You Will Get Owned in 2016

What are you going to do about it?

Who Am I

Penetration Tester - https://www.asgconsulting.co/

Developer - https://github.com/averagesecurityguy

Author - https://averagesecurityguy.files.wordpress.com/2015/01/hack-yourself-first-final.pdf

Who Am I

Speaker - https://github.com/averagesecurityguy/presentations

Blogger - http://avergsecurityguy.info

Get in Touch

Twitter: @averagesecguy

IRC: avrgsecguy

Email: stephen@averagesecurityguy.info

How Will You Get Owned?

Phishing Attacks

Web Application Vulnerabilities

Insider Attacks

Now What?

Fight back. Take control of your network and applications. Make the attacker work for every foothold, struggle for every machine, and fight to keep control.

Phishing

Phishing is one of the easiest ways to get into a company. With the right message, you can get 10 - 20% of people to visit a website or run an executable.

Phishing is one of the least tested attack vectors. It is very rare for a company to request social engineering and/or phishing in an engagement.

Phishing

https://github.com/tatanus/SPF

http://www.phishingfrenzy.com/

http://averagesecurityguy.info/2014/08/18/gone-phishing/

https://github.com/elceef/dnstwist

Phishing Protection

Teach your users how to spot a phishing email.

Verify they can spot a phishing email by phishing your users.

Keep your machines patched.

Run EMET.

Phishing Protection

All end user DNS traffic should be forced to go through a DNS server you control. DNSMasq will allow you to log every query and reply.

DNSMasq will also allow you to block specific domains like those generated by dnstwist.

Force all web traffic through a proxy server so you can log requests.

Web Application Vulnerabilities

Web applications are everywhere and most of them are poorly written. The OWASP Top 10 List from 2004 included Cross-Site Scripting (XSS), SQL Injection (SQLi), and Command Injection. The current OWASP Top 10 still includes all three.

The recent VTech breach was made possible by SQL Injection.

Web Application Vulnerability Protections

Do not hire developers who are not familiar with XSS, SQLi, and how to prevent them.

Train your developers on the rest of the OWASP top ten.

Build a software development life cycle with security baked in. At a minimum, introduce coding standards and source code reviews.

Web Application Vulnerability Protections

Every major language/framework has built-in features to prevent XSS and various code injection techniques. USE THEM.

Any developer who concatenates user input directly into a string should be retrained, disciplined, and then fired.

Have your web applications tested routinely by qualified testers.

Insider Attacks

Insiders still account for a large number of data breaches. Insider attacks could come from employees who have access to data they should not, employees whose access is not properly revoked after they leave, or rogue system administrators.

Insider Attack Prevention

Remove administrative privileges from end users.

Use different local admin passwords for each machine.

Limit the number of Domain Admin/Root users. Domain Admins do not need access to everything.

Insider Attack Prevention

Each admin should have their own account, no shared passwords.

Use appropriate permissions on network shares and review the permissions regularly.

Monitor anomalous outbound data transfers.

Develop a process for revoking employee access upon departure and FOLLOW IT.

Ain't Nobody Got Time For That

Make time by learning to automate common tasks like account creation/deletion, permissions audits, configuration audits, and hardware/software provisioning.

Learn a scripting language like PowerShell, Bash, Python, or Ruby.

Ain't Nobody Got Money For That

EMET - https://support.microsoft.com/en-us/kb/2458544

Artillery - https://www.binarydefense.com/project-artillery/

Ain't Nobody Got Money For That

LAPS - https://technet.microsoft.com/en-us/library/security/3062591.aspx

PoshSec - https://github.com/PoshSec/PoshSec

Questions

If you have any questions please feel free to contact me. I'm always happy to talk information security.

Twitter: @averagesecguy

IRC: avrgsecguy

Email: stephen@averagesecurityguy.info