SANS Hackfest

Secret Pentesting Techniques Part 2

Dave Kennedy
Founder, CEO
Twitter: @TrustedSec, @Binary_Defense @HackingDave
David Kennedy’s Background

• Founder of TrustedSec.
• Co-Founder and CTO Binary Defense Systems
• Co-Founder of DerbyCon
• Former Chief Security Officer for Diebold Incorporated
• Testified on Congress twice – numerous media interviews with Fox News, CNN, CNBC, Bloomberg, Huffington, BBC, and more.
• Creator of The Social-Engineer Toolkit (SET), Fast-Track, Artillery, exploits and open source.
• Co-Author of Metasploit: The Penetration Testers Guide.
• U.S Marine – Deployed to Iraq a few times.
Agenda

• Break some stuff..

• Different techniques.

• Thinking and framing yourself as an attacker.

• Have fun.
An an attacker

• It’s important for us to figure stuff out. Do things that are different.

• Using a tool is fine, writing the technique makes it fun.
An attacker (cont)

• It’s our job to make security better.

• Not just about owning, but also about teaching.
Story 1

• Large FI institution – mobile app assessment.

• Mobile apps are great.
From App to Shell

- Hardcoded master password stored encrypted in sqlite database.

- Encrypted but decrypt function was easy.
PowerShell Fun

• We still have Windows XP out there? Hurry up and patch.

• Shifting all malicious software to PowerShell is happening.
First my favorite – Unicorn

- Powershell Injection on steroids. (thanks Matthew Graeber)

- Why not mess everything up: AV, Application Whitelisting, NextGen and more.
PSEXEC_COMMAND PSH - Sidebar

- Ability to spray network with non-disk touching attacks.
- Already built into SET.
- Easy to use once hashes have been extracted.
Metasploit Issues

• Metasploit payloads rock – meterpreter is our go to.

• Second stage getting picked up in most cases.

• Can use EnableStageEncoding or do something custom 😊
Meterpreter over SSH

• Releasing code today
  – Paramiko (Python) module for SSH.

• Demo
Jacking with IR

• Get shells out, spawn new ones to legitimate business domains.
Story 2

• Oh Citrix.

• SET -> Java Applet -> Compromised Limited User Account.

• Access to like nothing.
IBM Communicator

• Noticed Processes with meterpreter that had no name associated.

• Migrated to process – now running as that user.
Yikes.

- Can authenticate to anything.
- RPC/SMB restricted.
- No pass the hash, no mimikatz fun - patched wdigest removal :(
- Kerberos tokens maybe, but still can’t connect to anything.
Main Specs

- 32GB Corsair Dominator Platinum DDR3-2133 (4x8GB)
- Seagate 2TB Seagate Barracuda 7200RPM (x4 raid)
- Asus Rampage IV Black
- Intel Core i7 4930K Six-core
- 4x AMD Radeon R9 290x 16GB GDDR5
- 1500 Watt EVGA SuperNova 80+ Power Supply
Benchmarks

• NTLM – 92.3 billion per second NTLM hashes.

• Cracks 9 character password in less than twenty minutes.

• 8 characters in few mins.
Cracked Password

• Password cracked *yay*.

• Go to authenticate VPN.

• Phone Factor – 2 factor auth.
RID Reversal

- Olllllddd school but made cool again.
- Targeting member servers.
- Chill while spilling the beans.
RIDENUM

• Most companies have prevention for null session RID cycling through domain controllers BUT – you can use a trusted connection from an already joined workstation/server to ride that connection to enumerate users if it isn’t applied domain wide.
Other fun things
SET v6.0.5
The Toolkit v6.0.5

• Ability to create fast and effective phishes to attack an organization.

• Ability to attack an organization and simulate a real-world example.
Warning!

• This is just a tool.

• Using this out of the box probably won’t be successful.

• Need to research who you are going after, and how you are going after them.
Proper OSINT/Recon/Homework

• Research your targets.

• Know your targets.

• Develop your attacks based on your target.
“Try not to become a man of success, but rather try to become a man of value.” – Albert Einstein
John Strand’s Pentesters Code of Ethics

- I will never copy and paste automated results
- I will never completely trust scan results
- I will strive to get caught (after being awesome)
- I will go beyond the scan results
- I will be a hacker in the original sense of the word
- I will always stay in scope
- My reports will rock
- I will always improve the security of my customer and make them better (added one)