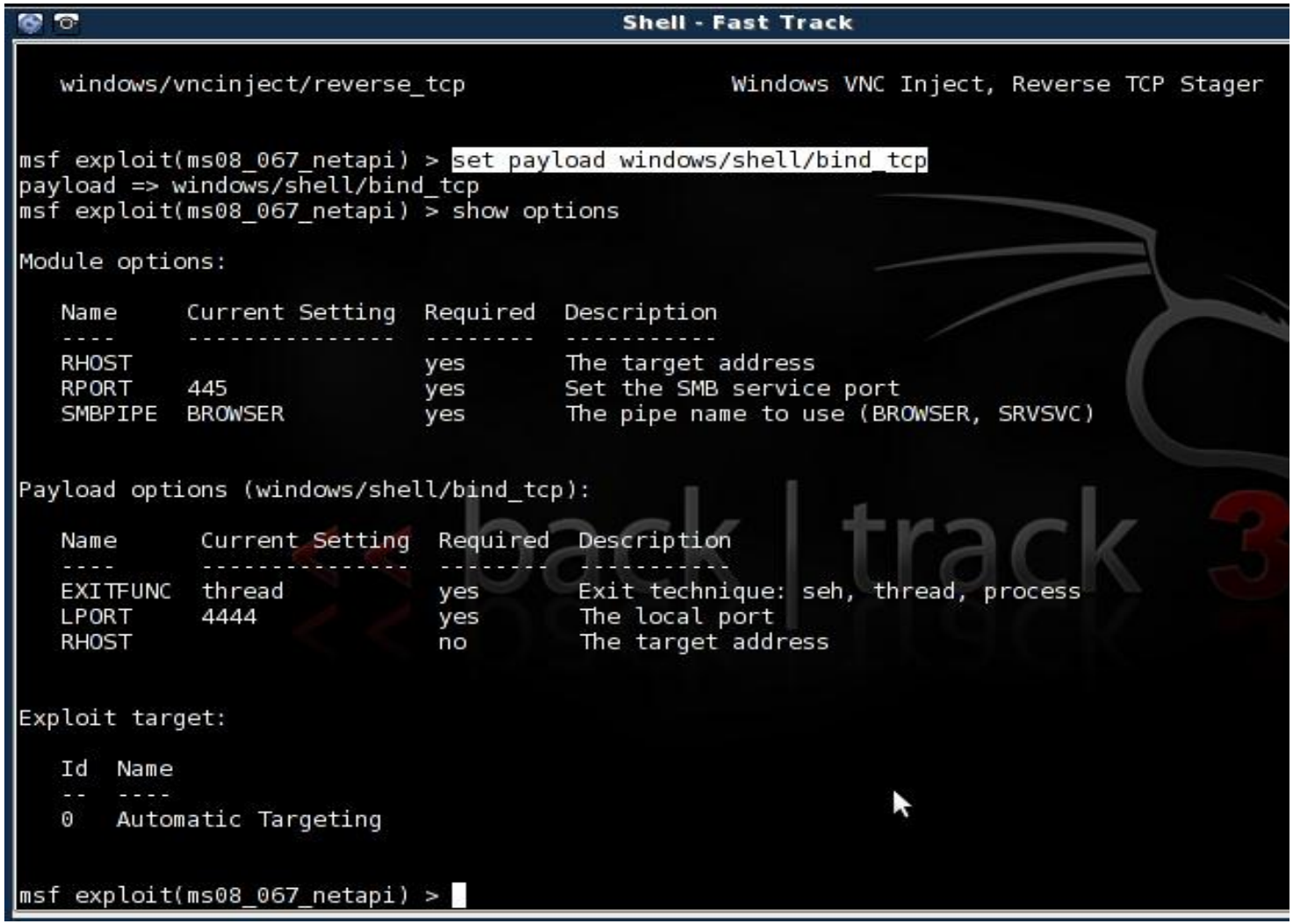
## Specific Controls

1. Continuously analyze and correlate IP-addresses used by attackers (from the different sources off evidence like the firewall logging, ids logging, spam, anti-virus and web application logging).
2. Analyze malware found on client computers or in spam and anti-virus control measures.
3. Continuously block suspicious IP's and alert providers or organizations via abuse messages and monitor on the origin of the IP's.
4. Inspect if these suspicious IP-addresses can already be linked to malicious activities.
5. Report confirmed intrusions to the Dutch National Police and Nationaal Cyber Security Centrum (NCSC).
6. Notice and takedown procedures.
7. Investigate the cause of unexpected crashes from services and computer systems and whether these events are related to hacking attempts.

# Penetrate example



# Penetrate example



# Persist

In this phase the hacker has been successful in exploiting a serious weakness in some vulnerable application, network service or outdated software version.

## Hacker Persist methods:

1. Implement easy access by using webshells (AspxSpy or http tunneling software ReduH)
2. Obtain admin accounts (Pwdump, Gdump, Hyena and Sysinternals)
3. Install backdoors/malware on network (C&C)
4. Deletes footprints sometimes☺

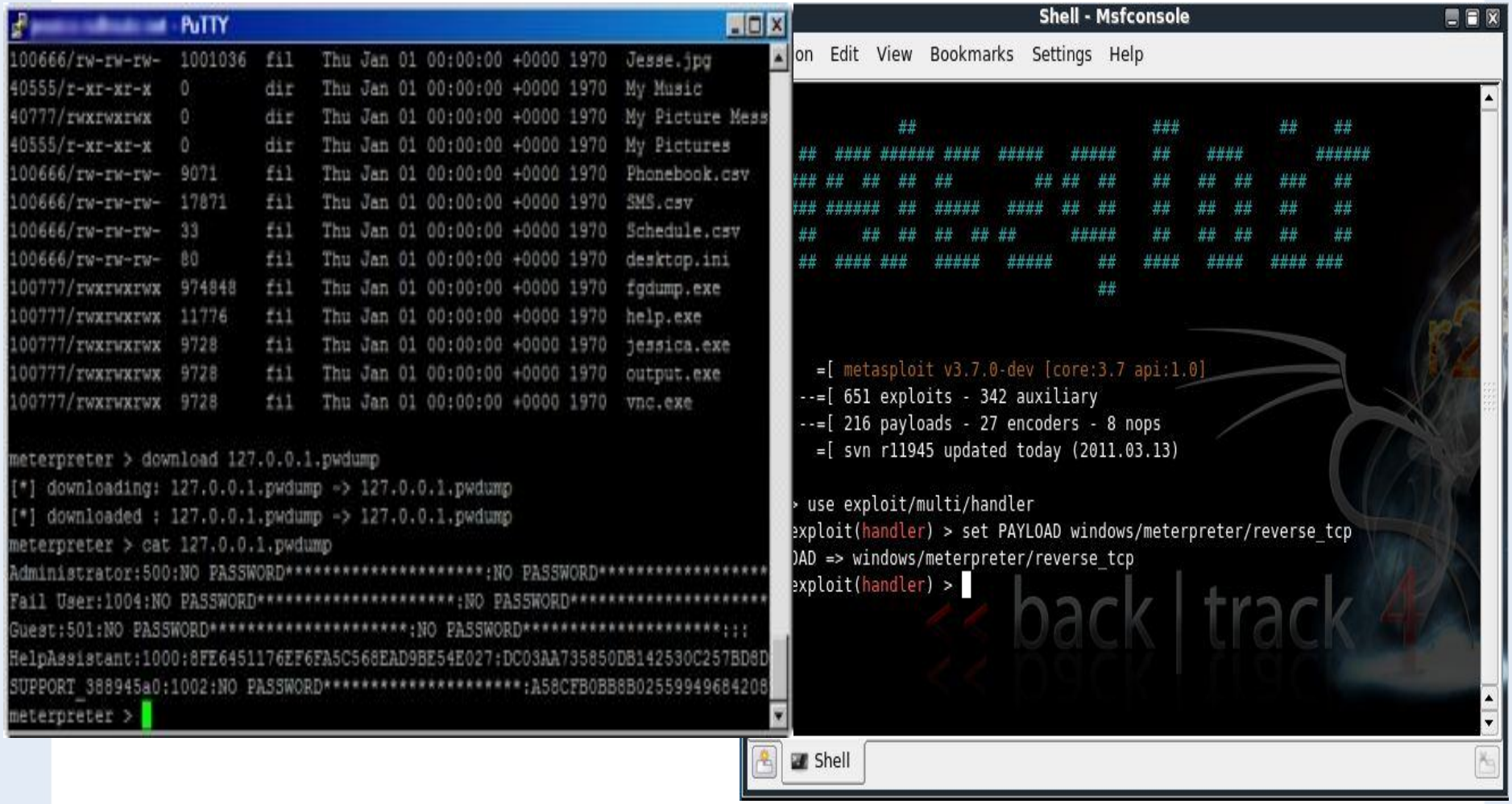
## General Controls

1. Setup secure logging on seperate server

## Specific Controls

1. Perform forensics and malware analyses on the malware found on compromised servers.
2. Analyze network traffic on indicators of compromise.
3. Blackhole certain and discovered malicious malware domains within DNS.
4. Change passwords from the users.
5. Create lists of compromised accounts and compromised hosts.
6. Analyze relevant log files, like security eventlogs, DNS, network dumps (pcap) or outbound traffic.
7. Create new network signatures for the intrusions detection systems.

# Persist example



# Propogate

- The next phase the attacker will try to do is to establish more control and try to control more segments of the compromised network.
- If the infection is for example a malicious worm the worm will try to infect as many systems it can connect to.
- Usually the hacker tries to install malware on as much servers he has access to. The infected servers will connect to C&C servers.

Hacker Propagate methods:

1. Infect compromised servers with multiple backdoors by using default system administration tools like psexec.

# Paralyze

This is the final stage in a targeted attack where an hacker reveals his true motivations of the attack. Is he interested in obtaining classified information, steal money or disrupt mission critical business services. This could be done by deleting critical components which could disturbe the continuity of a mission critical server. DDoS could also be the motive of a hacker group.

# Conclusion

- Most of the hacks can be detected early if a victim organization understands the signs of being hacked.
- Usually a lot of information is available in different log files of various services during the first stages of Probing,Penetrating and Persisting.

- From our experience we know that most if not all of these signs are being overlooked from extended periods of time. This period could be several weeks of even years!!

- It should be the main goal to integrate the logging information already present in the organization and to correlate them on signs of a compromise.

- If such a framework of controls is present and functions properly the window of the hacker will be detected in a early stage.

# Auditor lessons

- Being hacked is certain, create better visibility on hacker activity to respond sooner.
- Test the current security controls of a client and determine their securing effect!
  - How good are the virusscanners in detecting malware.
  - How good is your Intrusion/Extrusion detection process working. Are malware signatures detected by the sensors and employees?
  - Test humans and their security behaviour.
- Test if a central location exist of log file analysis (SIEM). Review logfiles based on “hack” indicators.
- Conduct a proper problem analysis vs. the “Whack  a Mole” approach.

# Discussion

- Questions?

r.mora@hoffmannbv.nl

# References


1. Norea Fact-sheet Hacking
2. Planning for failure, November 2011, Forrester report for Security and Risk professionals
3. NSA considers its networks compromised, http://www.net-security.org/secworld.php?id=10333
4. Of course there are other sources of evidence, like servers, computers, (e-mail) databases etc.
5. Managing Security with Snort & IDS Tools, http://onlamp.com/pub/a/security/excerpt/SnortandIDSTools_chap1/index.html
6. DirBuster is a tool to brute force directory and file names on web or application servers. Sqlmap is a tool to automate sql injections flaws.
7. NIST SP 800-61 Revision 1, Computer Security Incident Handling Guide
8. Microsoft Corporate Error Reporting, http://download.microsoft.com/download/5/9/2/592d2308-a6a2-48ad-ae8f-72f888b9d361/CER_Implementation_Plan.pdf
9. https://www.cpni.nl/projecten/notice-and-take-down, The notice and takedown procedure involves four steps:
    1. Signaling from certain illegal or malicious content on the Internet.
    2. Notice the intermediary party involved
    3. Assessment of the report
    4. Action (Take-down)
10. http://www.malwaredomains.com/bhdns.html, A list of domains that are known to be used to propagate spyware or malware are loaded into internal dns servers. When an infected computer is requesting these discovered malware domains a fake reply is sent.