What Audits Miss & How Penetration Testers Abuse Those Gaps

Rick Redman, Title,
KoreLogic

Governance, Risk & Compliance – G24

Intro

Rick Redman / Minga / @CrackMeIfYouCan
KoreLogic.com

Penetration Tester

Created 'Crack Me If You Can' - Password cracking contest at DEFCON

What audits miss?

My goal as a pentester:

Inform client about security risks they are **unaware** of.

Watch this talk I did about this subject in 2011.

"Rick Redman -- Tomorrow you can patch that 0day -- but your users will still get you p0wn3d"

http://www.youtube.com/watch?v=5c3rQ4rzTGI

All Fortune XXX companies have done audits.

Patching Audits, Architecture Audits, Compliance Audits... etc

So, Why are we **still** successful at penetration?

What audits miss? - Detection Ability – Will you catch me?

How will your team react?

Will they follow policy? What is the policy proper?

Does your detection technology work? 3Rd party? Have you tested your 3rd parties ability to detect internal attacks? How do they react?

Are admins/users trained on proper incident response?

Can a rogue device be detected and removed from the intranet?

Pentests are stealthy. When will your team finally catch us? During port scans? After the AD compromise? Via logs? Via behavior?

Note: Do these improve over time? How do you know?

- Stories:
  - Fortune 50 – No detection until AD compromise
  - Small company – immediate detection via portscans/cgi
  - –

What audits miss? Unsafe Architecture

- Architecture assessments help, but....
- What about the impact of bad architecture?
- How can it be used by attackers?
- Example: Webapps on port 80 – that auth to SSO/AD
- Example: Flat Enterprise Networks – HUGE risk!
- Example: Fortune XXX – Large SSO/LDAP infrastructure. SSL accelerator, but the 4 backend LDAP system were on the same flat network, and could be accessed directly. Access those systems, run a sniffer – get plain-text credentials.
- Examples: Proper 3-tier web application arch, but credentials on each tier lead to immediate compromise of next tier. (web app → middle ware → database

What audits miss? User/Administrator Behavior

- User/Administrator behavior is likely the largest risk to a network.
- Not usually the first thing we find (not the initial toe-hold)
- But, almost always is what eventually leads to complete system/network/enterprise compromise
- How do you audit for behavior? First, identify the problem behaviors
- Examples:
  - Password use/storage by users (passwords.txt .cvspass)
  - Password use/storage by service accounts
  - How do admins do their job? What is their behavior? (ssh keys? Rdesktop? Vnc? Separate accounts for user/admin?)
  - How are machines accessed? How do services access other services (LDAP / DBs)

What audits miss? User/Administrator Behavior (cont)

- Examples:
  - How do UNIX admins get root? Sudo (is a password required)? Shared password?
  - How do UNIX admins share information (email? IM? TXT files)
  - How do admins remember Administrator/root passwords?
  - Do administrators follow their own security policy? (password reuse / password changing / password complexity / etc)
  - Do UNIX admins have ssh private keys? Encrypted?
  - Do users/admins stored sensitive data (files with credentials) on network shares?
  - Are admin workstations firewalled / separated from the network?
  - What UNIX commands are people running? Are they doing them safely? (ex: passwords on the command line)

What audits miss? User/Administrator Behavior (cont)

- So how do you learn about (and audit) user/administrator behavior?
- Either:
  - 1) Ask them. Believe them. Don't audit. Trust administrators / users fully to not place network at risk.
  - 2) Perform an audit yourself looking for unsafe behavior.
  - 3) Actually perform a penetration test. Have a “bad guy” learn the most egregious techniques used by users/administrators. Provide examples and recommendations for fixing / preventing / training / mitigating the examples found.

What audits miss? Passwords!

- Passwords are a huge risk to the network
- Password policy is supposed to make stronger passwords – but it does not!
- Password rotation (every 30/90 days) introduces vulnerabilities for date-based passwords and simplistic rotations
- This does NOT occur on Internet-based passwords because Internet sites don't required password changing.
  - Summer2013 Spring2013 Winter2013
    - (Wireless assessment story goes here).
  - GreatPass1 GreatPass2 GreatPass3 ….
- What happens if I find an “old” password for California2012?

What audits miss? Passwords!

- Finger patterns – q1w2e3Q!W@E# qwe123QWE!@# Qwer!@#$!Qwerty1 iop890IOP*()
- If you require a special character – it is almost always going to be the **last** character of a password.
- Which special characters? There is logic to this. ! @ # $?
- If you require a number – it is almost always going to be at the end as well. Which numbers? 1 2 123 2013 2012 etc
  - Password1 Summer13 SanFrancisco123
- Administrators will use the same password (or a simple variation) for the admin and non-admin account. (How do you test for this? Are they going to tell you?)
- Are your users using these patterns? How do you know?

What audits miss? Passwords!

- What about patterns? We are human after all.
- Example: Oakland1 - Notice location of upper case / number
  - U L L L L L L D (U = Upper L = Lower D = digit)
- Spring13 – U L L L L L D D
- Love1234 – U L L L D D D D
- Fall2012! - U L L L D D D S (S = Special Character)
- There patterns are **universal** across enterprise networks!
- “No” tool prevent users from choosing passwords based on patterns.
- Are your users using these patterns? How do you know?

What audits miss? Passwords!

- These patterns are not only universal, they speed up the cracking/attacking drastically.
- For 9 character passwords: (8 characters is too easy).

ULLLLLLLD	Abcdefgh1
ULLLLDDDD	Abcde1234
ULLLLLLDD	Abcdefg12
ULLLLLDDD	Abcdef123
ULLLDDDDS	Abcd1234!
ULLLLLDDS	Abcdef12!
SULLLDDD	!Abcd1234

What audits miss? Passwords!

Very large company - 100% passes meet complexity requirements.

263356 of 263888 logins cracked - 7308 Patterns Found

Most Popular Patterns:

33458 ULLLLLDD (8 characters) 12% of cracks! 33,000+ passwords

33394 ULLLLLLDD (9 characters) 12% of cracks!

27898 ULLLDDDD 19190 ULLLLLLLDD

The first pattern, used 33,000+ times – cracks in 4 seconds.

The top 5 patterns – used by 48% of the time – cracks in about 15 min

The top 100 patterns – are used by 85% of the users – takes a few hours to crack

What audits miss? Passwords!

Example 2:

Large SSO for an enterprise – 449,000+ users

19200 ULLLLLDD (used by 4.3% of users) ex: Sanfra13

17914 ULLLLLDDS ex: Sanfra13!

14025 ULLDDDDS ex: San1234!

12477 ULLLLLDS ex: Sanfra2!

9216 ULLSDDDD ex: San!1234

Top 5 patterns - used by 16% of users.

Top 100 patterns – used by 62% of users. (vs. 85% in previous example)

What audits miss? Wrapping up Password discussion.

- Your users **are** choosing bad passwords.
- Trust, but **verify**, the password methods used by users / administrators. Prevent users from choosing trivial passwords
- They are “simple” to audit. (We can help)
- Repeatable process – easy to show improvement over time. (percentage cracked should go down).
- No denying their importance in the security realm. Every one uses a password. But are they using them properly?
- Multiple methods of mitigating risk. Improve complexity rules, training of users, reward users with strong passwords, etc.

What audits miss? Patching

- I trust the audit teams to deliver reports on what patches have not been installed. This is not the job of pentesters.
- But how do you rank importance? Risk? Threat?
- Easy to defend a 'dev' machine missing patches – but what if it shares the same passwords with the 'prod' system?
- Is that system as important as a prod system?
- Is the risk higher? The threat?
- During pentests – 'dev' systems are used to gain a 'toe hold' onto the network. Since 'dev' machines are managed by the same team that manages 'prod' – anything we learn about how systems are used/managed/access will likely apply to 'prod'.

What audits miss? Home Directories

- During pentests, home directories and file-shares (such as $HR used by HR department) are harvested for information.
- What do people do/store when they think no one is looking?
- Are users storing sensitive data?
- Is it encrypted?
- Do the proper users have access to these files? Do the non-proper users have it as well?
- Is the contents of these directories audited routinely for unsafe content?
- Does the configuration of home directories (such as via NFS) place the entire infrastructure at risk? (Hint: It does).

What audits miss? Internal Web Sites

- Audits will likely return a list of intranet web-sites, but what data is **on** those sites?
- Is any of it sensitive? Would it be useful to attackers?
- Can any of it be used by a “bad guy” to gain access to other resources?
- Are proper credentials required to access any internal site with sensitive data? (“sensitive” to auditors and pentesters might be different. Ex: system info – lists of users – documentation, etc).
- Example: SVN/CVS example from 2013
- Example: Edward Snowden. Used “other peoples” credentials to gain access to sensitive data. This made the audit trail of his activities very hard to follow. How did he obtain these other credentials?

What audits miss? Internal Web Applications

- Internal web applications are rarely assessed for web-based vulnerabilities
- Internal web applications are usually more vulnerable to web-based attacks
- Example: SQL injection/Command Injection/Source Disclosure
- Can lead to system compromise on critical intranet systems.
- This can be an initial toe-hold on important intranet systems
- Not likely to be seen in log files by administrators
- Not likely to be seen by IDS (if using HTTPS/SSL)

What audits miss? MISC:

- What is the impact of out-of-date Java?
- Domain Policy? LANMAN? Who can log into domain controller? Who has terminal services access?
- Are Admin:500: password the same on all workstations? Are they they same as the servers?
- Outbound firewall rules?
- Documentation reveal any credentials?
- How are routers/switches set up / managed / authenticated?

Questions ?

Comments ?

What audits miss?