VULNERABILITY TRIAGE (AKA THE SWEET SCIENCE OF PRIVILEGE ESCALATION)

BY ERIN ROSA

WHAT DO WE DO?

We are paid to hack into our targets and pwn as many things as possible in the time that is allotted to us.

WHAT DO WE DO?

~~We are paid to hack into our targets and pwn as many things as possible in the time that is allotted to us.~~

We are paid to..

- Hack into our targets
- Identify as many vulnerabilities as possible in the time allotted
- Document all findings and validate our data
- Offer an honest risk assessment and recommendations to mitigate risk
- Act ethically and with integrity when we do so

THE CRAZY EIGHT

What I look at first during engagements for optimum privilege escalation

1. BIG BAD VULNS

- RCEs, authentication bypass, and misconfigurations oh my!
- Anything that can get you a shell is an easy win

2. SMB/LDAP/KERBEROS

- The “Domain Admin” protocols
- Relay and password attacks
- You don’t want to see these open externally

3. INFORMATION LEAKAGE

- Passwords
- Cloud secrets
- API/session keys
- Sensitive PII and data

4. COMMON SOFT PORTS

- Anything that accepts a password and can be leveraged in password attacks
- Web portals, SSH, Telnet, FTP, SQL
- Don’t forget VNC!

5. MAIL SERVERS

- On prem Exchange servers (WHY do they still exist?!?!)
- Mail relaying and user impersonation
- Common entrance point for APTs

6. PRINTERS

- No, really
- Authentication coercion (printerbug)
- Can you see what the org is printing?

7. ADDITIONAL NETWORK DEVICES

- SNMP and community strings
- IPMI and out-of-band management platforms
- Cisco devices, network gizmos

8. ENCRYPTION

- Downgrade attacks, traffic sniffing
- PKI is complex, yo
- TLS/SSL issues are also boring to me
- Extremely important externally and internally

FIN

FIN ACK