The L@m3ne55 of Passw0rds: Notes from the field

Ben Williams
Senior Security Consultant

Previously

- Presented at various conferences including BlackHat and other smaller conferences in Europe
  - Exploitable vulnerabilities security appliances
  - Enumerating internal security products/policy externally

What we are covering today

- The experience of breaking into networks and applications with a variety of password attack tools and techniques
    - only a tiny part of what we do… but…
- What works and why
- Demos
- Advice

Password Attacks are not new, but…

- Things are much the same for the defender
  - Adoption of 2FA is slow and compartmentalised
  - Users choose passwords
- Regular iterative improvements for the attacker
  - New attack techniques
  - Improved tools and frameworks
  - Improved methodology and resources
  - Moore’s law of processor improvements
  - Network bandwidth improvements
  - Tor and botnets

External Demo

External Enumeration and Attacks

- External enumeration
  - Password dictionary data
  - Internal usernames, hostnames and IP addresses
  - Email addresses, and formats
  - LinkedIn, Facebook etc.
- Attacks
  - Web applications with password authentication
  - VPN, Portals etc
  - Phishing (fake portal, outlook web access, whatever)

Demo External Enumeration

Demo External Attack

Account lockout != Bruteforce protection

- Password policy + account lockout + timeout
  - Temporary locks often lead to user enumeration
  - Attacker would likely gain access to the application

- Password policy + account lockout + manual reset
  - Attacker could gain access to the application if they can enumerate enough real users separately
  - Account lockout DoS

- Password policy + account lockout + timeout + brute-force protection
  - Can be very resilient, but unauthorised access may still be possible

Internal Demos

Internal Domain 1: Initial access

- Unauthenticated enumeration
  - Find the DCs, Workstations and Servers
- Low hanging fruit
  - Weak credentials: admin/admin, anonymous ftp and shares, snmp public/private, sa/<blank>, tomcat jboss
- Unauthenticated attacks
  - Enumerating users
  - Collecting hashes with NetBIOS/NBNS Spoofing
  - Small targeted password attack

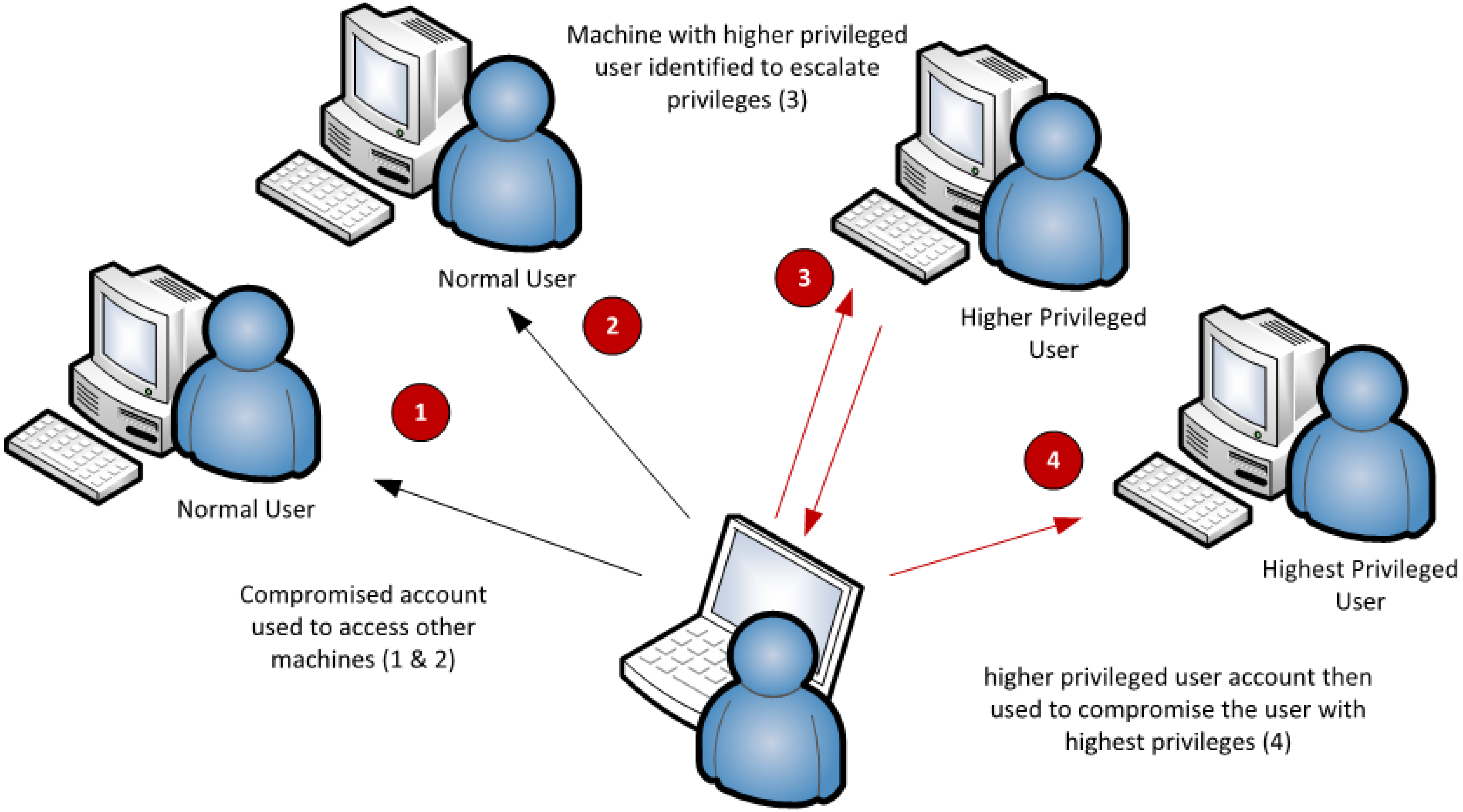
Demo Phase 1

Internal Domain 2: Authenticated enumeration

- Authenticated enumeration
  - Identify password policy
  - Identify all users, administrators and systems
- Moderate targeted password attack
- For the credentials we have
  - Where can we login?
  - What access do we have?
- Collecting more credentials
  - Hashes
  - Plaintext passwords

Demo Phase 2

Hopping from system to system



Machine with higher privileged user identified to escalate privileges (3)

Normal User

Normal User

Higher Privileged User

Highest Privileged User

Compromised account used to access other machines (1 & 2)

higher privileged user account then used to compromise the user with highest privileges (4)

Internal Domain: Getting Domain Admin

- Have a coffee and repeat
  - Iterative process
  - Workstations > Servers > Domain controller
  - Scale makes it easier

- Keep going…
  - Where can we login?
  - What access do we have?
  - Collect more credentials
  - Repeat

Internal Domain 3: Beyond Domain Admin

- Active Directory Passwords
  - Dumping and cracking hashes
- What about the ones I can’t crack?
  - Find where the admins are logged in
  - In memory Mimikatz DLL injection
- Now we have lots of passwords: Hit the other infrastructure
  - Firewalls, switches, routers, appliances
  - Basically everything, but how far do you want to go?

Demo Phase 3

Access all areas

- Domain Admins, and all user hashes
    - Can reuse hashes, don’t need to crack
    - Krbtgt hash – Golden ticket attack
- Cracking passwords, to compromise non-Windows resources
    - Unconnected Web applications
    - Appliances, network kit, other infrastructure
    - Third party systems

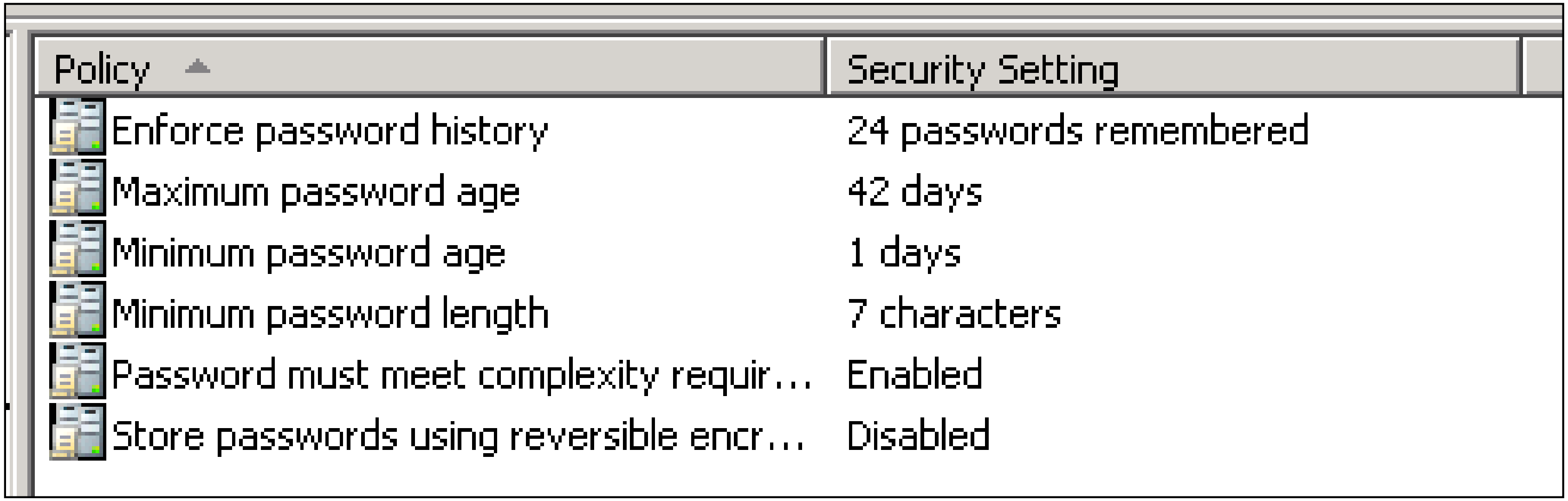
Password Stats from Real Tests

- This is a representative composite example from several tests

Top 10 passwords	Number
Welcome123	53 (5.8%)
Password1	15 (1.6%)
Changeme2013	10 (1.1%)
<obscure complex password>	9 (1.0%)
<football team>	8 (0.9%)
Monday1	8 (0.9%)
password	7 (0.7%)
<company reference>	6 (0.6%)
P@ssw0rd1	6 (0.6%)
Summer2014	5 (0.5%)

What about password policy

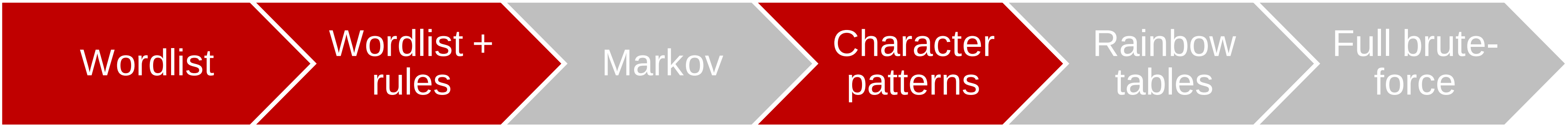
- What are the important factors in password policy?



Policy	Security Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requir…	Enabled
Store passwords using reversible encr…	Disabled

Hash cracking process

- A structured process gets results fast



Wordlist

Wordlist + rules

Markov

Character patterns

Rainbow tables

Full brute-force

- Wordlists are huge, and based data from real compromises
- (Many millions of real users passwords)
- Character patterns – most statistically relevant first

- Crack speed depends on hash algorithm

Statistical analysis of passwords

- 50% passwords follow 13 basic rules
- For example
  - ?l?l?l?l?l?l?l
  - ?u?l?l?l?l?l?n
  - ?u?l?l?l?l?l?l?n
  - ?u?l?l?l?l?n?n?n?n

- Good resources for further reading:
- http://www.praetorian.com/blog/statistics-will-crack-your-password-mask-structure
- http://wpengine.com/unmasked/
- http://www.datagenetics.com/blog/september32012/

How real users interpret password rules

“Passwords must contain at least 1 upper, 1 lower, 1 number, and be at least 7 characters long”

- Take a base word of 6, 7 or 8 characters
- Chose only one upper
- Make first character upper
- Add numbers on the end (one, two, or four numbers)
- Or, substitute numbers and symbols for letters which look like numbers and symbols (“P@ssw0rd!”)
- For password changes, users increment the number: "Manunited1!", "Manunited2!", "Manunited3!"…

NCC Group: Passcrack

- Two nodes, approximately £2500 for hardware
  - Each about the price of a fast gaming machine
  - + 1 Consultants time for building it
  - Currently using 5 graphics cards between the two
  - Not “nation state” level by any means

EVGA

SILVERSTONE
Designing Inspiration
STRIDER GOLD
Evolution
1200W
80 PLUS GOLD
MODEL NO: SST-ST1200-G
1200 WATT Active PFC SWITCH POWER SUPPLY
CAUTION! HAZARDOUS AREA
RADEON
RADEON

NCC Group: Passcrack

- Up to 100 billion password guesses per second
- Do you think your current password would be resilient?
- Do you think you could choose one that is?

How you could interpret password rules

“Passwords must contain at least 1 upper, 1 lower, 1 number, and be at least 7 characters long”

- Take two or three base words (10 – 15 characters, more?)
- Chose multiple upper and spread them around
- Put your numbers in different places
- Don’t use predictable L337spe@k
- When you need to change your password, actually change the base words, and use different base words for each application/site

- Examples: “£$9ThisisNotharD”,“doesnothAvetobe2cOmplex”

Make Password Attacks Harder (Top 10)

- 2FA or brute-force protection on external apps/portals
- Increase the length of passwords to 10+
  - Include user education
- Remove low hanging fruit
  - Weak credentials: admin/admin, anonymous ftp and shares, snmp public/private, sa/<blank>, tomcat jboss etc.
- Remove all legacy Windows systems: 2000, XP, 2003
- Regularly identify and disable unused user accounts
  - Ongoing maintenance task
- No service accounts in “Domain Admins” group
  - Membership of this group should be very restricted

Make Password Attacks Harder (Top 10)

- Mitigate NBNS spoofing
  - http://www.leonteale.co.uk/netbios-nbns-spoofing/
- No common local administrator account passwords
  - Microsoft LAPS:
  - https://technet.microsoft.com/en-us/library/security/3062591.aspx
- Active Directory password audit
  - Remediate accounts with weak passwords
- Internal network segregation
  - Separate Workstations from Servers (internal filtering)
  - Host-based firewalls
- Don’t give users “local administrator” access

www.nccgroup.com

ben.williams(at)nccgroup.com

@insidetrust

For more information see nccgroup blog post

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Thame

European Offices

Amsterdam - Netherlands

Munich – Germany

Zurich - Switzerland

North American Offices

San Francisco

Atlanta

New York

Seattle

Australian Offices

Sydney