Adversary initial foothold into networks

Presented By

BLAY ABU SAFIAN

INVETECK
GLOBAL

Whoami?

BLAY ABU SAFIAN

FOUNDER/CEO INVETECK GLOBAL

- CTF Team Lead For Black Cybersecurity Association(USA)
- Red Teamer
- Offensive Trainer
- Int. Speaker

Get Social

in BLAY ABU SAFIAN

INSTAGRAM: K1NGBLAY

Today’s Agenda

01. Previous Footholds into networks

02. Goal of Compromisation

03. Initial Foothold Technique

04. Live Demo

05. Prevention and mitigation

Previous Footholds into networks

01. Ratankba Attack.

02. Bronze Butler.

Goal of Compromisation

INVETECK GLOBAL

01. Gain limited privilege in network.

02. Escalate or elevate privilege.

03. Accomplish a mission.

Initial Foothold Technique

INVETECK GLOBAL

01. Default Accounts - Abusing default credentials of a default account to gain initial foothold into the network.

02. Spear phishing- Sending emails with links to gain access to the target's network.

03. Exploiting public facing application- Such as websites, standard applications like (FTP,SSH,SMB).

04. Exploiting public facing remote services - exploiting remote service gateways such as VPN's and Citrix etc to gain access into internal networks.

DEMO TIME

100 HACKER 10
0100 DATA SECURITY 1001001
0110010 PASSWORD 00100100
00 IDENTITY THEFT 1001001

Prevention and mitigation

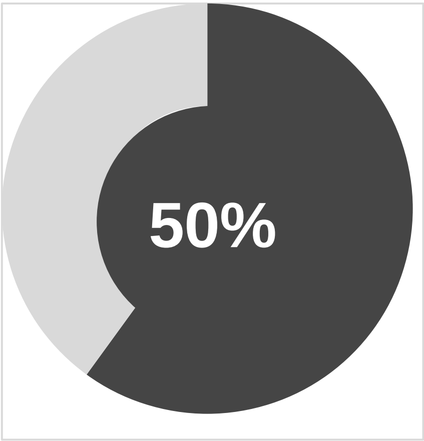
Ensure strong password policies.

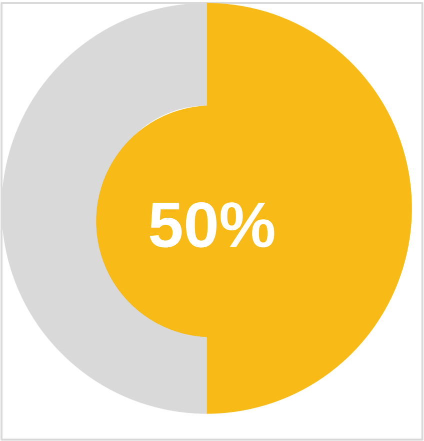
User Awareness Training.

Regularly conduct vulnerability assessment and penetration testing (VAPT) on organization.

Enable multi-factor authetication.

Questions & Answers





THANK YOU

For Your Time & Undivided Attention