CrucialLogics
consulting with a conscience

Packetlabs

The Cybersecurity Experts:

Amol Joshi
Chris Diachok

Richard Rogerson
Ian Lin

hack me

if you can

Thank you for joining us today!

- This session is being recorded for replay
- Listen-only mode during the presentation
- Ask questions! Please submit questions via the chat

But First, The Facts

Cybercrime is now considered the most serious economic and national security challenge

$6T

Expected global losses in 2021

80%

IT executives that believe they have insufficient protection

64%

Increase in email attacks in 2020

Speaker

Amol Joshi

Partner Enterprise Services, CrucialLogics

Amol is a senior security executive with over 16 years of experience in leading and executing complex IT transformations and security programs. He's a firm believer in achieving security through standardization, avoiding complexity and that security be achieved using native, easy-to-use technologies. Amol approaches business challenges in a detail-oriented way and demonstrates quantifiable results throughout the course of highly technical and complex engagements.

Speaker

Chris Diachok

Principal Consultant Enterprise Solutions, CrucialLogics

Chris is a senior IT professional with 25+ years of experience. Chris's diverse IT experience emphasizes Microsoft platform systems, networking, design, engineering, installation/implementation, integration, security, and administration in large, complex Fortune 500 companies and mid-size organizations with diverse datacenter and branch environments.

Speaker

Richard Rogerson

Managing Partner, Packetlabs

Richard leads a team of ethical hackers who find critical vulnerabilities in client systems before a breach. He has 10+ years of professional consulting experience delivering and leading offensive campaigns. He has several of the most advanced cybersecurity certifications and has been featured in the media several times for his views on cybersecurity breaches including Business E-mail Compromise, Ransomware and Nation-state APTs.

Speaker

Ian Lin

Tech Lead, Packetlabs

Ian has experience in a wide variety of security projects. When he isn’t in someone else’s network, he is actively researching and advancing the team's methodologies and offensive tradecraft. Aside from that, he has a knack for catching penetration testers and adversaries inside a client's network.

Today's Agenda

- A checklist of quick fixes you can implement yourself
- 6 tips from the experts
- Microsoft Defender for Endpoint
- Pentest-as-a-Service and continuous compliance

Your Checklist

- [x] Multifactor authentication using modern authentication
- [x] Endpoint management with all the security best practices (BitLocker, AV updates, patch management)
- [x] Disable legacy protocols
- [x] Periodic patching and firewall update cycles
- [x] Conditional access
- [x] Periodic penetration and vulnerability assessments

Insecure Active Directory Permissions

What is it?

- Storing passwords in the Active Directory description fields
- Overly permissive Active Directory Discretionary Access Control Lists (DACLs) and Access Control Entries (ACEs) that allow unprivileged groups to take over privileged accounts

Remediation

- Audit and script period review of description fields
- Baseline security permissions with AD ACL Scanner tool and review periodically

SMB Relay Attack Vulnerability

What is it?

- SMB signing is a security mechanism that allows SMB packets to prove/enforce their integrity (meaning that they have not been modified in transit), and is a setting that is not turned on by default for most servers (except DCs)
- Forced authentication in shared folders or writable shares
- Captured hashes can be redirected to servers without SMB signing leading to unauthorized access

Remediation

- Implement security baseline GPO's
  - NTLMv2 | Disable anonymous SMB | Remove SMBv1
- Audit shares on periodic basis for miss configuration

CrucialLogics
consulting with a conscience™

Multiple Uses of Local Administrator

What is it?

- The same administrator account name and password exists on multiple computers
- The same account can be used to login to multiple systems
- The compromise of one endpoint/server leads to the compromise of all systems

Remediation

- Disable and remove all local admin access (if possible)
- Implement Local Administrator Password Solution (LAPS)

Cached Credentials

What is it?

- Domain administrators or privileged accounts login to untrusted systems (servers, workstations, non-DCs)
- Organizations that leverage the use of RDS servers that lack or have insufficient hardening processes
- Broken/Inadequate AV/EDR measures that allow privileged users to access areas of the operating system where credentials/hashes reside

Remediation

- Implement tiered access by delegating roles (e.g. Server Admin, Workstation Admin) and PAW
- Implement security baseline GPO's
- Implement Microsoft Defender for Endpoint (AV, EDR)

Broadcast and Poisoning Attacks

What is it?

- Impersonating different services and force users to access our services through legacy protocols (e.g. LLMNR/NBT-NS/mDNS) to capture hashes/relay credentials
- Hijack workstation DNS servers and serve malicious WPAD files (DHCPv6) to capture hashes/relay credentials
- Spoofing SSDP and uPnP devices to coerce forced authentication to capture hashes/relay credentials

Remediation

- Mitigation with GPO and scripting (Disable NetBIOS over TCP/IP)
- Add an entry for “wpad” in your DNS zone | Disable TCP/IPv6 (if possible)
- Disable UPnP devices | Monitor network for passwords in cleartext

CrucialLogics
consulting with a conscience™

Active Directory Forests as Security Boundary

What is it?

- Too many two-way trusts or trusts without proper security controls
- If an attacker can compromise a single machine with unconstrained delegation (e.g. Domain Controller) in a foreign forest, this can be leveraged to compromise your primary forest and every domain within it

Remediation

- Implement a selective domain trust to limit trusted users and groups or remove two-way trust (if possible)
- Ensure SIDHistory and SIDFiltering is configured properly for the trust
- Disable Kerberos delegation where possible
- Enable “Account is sensitive and cannot be delegated” for high privileged accounts

CrucialLogics
consulting with a conscience™

Microsoft Defender for Endpoint

Built-in. Cloud-powered.

ATTACK SURFACE REDUCTION

Resist attacks and exploitations

NEXT GENERATION PROTECTION

Protect against all types of emerging threats

ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks

AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale

SECURITY POSTURE

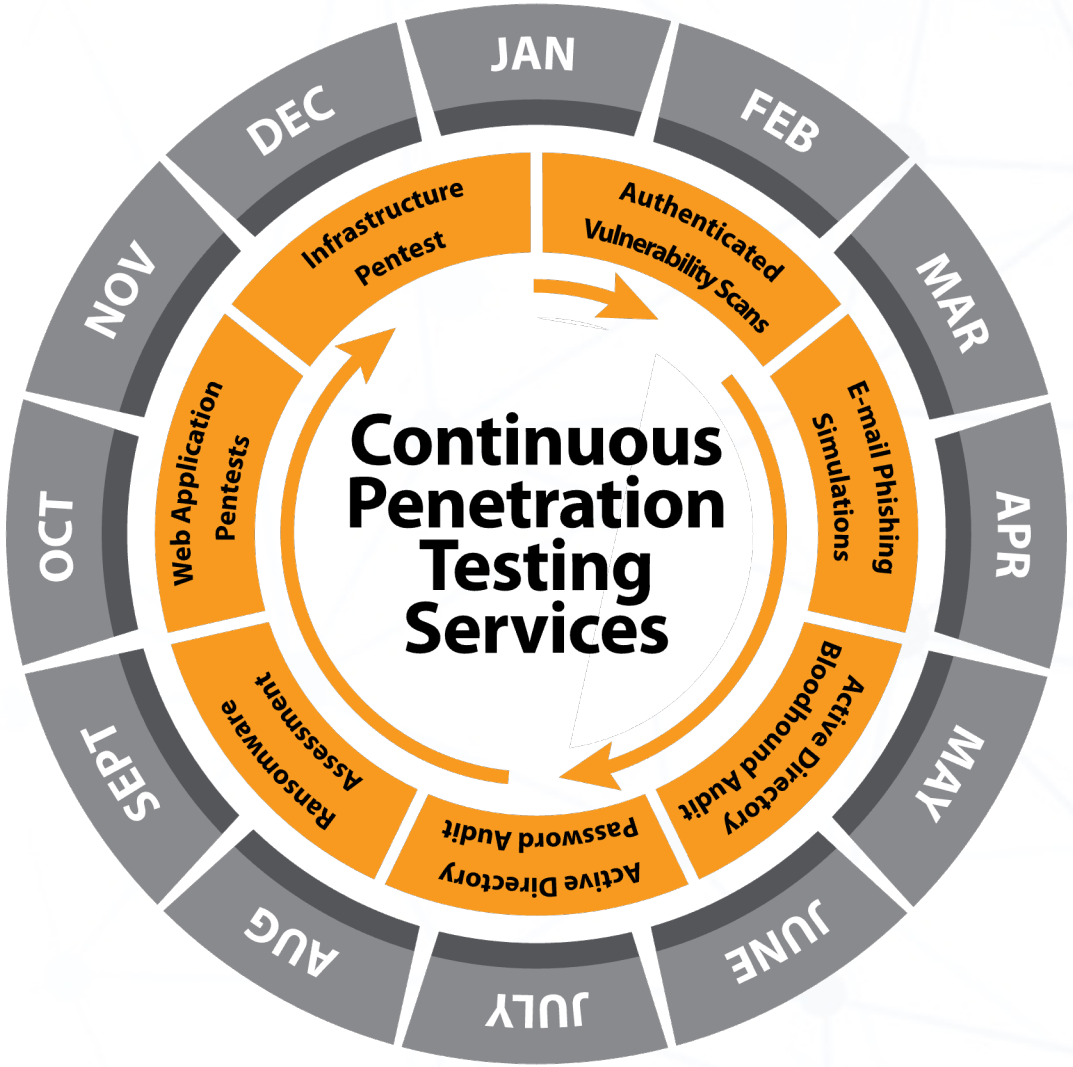
Track and improve your organization security posture

ADVANCED HUNTING

Advanced threat hunting

Management and APIs

Pentest as a Service



How This Helps You

- Continuous Protection
- Reduced Exposure (more testing, less drifting)
- Proactive vs Reactive
- Realistic Simulation (Attacker mindset)
- Flexible Scheduling

CrucialLogics
consulting with a conscience™

Packetlabs

The Final Word

What is in a name?

What's Next?

A 60-minute video meeting with members of this team (as required) for a personalized review of your steps required to become better protected.

Contact any of our speakers or respond to our follow up email to book it.

The meeting must occur prior to November 30, 2021.

Questions?

To ask our speakers a question, type your question into the Chat located in the bottom right portion of the screen.

Thank you for joining us today.

Amol Joshi
CrucialLogics
Amol.Joshi@cruciallogics.com

Richard Rogerson
Packetlabs
Rogerson@packetlabs.net