Brute Force

n n a m a m a u m



"What is Brute Force"

- Attempting to guess the correct secret by trying all, or a chosen subset of all, possible options
- Does not try to crack the pass phrase, rather tries to guess/duplicate it
- Runs through the entire available keyspace
- One of the oldest and easiest types of attack vector
- Generally viewed as the easy way in, a sign of a script kiddie
- Has spawned various derivatives
 - Dictionary
 - Hybrid
 - Rainbow

n а m a m \mathbf{a}



"Explain Keyspace"

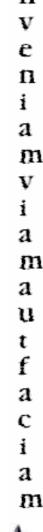
- Keyspace is the number of possible combinations a secret requires
 - alphabetic lowercase password of 6 characters..
 - that's 308915776 combinations
 - brute forcing at 10,000 a second = 8.5 hours maximum
 - alphanumeric lowercase password of 6 characters..
 - that's 2176782336 combinations
 - brute forcing at 10,000 a second = 2.5 days maximum
 - alphabetic lowercase password of 8 characters..
 - that's 208827064576 combinations
 - brute forcing at 10,000 a second = 241.6 days maximum
- Bear in mind that these calculations do not account for..
 - weak password implementations
 - brute force attempts greater then 10,000 a second
 - finding the password halfway through the process

n \mathbf{a} m a m а



"Why is it Dangerous?"

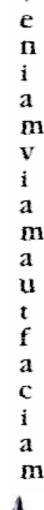
- Requires very little technical skill
- There are many advanced tools out there
- All public or server-client services require some sort of authentication
- Attacks the weakest point in security human nature
- Even now many people under estimate it effectiveness
- As technology advances, previously impossible scenarios become possible
- It is very difficult to stop because it is legitimate traffic





"Is it really that bad?"

- Some of the more dangerous programs include..
 - Hydra
 - John the Ripper
 - Cain and Abel
 - Brutus
 - LCPCrack
- It is also trivial to get dictionaries and wordlists for any occasion
- I was going to show how each tool can work, but I figured I would rather demonstrate how I used these methods in a recent pentest..
- <Jump to.."What-Me-Worry.doc">



n



- Everything we gone through so far most of you probably knew, but..
- Quantum computing
- Computational timings
- Distributed computing
- Randomality creation
- Normal Progress More bandwidth and Moore's law
- And it will carry on..

n a m m



"What can be done to protect against it?"

- Understanding
- Proper passwords
- Multi-factor authentication
- Extras Like port-knocking for example
- Stricter access where possible regarding origins and lockouts
- We need to be able to think laterally "out of the box" as it were
- Properly configure public facing services
- Check logs
- Educate users

n \mathbf{a} m



Thank you for your attention

Hydra - http://thc.segfault.net/thc-hydra/

John the Ripper - http://www.openwall.com/john/

LCPCrack - http://www.lcpsoft.com/english/index.htm

Rainbow Crack - http://www.antsight.com/zsl/rainbowcrack/

Cain and Abel - http://www.oxid.it/cain.html

Brutus - http://www.hoobie.net/brutus/brutus-download.html

Wordlists - http://www.openwall.com/passwords/wordlists/

Wordlists - http://coast.cs.purdue.edu/pub/dict/

Wordlists - http://www.dcs.shef.ac.uk/research/ilash/Moby/

 \mathbf{n} n a m a m a u

