Adventures in Hacking
Fortinet Intro

BROAD
Visibility of the entire digital attack surface

INTEGRATED
AI-driven breach prevention across devices, networks, and applications

AUTOMATED
Operations, orchestration, and response
Agenda

- What’s at stake
- Information Gathering Techniques
- Advanced Attacks
- Best Preventative Practices
- FAQs
What’s At Stake

• Moss Adams [2019-12-29 ]
  One of the largest public accounting firms in the United States, Moss Adams, has suffered a data breach.
    Exposed names and SSNs

• Landry’s Inc. – [2020-01-05]
  Landry’s Inc., a Houston-based company behind more than 600 restaurants, hotels and casinos in the United States, warned customers about a data breach that could have compromised credit card information.
    Landry's, which owns restaurants like Bubba Gump Shrimp Co., Joe's Crab Shack and Saltgrass Steak House, warned customers after a data breach may have compromised credit card information.
What’s At Stake

Examples of sensitive information collected through ethical hacking:
• Administrator access
• Employee names, addresses, SSNs
• Images of digital signatures
• Images of cancelled checks
• Proprietary intellectual property
• Access to Customer B via Customer A
• Access to IP Surveillance Cameras
What’s At Stake
What’s At Stake
What’s At Stake
Agenda

- What’s at stake
- Information Gathering Techniques
- Advanced Attacks
- Best Preventative Practices
- FAQs
Information Gathering Techniques

- Google:
  - Intitle
  - Inurl (next slide)
- Dating site?
- Whois
- NSLOOKUP
- Port Scanning
- Company Website
- Phishing
- Social Engineering
- Resumes?!?!!
Whois

inetnum: 195.196.34.0 - 195.196.36.255
netname: PAJALA
descr: Pajala Kommun
country: SE
admin-c: FK176-RIPE
tech-c: MM8452-RIPE
tech-c: FK176-RIPE
tech-c: SP2768-RIPE
status: ASSIGNED PA
mnt-by: BD-NOC
created: 2004-09-08T06:40:20Z
last-modified: 2004-09-08T08:27:17Z
source: RIPE
Agenda

• What’s at stake
• Information Gathering Techniques
• Advanced Attacks
• Best Preventative Practices
• FAQs
Advanced Attacks (Custom Programming for Reconnaissance)
Advanced Attacks (Custom Programming for Reconnaissance)
Advanced Attacks (Building The Pieces)

• Run WireShark (packet sniffer) while performing an action (POST as an example)
• If necessary, build a similar environment in a lab
• Use WebRequest POSTer / Recorder to tweak variables until you learn what does what

• Example:
• http://www.<removed>.com/<removed>/AddScore.asp?s=7221&n=Name&l=20&m=pas
dsword-string?
  • S = score
  • N = name
  • L = level
  • M = Possible password string (weak security, but certainly eliminates n00bs)
Advanced Attacks (Custom Programming in Action)

• Per hour: 33,000 attempts
• Weekend: 2.4 million attempts (usually compromising 50 to 60 accounts)
• This customer had about 20,000 employees, so the “Speed” (throttling) bar allowed me to get around account lockout.
Advanced Attacks (Volume Attacks)

mastermind

Is NOT a good password!
Advanced Attacks (Decompiling Intermediate Language)
Advanced Attacks (Decompiling Flash Applets)
Agenda

• What’s at stake
• Information Gathering Techniques
• Advanced Attacks
• Best Preventative Practices
• FAQs
Best Preventative Practices

• Technical Best Practices
  • Security devices should communicate with each other (APIs, etc.)
  • Use full SSL inspection (if the firewall can’t see it, it can’t block it)
  • Incorporate automation into everything you do
  • Know what is visible and accessible from the Internet
  • Ensure those services are always up to date with any vendor security patches

• Information Security Program
  • Two-factor authentication
  • Password management databases (security questions? Example being...)
  • Corporate policies (that influence user behavior)
  • Risk assessment / management
Agenda

• What’s at stake
• Information Gathering Techniques
• Advanced Attacks
• Best Preventative Practices
• FAQs
FAQs

• Q: Why would a hacker pick my company? We are small and in the middle of nowhere.
  • A: This does not matter. A hacker may target a particular piece of software / hardware to make a name for themselves (“I broke into X Exchange Servers last night (inurl: /SomethingExploitable.asp)

• Q: I have account lockout turned on. Am I safe?
  • A: NO!!! “Volume Attacks”, “Timed Attacks” (all logical attacks) can be carried out.

• Q: I went to Google and searched for “ABC Exploit” or “XYZ Brute Forcer” and nothing came up. Am I safe?
  • A: NO!!! True Hackers are programmers. They know how to determine if an exploit will work (minimal reconnaissance) and know how to carry it out.

• Q: Have I ever been hacked into?
  • A: The wrong answer to this question is “No”. The more appropriate answer is “Not that I know of...”