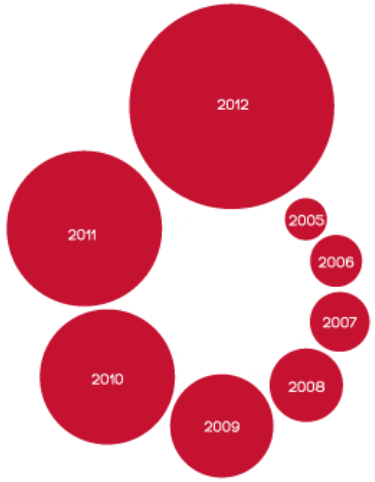
nccgroup
freedom from doubt

How we breach network infrastructures and how to protect them

Bernardo Damele, NCC Group

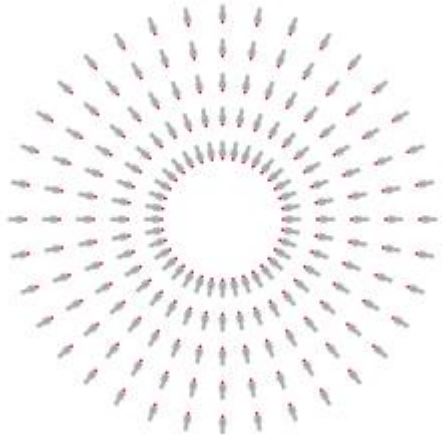
About NCC Group



Eighth successive year of double digit growth

We protect 15,000 clients worldwide

We monitor over 16 million web pages every week



World's largest penetration testing team

Agenda

- What is **security**?

- How we **assess and breach** networks
  - Common mistakes
  - Overlooked areas
  - Network design mistakes
  - Defective assumptions
  - Weakest entry points of a network perimeter
  - Leverage access to the network and why

- How to **protect** networks

What is security?

"Security is a degree of resistance to, or protection from a threat."

Security provides

"A form of protection where a separation is created between the assets and the threat."

Key facets of successful security

- **Processes and procedures**
  - What is expected within the business
- **People**
  - Who are trained
  - Who have a sense of risk ownership
  - Who don't feel afraid to report
- **Technology**
  - Helps people
  - Technology on its own cannot solve cyber security

Who are their targets and why?

- **Casual**
  - Target: Anything
- **Criminals / Employees**
  - Target: SME On-Line Banking
  - Target: Extortion (e.g. CryptoLocker)
- **State Sponsored**
  - Very targeted attack
  - Target: IP
  - Target: System (disruption)

How we assess networks

nccgroup
freedom from doubt

Lifecycle of an infrastructure security assessment

- **Discovery** – scan the network to establish live hosts, their open ports and services exposed
- **Vulnerability assessment** – establish where security issues exist from an unauthenticated standpoint and investigate potential entry points into the network

- **Exploitation** – compromise of a host through a vulnerability, or misconfiguration
- **Post exploitation** – credential harvesting and progression through the network to achieve maximum compromise within the network boundaries of the scope

Exploitation and post exploitation

Why is it important to **exploit** vulnerabilities?

To evaluate their **risk and impact in the context of the network under assessment** and produce a high-value report to the client

External versus internal assessment

External infrastructure assessment is carried out beyond the network perimeter of the client

- Focused on services exposed to the Internet across an IP range defined by the client

Internal infrastructure assessment is carried out at the client's site, with a direct connection to the corporate network or DMZ depending on the scope

- Larger network footprint
- Greater number of exposed services
- Numerous Layer 2 and Layer 3 weaknesses and attacks

How we breach networks

- Lack of security patches
- Default credentials
- Excessive network footprint
- Lack or weak network segregation
- Exceptions
- White-listing preferred over black-listing
- More

How we breach networks

- **Lack of security patches**
- Default credentials
- Excessive network footprint
- Lack or weak network segregation
- Exceptions
- White-listing preferred over black-listing
- More

Lack of security patches

- Missing patches are easy entry points for attackers
- For a large number of critical publicly known vulnerabilities there are reliable exploits
- In a typical Windows network changes are high that one workstation will not be patched
  - Till
  - Smart card reader
  - Camera
  - Embedded devices in general

Lack of security patches – scenario

- Office-based network
  - Windows powered

- No centralized solution (e.g. WSUS) to deploy Microsoft patched onto the workstations
  - Different patching levels

- Largely outdated machines – vulnerable to reliable exploits
  - Local System is an easy win
  - Leverage foothold and compromise the Windows domain / forest

How we breach networks

- Lack of security patches
- **Default credentials**
- Excessive network footprint
- Lack or weak network segregation
- Exceptions
- White-listing preferred over black-listing
- More

Default credentials

- It is a fact that device under test are kept with default credentials
- Application servers and management interfaces too
- Wordlists of default credentials for all these are easily available
- Tools to carry on login brute-force attacks exist
  - When they do not, they are easy to develop with limited development skills

Default credentials – scenario

- DMZ environment
  - UNIX / Linux powered
- Exploitation of memory corruption vulnerabilities is not an option
  - DoS condition avoidance is mandated
- Apache Tomcat runs with default credentials admin / tomcat
  - Used to deploy a custom WAR to achieve command execution
  - Local users' password hashes dumped, cracked offline
  - Leveraged to access over SSH / Telnet the rest of the servers

How we breach networks

- Lack of security patches
- Default credentials
- **Excessive network footprint**
- Lack or weak network segregation
- Exceptions
- White-listing preferred over black-listing
- More

Excessive network footprint

- Unnecessary services are often exposed internally to the network perimeter
- Effort to maintain large heterogeneous networks leave room for oversight in network footprint
- Services that run on localhost may prove helpful to compromise further the network – post exploitation

Excessive network footprint – scenario

- Despite SSH in use, R*Services are still used for management purposes
  - Easy to brute-force ACL for R*Services remotely

- Or… NIS used to manage users centrally on a UNIX / Linux network
  - Can be queried anonymously to retrieve users' password hashes
  - Cracked offline
  - Leverage to compromise the rest of the systems

How we breach networks

- Lack of security patches
- Default credentials
- Excessive network footprint
- **Lack or weak network segregation**
- Exceptions
- White-listing preferred over black-listing
- More

Lack or weak network segregation

- Network segregation by mere DHCP netmask restriction is ineffective
- Segregating at the application layer is defective
  - Leaves room to exfiltration / tunnelling attacks
- MAC filtering is ineffective
- NAC solutions do not always guarantee network segregation / access

Lack or weak network segregation – scenario

- Two distinct Windows domains: **CORP** and GUEST
  - Not part of the same Windows forest
  - No direct access between the two networks
  - They're physically hosted in two separate buildings, different physical devices, no apparent interconnections

- Users of the GUEST domain can surf the Internet, so can users of the **CORP** domain
  - They share the same web proxy on a third network
  - This proxy is reachable by both networks
  - Hence, it can be used to pivot traffic from the GUEST network to the CORP network – `CONNECT` method (enabled by default, for HTTPS)

How we breach networks

- Lack of security patches
- Default credentials
- Excessive network footprint
- Lack or weak network segregation
- **Exceptions**
- White-listing preferred over black-listing
- More

Exceptions

- Temporary firewall rules turn permanent
- Network configurations are usually complex, undocumented and hard to maintain, hence exceptions are added and rules overwrite / duplicate one another
- Exceptions and defective regular expressions may lead to more harm than good

Exceptions – scenario

- Web management interface

- Backed by JBoss Application Server
  - Configured manually to prompt user for credentials at any unauthenticated GET and POST request

- HTTP Verb Tampering
  - Intercept the login request and replace POST with HEAD
  - Get a valid session ID tied to a high-privileged user

- Once authenticated, from the web management compromise the underlying OS

How we breach networks

- Lack of security patches
- Default credentials
- Excessive network footprint
- Lack or weak network segregation
- Exceptions
- **White-listing preferred over black-listing**
- More

White-listing over black-listing

- **Black-list** ("reject known bad")
  - Reject data matching a list of known attack strings or patterns
  - Accept everything else
  - Can hinder simple attacks and automated attack tools
  - Highly vulnerable to bypasses using encoding and other techniques

- **White-list** ("accept known good")
  - Accept data matching a list of known benign strings or patterns
  - Reject everything else
  - Highly effective method if feasible

Prioritise avenues of attack

- Abuse of intended functionality
  - Example: download of files from an anonymous FTP server
- Extended use of functionality
  - Example: using xp_cmdshell extended stored procedure on a Microsoft SQL Server
- Mature, public exploit
  - Example: exploit for MS08-067 vulnerability
- Proof of concept code
  - Example: code downloaded from exploit-db.com or other exploit repository to exploit a third-party product

Move sideways

- Once a foothold onto the target network is gained, next step is to **retain access**
  - Create an admin user, deploy a backdoor, etc.

- **Leverage access** to inspect the file system, query the DC, sniff traffic

- **Move sideways**
  - Password reuse for local OS users is a very bad practice
  - Once dumped, password hashes can be **sprayed**, no need to be cracked offline
  - Dual-homed systems – **pivot** traffic / extend control

Controls

*"Security **controls** are safeguards or countermeasures to avoid, counteract or minimize security risks relating to personal property, or any company property."*

Controls

nccgroup
freedom from doubt

Preventative

- Attempt to stop an event from occurring

Detective

- Identify and alert when the event occurs

Corrective

- Remediate after the event has occurred

Controls

Physical

- Fences, locks

Procedural

- Policies, standards and processes

Technical

- Firewalls, anti-virus, encryption

Legal and Regulatory

- Jurisdictional law, PCI-DSS

Controls

Cyber Streetwise

- www.cyberstreetwise.com

CPNI **Top 20 Controls** – based on SANS

- www.cpni.gov.uk/advice/cyber/Critical-controls/
- http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-critical-security-controls.pdf

Top 20 Controls

- Critical Control 5: Malware Defenses
  - Microsoft Security Essentials
  - Commercial solutions

- Critical Control 6: Application Software Security
  - OWASP Top 10 – www.owasp.org
  - SANS Top 25 Most Dangerous Programming Errors – www.sans.org
  - Security Development Life Cycle (SDLC)
  - Open Software Assurance Maturity Model
  - White-box and black-box assessments

Top 20 Controls

- Critical Control 7: Wireless Device Control
  - Ensure you are using WPA2-CCMP or better 802.1x EAP-TLS
  - Disable WEP
  - Disable WPS
- Critical Control 8: Data Recovery Capability
  - Test your restore functionality
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
  - User awareness training
  - Don't click on links
  - Lock workstations

Top 20 Controls

- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
  - Disable unused services
  - Limit access to services
  - Web proxy
  - Network traffic filtering

- Critical Control 13: Boundary Defense
  - Ingress filtering
  - Egress filtering

Top 20 Controls

- Critical Control 12: Controlled Use of Administrative Privileges
  - Limit service account privileges
  - Limit admin users
  - Admin users use separate account
- Critical Control 19: Secure Network Engineering
  - Segmentation
  - Segregation
- Critical Control 20: Penetration Tests and Red Team Exercises
  - Test your controls

If you do 7 things right…

1. Transparent security principle
2. Teach staff about phishing
3. Force strong password policy
4. Get rid of Windows XP, Office 2000-2007 and Internet Explorer 6-8
5. Update third-party software (Adobe, Java if needed, Firefox)
6. Use up-to-date anti-virus
7. Test your disaster recovery processes

Longer term strategies

- Perform risk assessments

- Implement a level of the 20 CSC
  - Harden devices
  - Segregate your network
  - Limit and control administrative privileges
  - Limit and control network services
  - Encrypt your USB sticks / laptops
  - Create an IR plan

Always remember

- Don’t buy product vendor hype
- Cyber security is not about products
- Cyber security doesn’t have to be costly
- An incident will likely happen so have a plan

Resources

- www.nccgroup.com
- www.cpni.gov.uk
- www.cyberstreetwise.com
- www.sans.org
- www.cisecurity.org
- www.owasp.org

Thank you! Questions?

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Milton Keynes

European Offices

Amsterdam – Netherlands

Copenhagen – Denmark

Munich – Germany

Zurich – Switzerland

North American Offices

San Francisco

New York

Seattle

Chicago

Austin

Atlanta

Australian Offices

Sydney

Contact us

training@nccgroup.com